Int J Theor Phys (2017) 56:2783–2791
DOI 10.1007/s10773-017-3442-3

An Novel Protocol for the Quantum Secure Multi-Party Summation Based on Two-Particle Bell States

Wen Liu[1] · Yong-Bin Wang[1] · Wen-Qin Fan[1]

Received: 20 February 2017 / Accepted: 5 June 2017 / Published online: 17 June 2017

Abstract A protocol for the quantum secure multi-party summation based on two-particle Bell states is proposed. In this protocol, two-particle Bell states are used as private information carriers. Without using the entangled character of Bell states, we also use Pauli matrices operations to encode information and Hadamard matrix to extract information. The proposed protocol can also resist various attacks and overcomes the problem of information leakage with acceptable efficiency. In theory, our protocol can be used to build complex secure protocols for other multiparty computations and also lots of other important applications in distributed networks.

Keywords Quantum secure multi-party summation · Bell states · Security · Information leakage

1 Introduction

Secure multi-party computation(SMC) is an important subfield of cryptography, which was introduced by Goldreich in [1]. Secure multi-party computation has been extended to the quantum field and many researchers have investigated secure multi-party computation problems based on quantum states, such as quantum protocol for millionaire problem [2–6], quantum private comparison protocol [7–16], secure multiparty quantum summation [17–22], quantum private query [23–27] etc.

Secure multi-party summation problem is a special problem in secure multi-party computation. The problem of secure multi-party summation is described as follows: there are n parties P_1, P_2, .., P_n and every party P_i has a private information x_i. They want to correctly

✉ Wen Liu
lw_8206@163.com

[1] School of Computer Science, Communication University of China, Beijing, 100024, China

calculate a summation function $F(x_1, x_2, ..., x_n)$ without revealing any party's secret information. It is a fundamental primitive of SMC, which can be used to build complex secure protocols for other multiparty computations.

However, there are only a few quantum protocols for Secure Multiparty Summation. In 2006, Hillery et al. [17], proposed a multi-party summation protocol with the two-particle N-level entangled states. In 2007, Du et al. [18] presented a secure quantum addition module $n+1$ based on non-orthogonal single states. In 2010, Chen et al. [19] presented a quantum summation protocol with the multi-particle entangled GHZ states. In 2014, Zhang et al. [20] employed single photons in both polarization and spatial-mode degrees of freedom to design a quantum summation protocol. In 2015, Zhang et al. [21] proposed a quantum summation protocol based on the genuinely maximally entangled six-qubit states. In 2016, Shi et al. [22] present a quantum summation protocol based on quantum Fourier transform and CNOT gate operators.

In this paper, we firstly proposed a quantum secure two-party summation protocol based on two-particle Bell states. This protocols includes a semi-honest third party(TP). TP can prepares the initial states and gets the calculation results. TP also executes the protocol loyally, keeps a record of all its intermediate computations and might try to steal the players' private inputs from the record, but he cannot be corrupted by the adversary. Then, we extent the two-party protocol to multi-party quantum summation without TP. Secure multiparty summation can be applied in secret sharing, electronic voting, secure sorting, data mining and so on. In our protocol, participants only use common EPR states and single particle operations without using entanglement swapping. So our protocol is simpler and easier to implement.

The structure of this paper is as follows: we propose a quantum secure two-party summation protocol based on two-particle Bell states in Section 2; and we analyze the security of this protocol in Section 3; we propose a quantum secure multi-party summation protocol based on two-particle Bell states in Section 4. A brief discussion and the concluding summary are given in Section 5.

2 The Quantum Secure Two-Party Summation Protocol Based on Two-Particle Bell States

Before presenting the protocol, we firstly give a description of two-level EPR states used in our protocol as follows:

$$|B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |B_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{1}$$

The four Pauli matrices are described as follows:

$$\begin{aligned} \sigma_{00} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_{10} &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \sigma_{11} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \end{aligned} \tag{2}$$

Using these Pauli matrices operations on $|0\rangle, |1\rangle$, we can get that:

$$\begin{aligned} &\sigma_{00}|0\rangle = |0\rangle, \sigma_{00}|1\rangle = |1\rangle, \sigma_{01}|0\rangle = |1\rangle, \sigma_{01}|1\rangle = |0\rangle, \\ &\sigma_{10}|0\rangle = |0\rangle, \sigma_{10}|1\rangle = -|1\rangle, \sigma_{11}|0\rangle = |1\rangle, \sigma_{11}|1\rangle = -|0\rangle. \end{aligned} \tag{3}$$

Supposed that there are two binary numbers $x_1, x_2 \in \{0, 1\}$, we apply $\sigma_{x_1x_2}$ on $|B_{00}\rangle, |B_{11}\rangle$:

$$\begin{aligned} \sigma_{x_1x_2} |B_{00}\rangle &= |B_{00}\rangle \\ \sigma_{x_1x_2} |B_{11}\rangle &= (-1)^{x_1 \oplus x_2} |B_{11}\rangle \end{aligned} \tag{4}$$

The Hadamard matrix is described as follows:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{5}$$

Using these Hadamard matrix on $|0\rangle, |1\rangle$, we can get that:

$$\begin{aligned} &H |0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), H |1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &H \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^0 |1\rangle) = |0\rangle, \ H \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^1 |1\rangle) = |1\rangle \end{aligned} \tag{6}$$

Supposed that there two parties, Alice and Bob, where Alice has a secret X and Bob has a secret Y. The binary strings of X, Y are $(x_1, x_2, ...x_L)$, $(y_1, y_2, ...y_L)$. TP can get the summation result $(x_1 \oplus y_1, x_2 \oplus y_2, ...x_L \oplus y_L)$, where $\oplus$ denotes the addition module 2. The detail of our secure two-party summation protocol is described as follows:

(1) TP prepares a L-length sequence of three-particle states:
$\frac{1}{\sqrt{2}}(|0\rangle |B_{00}\rangle + |1\rangle |B_{11}\rangle)_{T_1A_1B_1}, ..., \frac{1}{\sqrt{2}}(|0\rangle |B_{00}\rangle + |1\rangle |B_{11}\rangle)_{T_LA_LB_L}$.
TP takes the first particle from each state in this sequence to form an ordered particles sequence

$$[(P_{T_1}), (P_{T_2}), ..., (P_{T_L})] \tag{7}$$

which is called S_T.
TP takes the second particle from each state in this sequence to form an ordered particles sequence

$$[(P_{A_1}), (P_{A_2}), ..., (P_{A_L})] \tag{8}$$

which is called S_A.
TP takes the third particle from each state in this sequence to form an ordered particles sequence

$$[(P_{B_1}), (P_{B_2}), ..., (P_{B_L})] \tag{9}$$

which is called S_B.
TP also prepares two sequences of L' particles, which are randomly chosen from four photon states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and randomly inserts these two sequences of L' particles into S_A, S_B to form two new sequence S'_A, S'_B. TP records the insert positions sequences Po_A, Po_B and sends S'_A, S'_B to Alice,Bob respectively.

(2) After receiving $S'_A(S'_B)$, Alice(Bob) and TP perform the eavesdropping check. TP announces the insert positions $Po_A(Po_B)$ and the measuring bases of $S'_A(S'_B)$. If the insert particle is $|0\rangle$ or $|1\rangle$, the measuring basis is Z basis; if the insert particle is $|+\rangle$ or $|-\rangle$, the measuring basis is X basis. Then Alice(Bob) chooses the L' particles from $S'_A(S'_B)$ according to the insert positions $Po_A(Po_B)$ and measures these particles according to the measuring bases. Alice(Bob) and TP can find the existence of an eavesdropper by a predetermined threshold of error rate according to their measuring results. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they discards the measured photons in $S'_A(S'_B)$ and continue to the next step.
For $i = 1, 2, ..., L$, Alice calculates $P'_{A_i} = \sigma_{x_i,r_i} P_{A_i}$. The sequence of P'_{A_1}, $P'_{A_2}, ..., P'_{A_L}$ is denoted by Sq_A.

For $i = 1, 2, ..., L$, Bob calculates $P'_{B_i} = \sigma_{y_i,r_i} P_{B_i}$. The sequence of P'_{B_1}, P'_{B_2}, ..., P'_{B_L} is denoted by Sq_B.

where $r_i (i = 1, 2, ..., L)$ is randomly chosen from 0, 1.

Alice(Bob) also prepares a L'-particle sequence, which are randomly chosen from four photon states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and randomly inserts these L' particles into $Sq_A(Sq_B)$ to form a new sequence $Sq'_A(Sq'_B)$. Alice(Bob) records the insert positions $Po'_A(Po'_B)$ and sends $Sq'_A(Sq'_B)$ to TP.

(3) After receiving $Sq'_A(Sq'_B)$, Alice(Bob) and TP perform the eavesdropping check. Alice(Bob) announces the insert positions $Po'_A(Po'_B)$ and the measuring bases of $Sq'_A(Sq'_B)$. If the insert particle is $|0\rangle$ or $|1\rangle$, the measuring basis is Z basis; if the insert particle is $|+\rangle$ or $|-\rangle$, the measuring basis is X basis. Then TP chooses the L' particles from $Sq'_A(Sq'_B)$ according to the insert positions $Po'_A(Po'_B)$ and measures these particles according to the measuring bases. Alice(Bob) and TP can find the existence of an eavesdropper by a predetermined threshold of error rate according to their measuring results. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they discards the measured photons in $Sq'_A(Sq'_B)$ and continue to the next step.

For $i = 1, 2, ..., L$:

Except the first particle, TP sets others particles to 0 and applies the Hadamard operation to the first particle P_{T_i}:

$$H(|0\rangle + (-1)^{x_i \oplus r_i}(-1)^{y_i \oplus r_i}|1\rangle) = |x_i \oplus y_i\rangle . \tag{10}$$

P_1 uses Z basis to measure the state and gets $x_i \oplus y_i$.

3 Security Analysis

Firstly, we show that the outside attack is invalid to our protocol. Secondly, we show that the Alice, Bob, TP can not get any information about the private information of each other.

3.1 Outside Attack

We analyze the possibility of the outside eavesdropper to get information about X and Y in every step of protocol. In our protocol, the chance of attack from the outside eavesdropper is to attack the quantum channel in Step (2). In Step (2), the outside eavesdropper can attack the quantum channel when Alice,Bob sent Sq_A, Sq_B to TP. Because of the use of nonorthogonal decoy photons, we performed eavesdropper checking process in Step (3) and several kinds of outside attacks, such as the intercept-resend attack, the measure-resend attack, the entangle-measure attack, were detected with nonzero probability. Anyone who do not know the insert positions and bases of decoy particles cannot distinguish the decoy particles and the signal particles. For some special attacks, such as the photon-number-splitting (PNS) attack, the decoy-photon Trojan horse attack and the invisible photon Trojan horse attack, participants can defeat these attacks by using some beam splitters to split the sampling signals chosen for eavesdropping check before their operations and inserting filters in front of their devices to filter out the photon signal with an illegitimate wavelength. So, our quantum protocol is robust against outside attack.

3.2 Participant Attack

The term "participant attack", which emphasizes that the attacks from dishonest users are generally more powerful and should be paid more attention to, is first proposed by Gao et al. in Ref. [28] and has attracted much attention in the cryptanalysis of quantum cryptography [29–34]. We analyze the possibility of the three parties to get information about X and Y in our protocol. We firstly analyze the case that Alice wants to learn Bob's private information Y. Secondly, we analyze the case that TP wants to learn the private information X, Y of Alice and Bob.

Case 1: Alice and Bob want to learn the private information of each other.

In our protocol, Alice can only gets $P_{A_1}, P_{A_2}, ..., P_{A_L}$ from TP and Bob can only gets $P_{B_1}, P_{B_2}, ..., P_{B_L}$. These particles aren't related to Alice's or Bob's private information B. So Alice and Bob cannot infer any information about the private information of each other.

Case 2: TP wants to learn the private information X, Y of Alice and Bob.

In our protocol, TP knows $P_{A_1}, P_{A_2}, ..., P_{A_L}, P_{B_1}, P_{B_2}, ..., P_{B_L}$ and also gets $P'_{A_1}, P'_{A_2}, ..., P'_{A_L}, P'_{B_1}, P'_{B_2}, ..., P'_{B_L}$.

For $i = 1, 2, ..., L$: $P'_{A_i} = \sigma_{x_i,r_i} P_{A_i}$; $P'_{B_i} = \sigma_{y_i,r_i} P_{B_i}$.

Because $r_i (i = 1, 2, ..., L)$ is randomly chosen from $\{0, 1\}$ by Alice and Bob, TP cannot exactly know $r_i (i = 1, 2, ..., L)$. So TP cannot infer any information about the private information of Alice and Bob.

4 The Quantum Secure Multi-Party Summation Protocol Based on Two-Particle Bell States

Supposed that there n parties, $P_1, P_2, ..., P_n$, where each P_i has a secret X_i. The binary strings of X_i is $\left(x_i^1, x_i^2, ...x_i^L\right)$. $P_1, P_2, ..., P_n$ can get the summation result $\left(\bigoplus_{i=1}^{n} x_i^1, \bigoplus_{i=1}^{n} x_i^2, ..., \bigoplus_{i=1}^{n} x_i^L\right)$, where $\oplus$ denotes the addition module 2. In this case, we suppose that the player P_1 can act as TP.

The detail of our secure multi-party summation protocol is described as follows:

(1) If $n - 1 \mod 2 = 0$, P_1 prepares a L-length sequence of n-particle states: $((|0\rangle |B_{00}\rangle ... |B_{00}\rangle + |1\rangle |B_{11}\rangle ... |B_{11}\rangle)_{P_1^1 P_1^2 ... P_1^n}, ..., (|0\rangle |B_{00}\rangle ... |B_{00}\rangle + |1\rangle |B_{11}\rangle ... |B_{11}\rangle)_{P_L^1 P_L^2 ... P_L^n})$.

P_1 takes the ith particle from each state in this sequence to form an ordered particles sequence

$$\left[(P_1^i), (P_2^i), ..., (P_L^i)\right] \tag{11}$$

which is called $S_i (i = 1, ..., n)$ sequence.

P_1 keeps S_1 and prepares $n-1$ L'-particle sequences. He inserts these particles into $S_2, ..., S_n$ respectively and gets new sequences $S'_2, ..., S'_n$. He also also records insert positions Po_i and sends S_i to P_i, where $i = 2, ..., n$.

If $n - 1 \mod 2 = 1$, P_1 prepares a L-length sequence of $n + 1$-particle states: $((|0\rangle |B_{00}\rangle ... |B_{00}\rangle + |1\rangle |B_{11}\rangle ... |B_{11}\rangle)_{P_1^1 ... P_1^{n+1}}, ..., (|0\rangle |B_{00}\rangle ... |B_{00}\rangle + |1\rangle |B_{11}\rangle ... |B_{11}\rangle)_{P_L^1 ... P_L^{n+1}})$.

P_1 takes the ith particle from each state in this sequence to form an ordered particles sequence

$$[(P_1^i), (P_2^i), ..., (P_L^i)] \tag{12}$$

which is called $S_i (i = 1, 2, ..., n + 1)$ sequence.

P_1 keeps S_1, S_{n+1} and prepares $n - 1$ L'-particle sequences. He inserts these particles into S_2, ..., S_n respectively and gets new sequences S_2', ..., S_n'. He also records insert positions Po_i sends S_i' to P_i, where $i = 2, ..., n$.

(2) If $n - 1 \mod 2 = 0$:

For $i = 2, ..., n$: After receiving S_i', P_1 and P_i perform the eavesdropping check. P_i announces the insert positions Po_i and the measuring bases of S_i'. If the insert particle is $|0\rangle$ or $|1\rangle$, the measuring basis is Z basis; if the insert particle is $|+\rangle$ or $|-\rangle$, the measuring basis is X basis. Then P_i chooses the L' particles from S_i' according to the insert positions Po_i and measures these particles according to the measuring bases. P_1 and P_i can find the existence of an eavesdropper by a predetermined threshold of error rate according to their measuring results. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they discards the measured photons in S_i' and continue to the next step.

For $i = 2, ..., n$:

For $k = 1, 2, ..., L$:

P_i calculates $P_k^{i'} = \sigma_{x_i^k, r_{\lceil \frac{i}{2} \rceil}} P_k^i$. The sequence of $P_1^{i'}$, $P_2^{i'}$, ..., $P_L^{i'}$ is denoted by Sq_i, where $r_{\lceil \frac{i}{2} \rceil}$ is randomly chosen from 0, 1.

For $i = 2, ..., n$:

P_i also prepares a L'-particle sequence, which are randomly chosen from four photon states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ and randomly inserts these L' particles into Sq_i to form a new sequence Sq_i'. P_i records the insert positions Po_i' and sends Sq_i' to P_1.

For $i = 2, ..., n$: After receiving Sq_i', P_1 and P_i perform the eavesdropping check. P_i announces the insert positions Po_i and the measuring bases of Sq_i'. If the insert particle is $|0\rangle$ or $|1\rangle$, the measuring basis is Z basis; if the insert particle is $|+\rangle$ or $|-\rangle$, the measuring basis is X basis. Then P_i chooses the L' particles from Sq_i' according to the insert positions Po_i' and measures these particles according to the measuring bases. P_1 and P_i can find the existence of an eavesdropper by a predetermined threshold of error rate according to their measuring results. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they discards the measured photons in Sq_i' and continue to the next step.

If $n - 1 \mod 2 = 1$:

For $i = 2, ..., n$: After receiving S_i', P_1 and P_i perform the eavesdropping check. P_i announces the insert positions Po_i and the measuring bases of S_{i+1}'. If the insert particle is $|0\rangle$ or $|1\rangle$, the measuring basis is Z basis; if the insert particle is $|+\rangle$ or $|-\rangle$, the measuring basis is X basis. Then P_i chooses the L' particles from S_i' according to the insert positions Po_i and measures these particles according to the measuring bases. P_1 and P_i can find the existence of an eavesdropper by a predetermined threshold of error rate according to their measuring results. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they discards the measured photons in S_i' and continue to the next step.

For $i = 2, ..., n$:

For $k = 1, 2, ..., L$:

P_i calculates $P_k^{i'} = \sigma_{x_i^k, r_{\lceil \frac{i}{2} \rceil}} P_i$. The sequence of $P_1^{i'}$, $P_2^{i'}$, ..., $P_L^{i'}$ is denoted by Sq_i, where $r_{\lceil \frac{i}{2} \rceil}$ is randomly chosen from 0, 1.

For $k = 1, 2, ..., L$:

P_1 calculates $P_k^{n+1'} = \sigma_{r_1^k, r_{\lceil \frac{n}{2} \rceil}} P_k^{n+1}$. The sequence of $P_1^{n+1'}$, $P_2^{n+1'}$, ..., $P_L^{n+1'}$ denoted by Sq_{n+1}, where $r_1^k = 0$.

For $i = 2, ..., n$:

P_i also prepares a L'-particle sequence, which are randomly chosen from four photon states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ and randomly inserts these L' particles into Sq_i to form a new sequence Sq_i'. P_i records the insert positions Po_i' and sends Sq_i' to P_1.

For $i = 2, ..., n$:

After receiving Sq_i', P_1 and P_i perform the eavesdropping check. P_i announces the insert positions Po_i and the measuring bases of Sq_i'. If the insert particle is $|0\rangle$ or $|1\rangle$, the measuring basis is Z basis; if the insert particle is $|+\rangle$ or $|-\rangle$, the measuring basis is X basis. Then P_i chooses the L' particles from Sq_i' according to the insert positions Po_i' and measures these particles according to the measuring bases. P_1 and P_i can find the existence of an eavesdropper by a predetermined threshold of error rate according to their measuring results. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they discards the measured photons in Sq_i' and continue to the next step.

(3) If $n - 1 \mod 2 = 0$: For $k = 1, 2, ..., L$:

Except the first particle, P_1 sets others particles to 0 and applies the Hadamard operation to the first particle:

$$H\left(|0\rangle + (-1)^{\bigoplus_{i=2}^{n}\left(x_i^k \oplus r_{\lceil \frac{i}{2} \rceil}\right)} |1\rangle\right) = \left|\bigoplus_{i=2}^{n}\left(x_i^k\right)\right\rangle. \tag{13}$$

P_1 uses Z basis to measure the state and gets $\bigoplus_{i=2}^{n}\left(x_i^k\right)$. Then, he adds his secret x_1^k to the summation and obtains the final result $\bigoplus_{i=1}^{n}\left(x_i^k\right)$.

If $n - 1 \mod 2 = 1$:

For $k = 1, 2, ..., L$:

Except the first particle, P_1 sets others particles to 0 and applies the Hadamard operation to the first particle:

$$H\left(|0\rangle + (-1)^{\bigoplus_{i=2}^{n}\left(x_i^k \oplus r_{\lceil \frac{i}{2} \rceil}\right)} |1\rangle\right) = \left|\bigoplus_{i=2}^{n}\left(x_i^k\right)\right\rangle. \tag{14}$$

P_1 uses Z basis to measure the state and gets $\bigoplus_{i=2}^{n}(x_i^k)$. Then, he adds his secret x_1^k to the summation and obtains the final result $\bigoplus_{i=1}^{n}(x_i^k)$.

The security of the present multi-party quantum summation protocol is the same as the two-party quantum summation protocol. The collusive attack performed by at most $n - 2$ players is invalid for this protocol.

5 Discussion and Conclusions

In summary, we have put forward a novel and efficient quantum protocol to compute secure multiparty summation. In our protocol, we use two-particle Bell states to carry private information. We also use Pauli matrices operations to encode information and Hadamard matrix to extract information. The proposed protocol can also resist various attacks, such as disturbance attack, Trojan horse attack, intercept-resend attack, entanglement-and-measure attack and man-in-the-middle attack. Without using the entanglement swapping of Bell states, our proposed quantum protocol overcomes the problem of information leakage with acceptable efficiency. In theory, our protocol can be generalized to compute lots of secure multiparty numerical computations.

Acknowledgements This paper is supported by the National Natural Science Foundation of China(Grant No.61502437); Beijing Youth Talent Plan(YETP0592); Engineering Course Programming Project of Communication University of China(Grant No.3132014XNG1412,31 32015XNG1524).

References

1. Goldreich, O., Micali, S., Wigderson, A.: How to Play Any Mental Game. ACM, New York (1987)
2. Jia, H.Y., Wen, Q.Y., Song, T.T., Gao, F.: Quantum protocol for millionaire problem. Opt. Commun. **284**, 545–549 (2011)
3. Lin, S., Sun, Y., Liu, X.-F., Yao, Z.-Q.: Quantum private comparison protocol with d-dimensional Bell states. Quantum Inf. Process **12**(1), 559–568 (2013)
4. Zhang, W.W., Li, D., Zhang, K.J., et al.: A quantum protocol for millionaire problem with Bell states. Quantum Inf. Process. **12**, 2241–2249 (2013)
5. Guo, F.Z., Gao, F., Qin, S.J., et al.: Quantum Inf. Process. **12**, 2793 (2013)
6. Zhou, Y.H., Shi, W.M., Yang, Y.G.: A quantum protocol for millionaire problem with continuous variables. Commun. Theor. Phys. **61**, 452–456 (2014)
7. 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)
8. Chen, X.B., Xu, G., Niu, X.X.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. **283**, 1561–1565 (2010)
9. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with w state. Opt. Commun. **284**, 1561–1565 (2011)
10. Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z.: A protocol for the quantum private comparison of equality with chi-type state. Int. J. Theor. Phys. **51**(1), 69–77 (2011)
11. Liu, W., Wang, Y.B.: Quantum private comparison based on GHZ entangled states. Int. J. Theor. Phys. **51**, 3596–3604 (2012)
12. Liu, W., Wang, Y.B., Jiang, Z.T., Cao, Y.Z., Cui, W.: New quantum private comparison protocol using-type state. Int. J. Theor. Phys. **51**(6), 1953–1960 (2012)
13. Liu, W., Wang, Y.B., Tao, J.Z., Cui, W.: Quantum private comparison protocol based on bell entangled states. Commun. Theor. Phys. **57**(4), 583–588 (2012)
14. Liu, W., Wang, Y.B., Wang, X.M.: Quantum multi-party private comparison protocol using d-dimensional bell states. Int. J. Theor. Phys. **54**, 1830–1839 (2015)
15. 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**, 1085–1091 (2014)
16. Liu, W., Wang, Y.B.: Dynamic multi-party quantum private comparison protocol with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **55**, 5307–5317 (2016)
17. Hillery, M., Ziman, M., Buek, V., Bielikov, M.: Phys. Lett. A **349**(1–4), 75 (2006)
18. Du, J.Z., Chen, X.B., Wen, Q.X., Zhu, F.C.: Secure multiparty quantum summation. Acta Phys. Sin-Ch Ed **56**, 6214–6219 (2007)
19. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: An efficient protocol for the secure multi-party quantum summation. Int. J. Theor. Phys. **49**, 2793–2804 (2010)

20. Zhang, C., Sun, Z.-W., Huang, X.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inf. **13**(2), 1550011 (2015)
21. Zhang, C., Sun, Z., Huang, Y.: High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **53**(3), 933–941 (2014)
22. Shi, R.-h., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
23. Jakobi, M., Simon, C., Gisin, N., Bancal, J.D., Branciard, C., Walenta, N., Zbinden, H.: Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A **83**(2), 022301 (2011)
24. Gao, F., Liu, B., Wen, Q.-Y.: Flexible quantum private queries based on quantum key distribution. Opt. Exp. **20**(16), 17411–17420 (2012)
25. Gao, F. et al.: IEEE J. Sel. Top. Quant. **21**, 6600111 (2015)
26. Liu, B., Gao, F., Huang, W., Wen, Q.-Y.: QKD-Based quantum private query without a failure probability. Sci. China Phys. Mech. Astron. **58**, 100301 (2015)
27. Wei, C.Y. et al.: Phys. Rev. A **93**, 042318 (2016)
28. Gao, F., Qin, S.J., Wen, Q.Y., et al.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. **7**, 329 (2007)
29. Qin, S.J., Gao, F., Wen, Q.Y., et al.: Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secretsharing protocol. Phys. Rev. A **76**, 062324 (2007)
30. Lin, S., Gao, F., Guo, F.Z., et al.: Comment on multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A **76**, 036301 (2007)
31. Lin, S., Wen, Q.Y., Gao, F., et al.: Improving the security of multiparty quantum secret sharing based on the improved Bostrom-Felbinger protocol. Opt. Commun. **281**, 4553 (2008)
32. Gao, F., Guo, F.Z., Wen, Q.Y., et al.: Comment on experimental demonstration of a quantum protocol for byzantine agreement and liar detection. Phys. Rev. Lett. **101**, 208901 (2008)
33. Song, T.T., Zhang, J., Gao, F., et al.: Participant attack on quantum secret sharing based on entanglement swapping. Chin. Phys. B **18**, 1333 (2009)
34. Guo, F.Z., Qin, S.J., Gao, F., et al.: Participant attack on a kind of MQSS schemes based on entanglement swapping. Eur. Phys. J. D **56**, 445 (2010)