Quantum Inf Process (2014) 13:2343–2352
DOI 10.1007/s11128-014-0805-z

Multi-party quantum private comparison protocol based on d-dimensional entangled states

Qing-bin Luo · Guo-wu Yang · Kun She · Wei-na Niu · Yu-qi Wang

Received: 25 May 2014 / Accepted: 29 July 2014 / Published online: 14 August 2014

Abstract In this paper, a novel quantum private comparison protocol with l-party and d-dimensional entangled states is proposed. In the protocol, l participants can sort their secret inputs in size, with the help of a semi-honest third party. However, if every participant wants to know the relation of size among the l secret inputs, these two-participant protocols have to be executed repeatedly $\frac{l(l-1)}{2}$ times. Consequently, the proposed protocol needs to be executed one time. Without performing unitary operation on particles, it only need to prepare the initial entanglement states and only need to measure single particles. It is shown that the participants will not leak their private information by security analysis.

Keywords Quantum cryptography · Private comparison · Entangled state

1 Introduction

Since Bennett and Brassard [1] presented the first quantum key distribution protocol (BB84 protocol), quantum cryptography has been rapidly developed. Compared to classical cryptography, the main advantages is that an eavesdropper can easily be detected by using the characteristics of quantum mechanics. Therefore, a lot of results have been gained, such as quantum key distribution [1–4], quantum commitment

Q. Luo (✉) · K. She
School of Information and Software Engineering, University of Electronic Science
and Technology of China, Chengdu 611731, China
e-mail: qingbinluo@126.com

K. She
e-mail: kunshe@126.com

G. Yang · W. Niu · Y. Wang
School of Computer Science and Engineering, University of Electronic Science
and Technology of China, Chengdu 611731, China

[5–8], quantum secret sharing [9–12], quantum secure direct communication [13–16], quantum conversation [17] and so on.

In recent years, quantum privacy comparison (QPC) protocols attract many researchers' attention. Privacy comparison protocol can be traced to the millionaire problem proposed by Professor Yao [18]. He pointed out that 'Two millionaires wish to know who is richer; however, they do not want to find out inadvertently any additional information about each other's wealth. How can they carry out such a conversation?'. By this question, Professor Yao introduced Secure computation. Then, Goldreich et al. [19] developed it as a secure multiparty computation. Unfortunately, Lo [20] pointed out that a quantum two-party secure computation is impossible. However, Yang and Wen [21] presented a QPC protocol with the assistance of a semi-trusted third party. In the ensuing years, there are numerous results on QPC protocol.

We put these studies into four stages. In the first stage, two distrustful participants compared the equivalence of their private information. According to what Liu et al summarized in Ref. [22], the research results of this stage have been divided into three categories: (1) the quantum cryptography QPC [23,24], (2) the superdense coding QPC [21,25–27], (3) the entanglement swapping QPC [28–30]. In the second stage, two participants compared the size of their secret inputs. Lin et al. [31] proposed a QPC protocol which can compare the size of two participants' inputs based on d-dimensional Bell states, Zhang et al. [32] solved the millionaires problem based on it. In the third stage, multiple participants compared the equivalence of information, Chang et al. [33] proposed a QPC protocol which can compare the equivalence of multi-participants' information using GHZ states. Liu et al. [34] presented a multi-party quantum private protocol based on d-dimensional basis states. In the fourth stage, multi-participants compare the size of their secret inputs. It is a pity that there are no research results appear so far. This paper focuses on this issue.

In this paper, we present a novel quantum private comparison protocol with l-party and d-dimensional entangled states, with the help of a semi-honest third party. l participants' secret inputs can be sorted in size. Here, semi-honest third party (TP) refers, he will be strictly in accordance with the implementation of the protocol. That is to say TP will not conspire with external attackers or participants, even though he may be very curious about participants' secret information, and want to deduce it. The rest of this paper is organized as follows. In Sect. 2, the preliminaries are introduced. In Sect. 3, the protocol is described in details. In Sect. 4, the security and efficiency are analyzsed. Finally, a short conclusion is given in Sect. 5.

2 Preliminaries

In this section, we will discuss the pre-knowledge of the protocol, which includes modulo d subtraction '$\ominus$', maximally entangled states which are l-party and d-dimension, and their properties.

2.1 The property of subtraction modulo d

Subtraction operation '$\ominus$' can be seen as the inverse operation of '$\oplus$' in the remainder plus group of modulo d $(Z_d, \oplus)$, i.e., for $\forall a, b \in Z_d$, $a \ominus b = a \oplus b^{-1}$(where b^{-1}

is the inverse element of b in group Z_d). So, '$\ominus$' operation can be seen the binary operation in residue class Z_d. We assume that the strict total order of the elements in Z_d is $\bar{0} < \bar{1} < \cdots < \overline{d-1}$(without confusion, we still denote the elements as $0, 1 \cdots d-1$). The '$\ominus$' operation has the property which will be used in the following pages as follows:

For two natural numbers $n_1, n_2 \in \{0, 1, \ldots, n\}$, set $d = 2n + 1$, the relationship in size between n_1 and n_2 can be ascertained by the mapping σ, where

$$\sigma(n_1 \ominus n_2) = \begin{cases} n_1 = n_2 & : \quad \text{if}(n_1 \ominus n_2 = 0) \\ n_1 > n_2 & : \quad \text{if} 0 < (n_1 \ominus n_2) \leq n \\ n_1 < n_2 & : \quad \text{if} n < (n_1 \ominus n_2) \leq 2n \end{cases} \tag{1}$$

In fact, for $n_1, n_2 \in \{0, 1, \ldots, n\}$, in the remainder plus group Z_d(where $d = 2n + 1$), if $n_1 = n_2$, then $n_1 \ominus n_2 = n_1 \oplus n_2^{-1} = n_1 \oplus n_1^{-1} = 0$. Because the inverse of the element in the group is unique, it is true, vice versa. If $n_1 > n_2$, set $n_1 = n_0 \oplus n_2$ (where $n_0 \in \{1, 2, \ldots, n\}$), then $n_1 \ominus n_2 = n_1 \oplus n_2^{-1} = n_0 \oplus n_2 \oplus n_2^{-1} = n_0$, so $0 < (n_1 \ominus n_2) \leq n$, and conversely. If $n_1 < n_2$, set $n_2 = n_0 \oplus n_1$, then $n_2^{-1} = n_1^{-1} \oplus n_0^{-1}$, now $n_1 \ominus n_2 = n_1 \oplus n_2^{-1} = n_1 \oplus n_1^{-1} \oplus n_0^{-1} = n_0^{-1}$, since $n_0 \in \{1, 2, \ldots, n\}$,$n_0^{-1} = d \ominus n_0 \in \{n + 1, n + 2, \ldots, 2n\}$, we conclude that $n < (n_1 \ominus n_2) \leq 2n$, and conversely.

2.2 L-party and d-dimensional entangled state

In this subsection, we introduce a maximally entangled state which is l-party and d-dimension, and its properties. Its application of superdense coding was discussed in Ref. [35].

$$|\psi^s_{v_2, v_3, \ldots, v_l}\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d-1} e^{\frac{2\pi ijs}{d}} |j \oplus 0\rangle \otimes |j \oplus v_2\rangle \otimes \cdots \otimes |j \oplus v_l\rangle \tag{2}$$

Here, '$\oplus$' is addition modulo d, where $s, v_2, v_3, \ldots, v_l \in \{0, 1, \ldots, d-1\}$, we set the increment of the first particle: $v_1 = 0$.

As same as Ref. [32], two mutually unbiased orthogonal bases are utilized. One is $MB = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$, the other is $MF = \{F|0\rangle, F|1\rangle, \ldots, F|d-1\rangle\}$, where '$F$'is discrete Fourier transform defined as follows

$$F|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^{d-1} e^{\frac{2\pi ijk}{d}} |k\rangle, j = 0, 1, \ldots, d-1. \tag{3}$$

Suppose the measurement value of the single-particle states $|0\rangle$ is 0, $|1\rangle$ is 1, ..., $|d-1\rangle$ is $d-1$ in the basis $MB = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. If the initial maximally entangled state in (1) has been known, the measurement value of ith and jth particle do '$\ominus$' operation, the value is $v_i \ominus v_j$.

In order to clearly explain the property, let us take the four-particle entangled state in (1) as an example. The four-particle entangled state is shown as follows:

$$|\psi_{130}^{0}\rangle = \frac{1}{2}(|0130\rangle + |1201\rangle + |2312\rangle + |3023\rangle) \tag{4}$$

set the measurement value of ith is k_i $(i = 1, 2, 3, 4)$, we know these value, $k_1 \ominus k_2 = 3$, $k_1 \ominus k_3 = 1$, $k_1 \ominus k_4 = 0$, $k_2 \ominus k_3 = 2$, $k_2 \ominus k_4 = 1$, $k_3 \ominus k_4 = 3$; $k_4 \ominus k_1 = 0$, $k_4 \ominus k_2 = 3$, $k_4 \ominus k_3 = 1$, $k_3 \ominus k_1 = 3$, $k_3 \ominus k_2 = 2$, $k_2 \ominus k_1 = 1$.

3 Protocol

In this section, a multi-participant QPC protocol is proposed in detail. Suppose l participants want to compare their private information in size. Then, they can proceed as follows:

Step 1. The l participants turn their private information into n-ary numbers $(n > l)$, suppose after transformation, the private information of ith participant is $M_i = (M_i^1 M_i^2 \ldots M_i^m)$, where $i \in \{1, 2, \ldots, l\}$ (If the number of some digits is less than m, then plus adequate 0 on their high-digit). then, the l participants share a group of appropriate long private key with a multiparty quantum key agreement (QKA) protocol [36–38], and turn them into n-ary keys, note the key as $K = (K^1 K^2 \ldots K^m)$.

Step 2. TP randomly prepares m $|\psi_{v_2,v_3,\ldots,v_l}^{s}\rangle(s, v_2, v_3, \ldots, v_l \in \{0, 1, \ldots, d-1\}$, $d = 2n+1)$ maximally entangled states. The first particles of these states form the sequence S_1, the second particles form the sequence S_2,. . ., the lth particles form the sequence S_l. To check the presence of eavesdroppers, TP generates $k'ml$ decoy particles from $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle, F|0\rangle, F|1\rangle, \ldots, F|d-1\rangle\}$, and uniformly insert them into the sequences $S_1, S_2, \ldots, S_l$ to get the new quantum sequences $S_1', S_2', \ldots, S_l'$, where k' is the detection rate. Finally, TP sends them to participant 1, participant 2, . . ., participant l, respectively.

Step 3. After the l participants receive the sequences, they send the acknowledgements to TP. Then, TP announces the positions and bases of the decoy particles, the l participants measure these particles and return the measurement results to TP. TP verifies these results and checks whether eavesdroppers exist in the quantum channels. If the error rate is less than the predetermined threshold ($\tau = 2 \sim 8.9\,\%$ [33]), move to next step, Otherwise, the protocol is aborted.

Step 4. Each of the l participants measure the remaining m particles. Here, distributing quantum measurement which is described in Ref. [39] is used, this measurement is indirect and non-destructive. Suppose the ith participant gets m measurement results $(k_i^1, k_i^2, \ldots, k_i^m)$ and combine them to $k_i (i = 1, 2, \ldots, l)$.

Step 5. Each of the l participants encoding their private information, i.e., compute $C_1 = M_1 \oplus K \oplus k_1$, $C_2 = M_2 \oplus K \oplus k_2, \ldots, C_l = M_l \oplus K \oplus k_l$. Then, they send the encoding information to TP via the authenticated classical channels, respectively.

Step 6. TP will finish sorting the private information in size according to the encoding information that he/she received. So, TP have to take out each digit from $C_1, C_2, \ldots, C_l$ to compare them. In order to improve the efficiency of sorting, quick sort is used when each digit of these is sorted, while radix sort is used when the whole is sorted. If the numbers of the tth digit between M_i and M_j will be compared, TP has known C_i,C_j and the initial quantum state $|\psi^{s^t}_{v^t_2, v^t_3, \ldots, v^t_l}\rangle$, so he/she can compute $r^t_{i,j} = C^t_i \ominus C^t_j \oplus (v^t_j \ominus v^t_i)$, the relationship between M^t_i and M^t_j in size can be gained as follows:

$$\sigma(r^t_{i,j}) = \begin{cases} M^t_i = M^t_j : & \text{if } (r^t_{i,j} = 0) \\ M^t_i > M^t_j : & \text{if } 0 < r^t_{i,j} \leq n \\ M^t_i < M^t_j : & \text{if } n < r^t_{i,j} \leq 2n \end{cases} \tag{5}$$

In fact,

$$\begin{aligned} r^t_{i,j} &= C^t_i \ominus C^t_j \oplus (v^t_j \ominus v^t_i) && (6)\\ &= (M^t_i \oplus K^t \oplus k^t_i) \ominus (M^t_j \oplus K^t \oplus k^t_j) \oplus (v^t_j \ominus v^t_i) && (7)\\ &= (M^t_i \ominus M^t_j) \oplus (K^t \ominus K^t) \oplus (k^t_i \ominus k^t_j) \oplus (v^t_j \ominus v^t_i) && (8)\\ &= M^t_i \ominus M^t_j && (9) \end{aligned}$$

So, TP can sort these private information according to the compared results. After sorting the end, TP announces results.

An example is given for better understanding the presented protocol. Suppose there are 3 participants (Alice, Bob and Charlie), their private information are 3, 11 and 9, if they want to sort their secret inputs without leaking private information. According to protocol, set $n = 4$, $d = 9$. The protocol is executed as follows:

Step 1. Participants turn their private information into quaternary number $M_1 = 3 = (03)_4$, $M_2 = 11 = (23)_4$, $M_3 = 9 = (21)_4$, then private key $K = (31)_4$ is shared, and $m = 2$.

Step 2. TP prepares two 3-party and 9-dimensional maximally entangled states, suppose they are $|\psi^0_{4,1}\rangle$, $|\psi^3_{2,7}\rangle$. Next, the entangled states are divided into 3 particles sequences S_1, S_2, S_3. After enough decoy particles are inserted into quondam sequences to form new sequences S'_1, S'_2, S'_3, TP send them to Alice, Bob and Charlie, respectively.

Step 3. Suppose no eavesdropper is detected, then move to step 4.

Step 4. Alice, Bob and Charlie measure the remaining particles to gain keys. When one participant measure his/her particles to get results, the other participants' results will be certain, so 81 kinds of possible results will be generated with equal probability in this example. If the measurement results of Alice are $k^1_1 = 5$, $k^2_1 = 1$, then, the results of Bob and Charlie will be settled, they are $k^1_2 = 0$, $k^2_2 = 3$; $k^1_3 = 6$, $k^2_3 = 8$.

Step 5. In this step, Alice, Bob and Charlie can gain their ciphertext $C_1 = 85$, $C_2 = 57$, $C_3 = 21$, and send them to TP.

Step 6. TP will sort the private information by computing $r^t_{i,j}(i, j \in \{1, 2, 3\}, t = 1, 2)$. according to radix sort, the low digit (here is the second digit) will be compared firstly. suppose M^2_1 has been selected as pivot element, next compare M^2_1 and M^2_2,so compute $r^2_{1,2} = (C^2_1 \ominus C^2_2) \oplus (v^2_2 \ominus v^2_1) = (5 \ominus 7) \oplus (2 \ominus 0) = 0$,$M^2_1 = M^2_2$ can be get. in the same way, compute $r^2_{1,3} = 2$, then, $M^2_1 > M^2_3$, so, $M^2_1 = M^2_2 > M^2_3$ can be gained when comparing the number on the second digit. TP can also get $M^1_2 > M^1_3 = M^1_1$ by comparing the number on the first digit. The final order can be gained by radix sort, it is $M_2 > M_3 > M_1$. TP announces the result.

4 Security and efficiency analysis

In this section, the security of the proposed protocol will be analyzed. There are 3 attacks for our protocol; they are outsider attack, participant attack and TP attack. Now, we will prove that our protocol is secure against these attacks (Sect. 4.1, 4.2, 4.3) respectively. The efficiency of protocol is discussed in Sect. 4.4.

4.1 Outsider attack

If a malicious attacker Eve wonders the secret inputs of participants, the most general strategy for him is as follows: he first intercepts the transmitted sequences from TP, then he performs a joint operation U on the intercepted particles and the auxiliary particles $|\phi\rangle$, at last, he sends the operated particles to the participants. According to Schmidt decomposition, the states after operation can be written as:

$$U(|j\rangle|\phi\rangle)_{SE} = \sum_{k=0}^{d-1} \lambda^j_k |s^j_k\rangle|E^j_k\rangle,\ j = 0, 1, \ldots, d-1. \tag{10}$$

where $\sum_{k=0}^{d-1}(\lambda^j_k)^2 = 1$, $|s^j_k\rangle$ and $|E^j_k\rangle(j = 0, 1, \ldots, d-1)$ are standard orthogonal basis of the systems which the states $|j\rangle$ and $|\phi\rangle$ belong to. If Eve wants to extract the information precisely, the reduced density matrixes of his system $\sum_{k=0}^{d-1}(\lambda^j_k)^2|E^j_k\rangle\langle E^j_k|(j = 0, 1, \ldots, d-1)$ must be discriminated precisely. It requires that $\langle E^j_k|E^{j'}_{k'}\rangle = 0$, when $j \neq j'$ or $k \neq k'$ (where$j, j', k, k' = 0, 1, \ldots, d-1$). with this condition, the unitary operation U performs on the decoy particles and additional particles has the universal form as follows:

$$U(F|p\rangle|\phi\rangle) = U\left(\frac{1}{\sqrt{d}}\sum_{J=1}^{d-1} e^{\frac{2\pi ipj}{d}}|j\rangle|\phi\rangle\right) \tag{11}$$

$$= \frac{1}{\sqrt{d}} \sum_{J=1}^{d-1} e^{\frac{2\pi ipj}{d}} U(|j\rangle|\phi\rangle) \tag{12}$$

$$= \frac{1}{\sqrt{d}} \sum_{J=1}^{d-1} \sum_{k=0}^{d-1} \lambda_k^j e^{\frac{2\pi ipj}{d}} |s_k^j\rangle|E_k^j\rangle \tag{13}$$

where $p = 0, 1, \ldots, d-1$. The reduced density matrixes of participants' system are as follows:

$$\frac{1}{d} \sum_{j=1}^{d-1} \sum_{k=0}^{d-1} (\lambda_k^j)^2 |s_k^j\rangle\langle s_k^j|. \tag{14}$$

It is obviously that the density matrix has nothing to do with the variable p. That is to say, all the subsystems on the decoy particles' position in participants' hand are identical. So the error rate in the detection stage is maximized. Hence, we have proved that an eavesdropper cannot eavesdrop the participants' information without bringing in any disturbance.

4.2 Participant attack

In this subsection, we will analyze the participant attack. Participant attack is an usual attack mode in the protocols that the participants do not trust each other. In our protocol, all the participants have negotiated a same private key K which is unknown to TP. Another key is generated through l-party and d-dimensional entangled states, and the key is different and unknown to each participant. For a dishonest participant (without loss of generality, suppose that participant 1 is a dishonest one), when he/she intercepted the other's particle sequences, it is same as outsider attack. This case will be detected in step 3. Thus, the only possible way for participant 1 to do is to perform unitary transformation on his/her particles to extract other participants' information, the operation can be shown as:

$$(U_1 \otimes I_2 \otimes \cdots \otimes I_l) \left(\frac{1}{\sqrt{d}} \sum_{j=1}^{d-1} e^{\frac{2\pi ijs}{d}} |j \oplus 0\rangle \otimes |j \oplus v_2\rangle \otimes \cdots \otimes |j \oplus v_l\rangle \right). \tag{15}$$

The reduced density matrix of participant 1's subsystem is $\frac{1}{d} \sum_{j=1}^{d-1} U_1|j\rangle\langle j|U_1^\dagger$. When he/she does nothing on the particles, the reduced density matrix is $\frac{1}{d} \sum_{j=1}^{d-1} |j\rangle\langle j|$. Hence, he/she cannot extract any other participants' information by this way. By now, we have proved that our protocol is safe against participant attack.

4.3 TP attack

In this subsection, we will discuss TP attack from two aspects. On the one hand, it will be analyzed whether TP can gain the participants' key by some measures. On

Table 1 The quantum resources used in our protocol

Quantum resource	The number of quantum resources
Single particle	$\lceil m(m-1)\log n\rceil(k+1)$
Entangled state	m
Decoy particle	$k'ml$

the other hand, if TP cannot acquire the participants' key, can he/she deduce the participants' secret through ciphertext? For the first aspect, TP can prepare m $(l+1)$-party entangled states rather than l-party entangled ones in step 2, and leave a particle sequence for himself. So he/she can deduce the participants' key in step 4 through the initial sates and the measurement result of his/her particle sequence. But according to the security analysis of QKA protocol [36–38], TP cannot gain the key in step 1; hence, TP cannot obtain the whole key of participants. For the second one, suppose TP sorts the numbers of t-digit of private information through their cipher text, when M_i^t and $M_j^t(i, j = 1, 2, \ldots, l)$ are sorted, TP will not gain the specific value except the size. After $M_1^t, M_2^t, \ldots, M_l^t$ have been sorted, if all values are different and every number is l-ary, TP can infer that the smallest number is 0, the second smallest one is 1, ..., the biggest one is $l-1$. But in our protocol, $n > l$ is required, TP will not infer the value of $M_1^t, M_2^t, \ldots, M_l^t$. So, he/she will also not infer the information $M_1, M_2, \ldots, M_l$.

In addition, the analysis is similar to Ref. [33] on lossy and noisy channel, not repeat them here.

4.4 Efficiency analysis

Because there is no an appropriate model to describe the efficiency of our protocol, we illustrate this subject through the analysis of the number of quantum resources required in our protocol. Suppose there are l participants who want to rank the private information of m digit n-ary numbers in size. In step 1 of the protocol, a QKA protocol is used. If the QKA Protocol in Ref. [36] is employed, $x(x-1)(k+1)$ single particles are used (where k is the detection rate in Ref. [36]), when x bits key are negotiated. However, every digit is n-ary in our proposed protocol, so $\lceil m(m-1)\log n\rceil(k+1)$ single particles are used in step 1. In step 2, m entangled states which are l-party and d-dimension are prepared randomly by TP, and $k'ml$ decoy particles are used. No other quantum resource is generated in the remaining steps. This has been summarized in Table 1.

5 Conclusion

This paper proposes an l-participant QPC protocol using entangled states which is l-party and d-dimension. In this protocol, l participants can sort their private information in size within one execution, with the help of a semi-honest third party. Because it is feasible that the single particles are generated and measured without unitary transformation in QKA protocol such as Ref. [36], we only need to prepare the initial entanglement states and measure single particle in proposed protocol. It is known that the participants' private information does not leak through the analysis of outsider attack, participant attack and TP attack.

Acknowledgments The authors would like to thank associate professor Yong-bin Li, Dr. Xiao-yu Li and Dr. Fan Yang who come from UESTC for discussion and National Natural Science Foundation of China (Grant Nos. 61272175) for its support.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, New York, Bangalore, India, pp. 175–179 (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121–3124 (1992)
4. Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. **88**(5), 057902 (2002)
5. Kent, A.: Quantum bit string commitment. Phys. Rev. Lett. **90**(23), 237901 (2003)
6. Mayers, Dominic: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**(17), 3414–3417 (1997)
7. Kent, A.: Unconditionally secure bit commit by transmitting measurement outcomes. Phys. Rev. Lett. **109**, 130501 (2012)
8. Liu, Y., Cao, Y., Curty, M., et al.: Experimental unconditionally secure bit commitment. Phys. Rev. Lett. **112**, 010504 (2014)
9. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
10. Tyc, T., Rowe, D.J., Sanders, B.C.: Efficient sharing of a continuous-variable quantum secret. J. Phys. A. Math. Gen. **36**(27), 7625–7637 (2003)
11. Shi, R.H., Huang, L.S., Yang, W., Zhong, H.: Multiparty quantum secret sharing with Bell states and Bell measurements. Opt. Commun. **283**(11), 2476–2480 (2010)
12. Rahaman, R., Rahaman, M.G.: Quantum secret sharing based on local distinguishability. arXiv:1403.1097 [quant-ph] (2014)
13. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
14. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high dimension quantum superdense coding. Phys. Rev. A **71**, 044305 (2005)
15. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Robust quantum secure direct communication over collective rotating channel. Commun. Theor. Phys. **53**, 645C647 (2010)
16. Hwang, T., Lin, T.H., Kao, S.H.: Quantum Secure Direct Communication between Two Strangers. arXiv:1402.6423 [quant-ph] (2014)
17. Jain, S., Muralidharan, S., Panigrahi, P.K.: Secure quantum conversation through non-destructive discrimination of highly entangled multipartite states. Europhys. Lett. **87**(6), 60008 (2009)
18. Yao, A.C.: Protocols for secure computations. In: Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (FOCS'82), Washington, DC, USA, pp. 160–164. (1982)
19. Goldreich, O., Micali, S., Wigderson, A.:How to play ANY mental game. In: Proceedings of the Nineteenth Annual ACM Conference on Theory of Computing. NewYork, pp. 218–229 (1987)
20. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**, 1154–1162 (1997)
21. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A Math. Theor. **42**, 055305 (2009)
22. Liu, W.J., Liu, C., Wang, H., et al.: Quantum private comparison: a review. IETE Tech. Rev. **30**(5), 439–444 (2013)
23. Chen, X.B., Xu, G., Niu, X.X., et al.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single particle measurement. Opt. Commun. **283**(7), 1561–1565 (2010)

24. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
25. Liu, B., Gao, F., Jia, H.Y., et al.: Efficient quantum private comparison employing single photons and collective detection. Quantum Inf. Process. **12**(2), 887–897 (2013)
26. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with W state. Opt. Commun. **284**(12), 3160–3163 (2011)
27. Jia, H.Y., Wen, Q.Y., Li, Y.B., Gao, F.: Quantum private comparison using genuine four particle entangled states. Int. J. Theor. Phys. **51**(4), 1187–1194 (2012)
28. Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z.: A protocol for the quantum private comparison of equality with type state. Int. J. Theor. Phys. **51**(1), 69–77 (2012)
29. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on bell entangled states. Commun. Theor. Phys. **57**(4), 583–588 (2012)
30. Liu, W., Wang, Y.B.: Quantum private comparison based on GHZ entangled states. Int. J. Theor. Phys. **51**(11), 3596–3604 (2012)
31. Lin, S., Sun, Y., Liu, X., Yao, Z.: Quantum private comparison protocol with d-dimensional Bell states. Quantum Inf. Process. **12**(1), 559–568 (2013)
32. Zhang, W.W., Li, D., Zhang, K., Zuo, H.: A quantum protocol for millionaire problem with Bell states. Quantum Inf. Process. **12**(6), 2241–2249 (2013)
33. Chang, Y., Tsai, C., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process. **12**(2), 1077–1088 (2013)
34. Liu, W., Wang, Y.B., Wang, X.M.: Multi-party quantum private comparison protocol using d-dimensional basis states without entanglement swapping. Int. J. Theor. Phys. **53**(4), 1085–1091 (2014)
35. Liu, X.S., Long, G.L., Tong, D.M., Li, F.: General scheme for super dense coding between multi-parties. Phys. Rev. A **65**, 022304 (2002)
36. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**(4), 1797–1805 (2013)
37. Sun, Z.W., Zhang, C., Wang, B.H., et al.: Improvements on multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**(11), 3411–3420 (2013)
38. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. **12**(2), 921–932 (2013)
39. Gupta, M., Pathak, A., Srikanth, R., et al.: General circuits for indirecting and distributing measurement in quantum computation. Int. J. Quantum Inf. **5**(04), 627–640 (2007)