Int J Theor Phys (2014) 53:933–941
DOI 10.1007/s10773-013-1884-9

High-Capacity Quantum Summation with Single Photons in Both Polarization and Spatial-Mode Degrees of Freedom

Cai Zhang · Zhiwei Sun · Yi Huang · Dongyang Long

Received: 27 April 2013 / Accepted: 18 October 2013 / Published online: 31 October 2013

Abstract In this paper, we employ single photons in both polarization and spatial-mode degrees of freedom to design a quantum summation protocol. We assume that the third party, i.e. TP, is semi-honest in our protocol. That TP is semi-honest means TP executes the protocol loyally, keeps a record of all its intermediate computations and might try to steal the participants' private inputs from the record, but he cannot be corrupted by the adversary. Participants can independently encode their private inputs on the polarization states and the spatial-mode states of single photons. Thus our protocol doubles the capacity of quantum communication compared with those based on single photons with only one degree of freedom. In addition, our protocol is feasible as the preparation and the measurement of single-photon quantum states in both the polarization and the spatial-mode degrees of freedom are available with current quantum techniques. We also analyze its security in this paper.

Keywords Quantum summation · Two degrees of freedom · Single photons · High-capacity

1 Introduction

Secure multi-party computation, first introduced in [1], is a subfield of cryptography and has been a significant and fruitful research area in recent years [2–4]. The principles in quantum mechanics provide good ways for quantum information processing. Thus quantum states can be used to deal with classical secure multi-party computation problems. Many researchers

C. Zhang (✉) · Z. Sun · D. Long
School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China
e-mail: zhangcai.sysu@gmail.com

Y. Huang
Key Laboratory of Pattern Recognition and Intelligent Information Processing, Institutions of Higher Education of Sichuan Province, Chengdu University, Chengdu 610106, China

Y. Huang
School of Information Science and Technology, Chengdu University, Chengdu 610106, China

have investigated secure multi-party computation in quantum settings [5–7]. Using quantum resources, Chau [8] presented a scheme for speeding up classical multi-party computation. In 2001, Smith [9] established that any multi-party quantum computation could be secure as long as the number of dishonest players is less than $n/6$. In 2006, Ben-Or et al. [7] studied how much trust is necessary, that is, in order for distributed quantum computations to be securely performed, how many players must remain honest.

Secure multi-party summation is a special case in secure multi-party computation and it can be described as follows: n participants $(P_1, P_2, \ldots, P_n)$ wish to compute a summation function $F(x_1, x_2, \ldots, x_n)$, where x_i is a private input offered by P_i. The result of the function F could be shown in public or privately to some particular participants. The goal of secure multi-party computation is to preserve the privacy of each participant's input and ensure the correctness of the computation. Heinrich [10, 11] investigated summation of sequences in the quantum model of computation. In 2003, Heinrich et al. [12] researched the quantum Boolean summation with repetitions in the Worst-Average Setting. Du et al. [13] presented a protocol for secure quantum addition module $n + 1$ $(n \geq 2)$ using nonorthogonal single particle states, allowing a number to be secretly added to an unknown number. In 2006, Hillery et al. [14] proposed a multi-party summation protocol with the two-particle N-level entangled states in which the summation of N players in voting procedure is performed, and the anonymity of the players can be guaranteed. In 2010, Chen et al. [15] presented a quantum summation protocol with the multi-particle entangled GHZ states.

The first quantum communication protocol based on photon systems in both the polarization and the spatial degrees of freedom was proposed by Wang [16]. Subsequently, these photon systems with two DOFs are employed for other tasks of quantum communication, including quantum secret sharing [17, 18] and quantum secure direct communication [19–21]. In 2013, Liu et al. [17] presented a high-capacity quantum secret sharing protocol with hyperentangled photon pairs and Wang et al. [18] put forward a high-capacity three-party quantum secret sharing protocol with single photons in both the polarization and the spatial-mode degrees of freedom. In 2011, Gu et al. proposed a bidirectional quantum secure direct communication network protocol with hyperentanglement [20] and studied a two-step quantum secure direct communication protocol with hyperentanglement [19]. In 2012, Liu et al. [21] presented a high-capacity quantum secure direct communication protocol with single photons in both polarization and spatial-mode degrees of freedom.

All the previous quantum summation protocols work with single degree of freedom and the capacity of quantum summation protocols can be improved if other degrees of freedom of photons are considered. In this paper, we present a quantum summation protocol with single photons in both the polarization and the spatial-mode degrees of freedom. Participants can independently encode their private inputs on the polarization states and the spatial-mode states of single photons. Thus our protocol doubles the capacity of quantum communication compared with those based on single photons with only one degree of freedom. In addition, our protocol is feasible as the preparation and the measurement of single-photon quantum states in both the polarization and the spatial-mode degrees of freedom are available with current quantum techniques. We also analyze its security in this paper.

2 Two-Party Quantum Summation Protocol

We can describe a single-photon state in both the polarization and the spatial-mode degrees of freedom as follows.

$$|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S \tag{1}$$

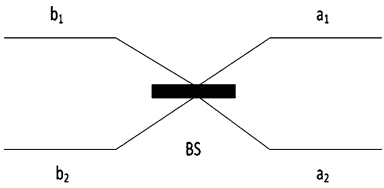

Fig. 1 Scheme diagram of a Hadamard operation in the spatial degree of freedom with a 50:50 beam splitter (BS)

where $|\phi\rangle_P$ and $|\phi\rangle_S$ are the single-photon states in the polarization and the spatial-mode degrees of freedom, respectively. We choose two nonorthogonal measuring bases in the polarization degree of freedom as $Z_P = \{|H\rangle, |V\rangle\}$ and $X_P = \{|S\rangle_P, |A\rangle_P\}$, respectively. Here

$$\begin{aligned} |S\rangle_P &= \frac{1}{\sqrt{2}}\big(|H\rangle + |V\rangle\big) \\ |A\rangle_P &= \frac{1}{\sqrt{2}}\big(|H\rangle - |V\rangle\big) \end{aligned} \tag{2}$$

where H and V denote the horizontal and vertical polarizations of single photons, respectively. We can also choose two nonorthogonal measuring bases in the spatial-mode degree of freedom as $Z_S = \{|a_1\rangle, |a_2\rangle\}$ and $X_S = \{|s\rangle_S, |a\rangle_S\}$, respectively. Here

$$\begin{aligned} |s\rangle_S &= \frac{1}{\sqrt{2}}\big(|a_1\rangle + |a_2\rangle\big) \\ |a\rangle_S &= \frac{1}{\sqrt{2}}\big(|a_1\rangle - |a_2\rangle\big) \end{aligned} \tag{3}$$

where a_1 and a_2 represent the upper spatial mode and the lower spatial mode of single photons, respectively. The quantum state $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$ can be in principle generated with a beam splitter (BS: 50/50): the participants first prepare a sequence of single-photon polarization states $|\phi\rangle_P$, and then use a BS or not on each photon to produce the spatial-mode states $|\phi\rangle_S$, as shown in Fig. 1. What the BS does is to complete the transformations as follows.

$$\begin{aligned} |b_1\rangle &\to \frac{1}{\sqrt{2}}\big(|a_1\rangle + |a_2\rangle\big), \\ |b_2\rangle &\to \frac{1}{\sqrt{2}}\big(|a_1\rangle - |a_2\rangle\big). \end{aligned} \tag{4}$$

Similar to Refs. [22, 23], there are two interesting unitary operations in each degree of freedom of single photons, with which the basis of each single photon will not be changed. These unitary operations are

$$\begin{aligned} I_P &= |H\rangle\langle H| + |V\rangle\langle V|, \\ U_P &= |V\rangle\langle H| - |H\rangle\langle V|, \\ I_S &= |a_1\rangle\langle a_1| + |a_2\rangle\langle a_2|, \\ U_S &= |a_2\rangle\langle a_1| - |a_1\rangle\langle a_2|. \end{aligned} \tag{5}$$

From the above unitary operations, we can see that

$$\begin{aligned} &U_P|H\rangle = |V\rangle, \qquad U_S|a_1\rangle = |a_2\rangle, \\ &U_P|V\rangle = -|H\rangle, \qquad U_S|a_2\rangle = -|a_1\rangle, \\ &U_P|S\rangle_P = -|A\rangle_P, \qquad U_S|s\rangle_S = -|a\rangle_S, \\ &U_P|A\rangle_P = |S\rangle_P, \qquad U_S|a\rangle_S = |s\rangle_S. \end{aligned} \tag{6}$$

We will use these good properties to design our quantum summation protocol, in which TP obtains the final result without the knowledge of the participants' private secret bit strings. In this section, we present the two-party quantum summation protocol, and then analyze its security against outside and participant attacks. It will be generalized to n-party quantum summation protocol in Sect. 3.

In advance, all participants agree on the following encoding:

$$I_P(I_S) \to 0; \qquad U_P(U_S) \to 1. \tag{7}$$

For example, if a private input (bit string) of a participant is 10, the unitary operation $U_P \otimes I_S$ will be performed on the state $|\phi\rangle$ produced by TP.

2.1 The Process of Two-Party Quantum Summation Protocol

We assume that TP in our protocol is semi-honest [24]. That TP is semi-honest means TP executes the protocol loyally, keeps a record of all its intermediate computations and might try to steal the participants' private inputs from the record, but he cannot be corrupted by the adversary. Suppose that two participants P_1 and P_2 have secret bit strings K_1 and K_2, respectively. They wish TP to compute the summation $K_1 \oplus K_2$. Here, $\oplus$ denotes the addition module 2.

$$\begin{aligned} K_1 &= (k_{1L}, k_{1(L-1)}, \ldots, k_{11}) \\ K_2 &= (k_{2L}, k_{2(L-1)}, \ldots, k_{21}) \\ K_1 \oplus K_2 &= (k_{1L} \oplus k_{2L}, k_{1(L-1)} \oplus k_{2(L-1)}, \ldots, k_{11} \oplus k_{21}) \end{aligned} \tag{8}$$

where L represents the length of secret bit strings.

We use the method similar to [25] to design our protocol. The quantum summation protocol can be described as follows.

(S1) TP prepares a sequence of ordered $\lceil \frac{L}{2} \rceil$ ($\lceil\ \rceil$ denotes the ceiling function) single photons R. Each single photon is in one of the 16 quantum states $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$. Here $|\phi\rangle_P \in \{|H\rangle, |V\rangle, |S\rangle_P, |A\rangle_P\}$ and $|\phi\rangle_S \in \{|a_1\rangle, |a_2\rangle, |s\rangle_S, |a\rangle_S\}$. TP keeps the sequence R secret.

We exploit the decoy-photon technique [26, 27] for preventing the eavesdropping. TP prepares d decoy single photons, the same as above, each of which is in one of the 16 quantum states $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$. TP then randomly inserts the d decoy single photons into the sequence R to form a new one R^1. Note that anyone does not know the initial states and the positions of the d decoy single photons except TP. At last, TP transmits R^1 to P_1.

(S2) Confirm that P_1 have received all the single photons sent by TP. TP announces the positions of the decoy single photons, but keeps the initial states secret. In the following, P_1 measures the decoy single photons with one of the four bases $Z_P \otimes Z_S$,

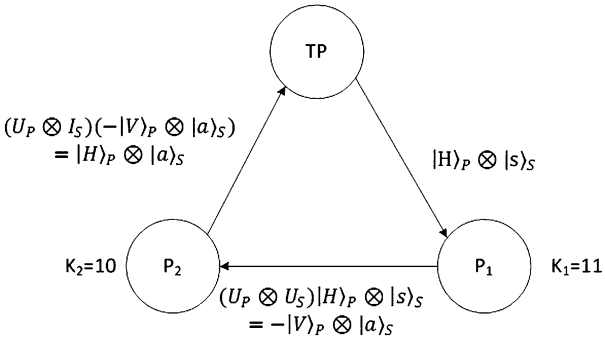

Fig. 2 The process of two-party quantum summation. Suppose that P_1 and P_2 have the secret bit strings $K_1 = 11$ and $K_2 = 10$, respectively. They wish TP to compute the summation $K_1 \oplus K_2$. At first TP is assumed to produce the single-photon state $|H\rangle_P \otimes |s\rangle_S$. Then P_1 and P_2 perform unitary operations on the state according to their secret bit strings, respectively. Finally, TP measures the operated single-photon state with the appropriate basis $Z_P \otimes X_S$ and obtains the summation result 01 by comparing the measurement result and the initial state, but he can not infer any participant's secret bit string from the summation result. During the communication, decoy single photons are used to check eavesdropping, which are omitted here

$Z_P \otimes X_S$, $X_P \otimes Z_S$, $X_P \otimes X_S$ randomly. Then P_1 publishes his measurement results. Later, TP can determine the error rate according to the initial states of the d decoy single photons. If the error rate exceeds the threshold, then this protocol will be aborted and repeat the step (S1). Otherwise, the protocol will go to the next step.

(S3) P_2 removes the decoy single photons and performs operations $U_P^1 \otimes U_S^2$ ($U_P^1 \in \{I_P, U_P\}$ and $U_S^2 \in \{I_S, U_S\}$) on each single photon of the ordered sequence R according to his secret bit string. To prevent eavesdropping, similar to TP, P_1 also prepares d decoy single photons, each of which is in one of the 16 quantum states $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$. Then he randomly inserts them into the sequence R to form a new one denoted by R^2. Finally P_1 sends R^2 to P_2.

(S4) Confirm that P_2 have received all the single photons sent by P_1. They use the same method as TP and P_1 to check whether the transmission is secure or not according to the threshold. If the transmission is not secure, they abort the communication and repeat the step (S1). Otherwise, the protocol will go to the next step.

(S5) In this step, P_2 does the similar work to that of P_1 according to his secret bit string. Finally P_2 sends the sequence R^3 back to TP.

(S6) TP and P_2 check whether or not the transmission is secure using the method as before. If the transmission is secure, TP will obtain the summation result. However he cannot get the secret bit string of each participant. Otherwise, they will abort the communication and repeat the step (S1).

Figure 2 shows our main idea of the protocol. Of course, the length of the bit strings may be odd. In this case, TP and the participants just agree on that the polarization of the last single photon can be neglected.

2.2 Security Analysis of Two-Party Quantum Summation

In this section, the security of our protocol will be analyzed. In general, the security analysis of quantum summation protocol is more complex than quantum key distribution (QKD) [28–33], quantum secure direct communication (QSDC) [22, 34–40] and quantum secret sharing (QSS) [41–50] because the attacks from all participants have to be considered in

quantum summation protocols. In the QKD and QSDC protocols, all participants are usually assumed to be honest. In QSS protocol, the distributor of the secret is assumed to be honest, but the other participants can be dishonest. In quantum summation protocol, the attacks from all participants (TP and other participants) should be considered. Thus the security analysis of quantum summation protocol will be more complicated. Outside eavesdroppers wish to steal the participants' secret bit strings. In addition, some participants may try to derive other participants' private secret information. Therefore, the security goal of quantum summation protocol is to prevent outside and participant attacks.

1. Outside Attacks
   In our protocol, TP and all participants use decoy single photons to prevent eavesdropping. This idea is derived from the BB84 QKD protocol [28]. And it has been proven to be unconditionally secure by researchers [51]. As we know, BB84 protocol remains secure even if the quantum channel is noisy, and thus our protocol can also work on the noisy channels. Any eavesdropping will be discovered in the detection stage. Thus outside Eve's several sorts of attacks, such as the intercept-resend attack, the measurement-resend attack, the entanglement-measurement attack and the denial-of-service (DOS) attack, will be caught during the detection stage. We take the intercept-resend attack as an example here: suppose that the initial decoy single-photon state is $|H\rangle_P \otimes |s\rangle_S$, and Eve randomly measures it with one of the four bases $Z_P \otimes Z_S$, $Z_P \otimes X_S$, $X_P \otimes Z_S$, $X_P \otimes X_S$, and then she sends the fake single photon prepared by herself based on the measurement outcomes to the receiver. Obviously, the probability of being discovered during the eavesdropping detection stage is $\frac{7}{16}$. When we use d decoy single photons for eavesdropping, the probability of being discovered will be $1-(\frac{9}{16})^{\frac{1}{4}d}$. Therefore, Eve will be detected in the eavesdropping detection stage.

   In two-way quantum communication, there exists Trojan horse attack [52–54], such as the delay-photon Trojan horse attack and the invisible photon eavesdropping (IPE) Trojan horse attack. In our protocol, because the communication between the sender (TP, participants) and the receiver (TP, participants) is one-way, Trojan horse attack has no impact on it. That is, our protocol can defeat such an attack.

   In addition, because the sequence of the initial single photons R prepared by TP is kept secret, the single photons employed to establish the quantum channel carry no secret messages, and Eve can not get any useful information in the detection stage.
2. Participant Attack: One of the two participants wants to steal the other's secret bit string
   We can assume that P_1 wishes to steal P_2's secret bit string because the role of P_1 is the same as P_2. In order to do that, P_1 has to catch the single photons sent from P_2 to TP, and then measures the sequence of single photons R with correct basis. However, TP keeps this sequence R secret all the time. Any measurements will be discovered in the detection stage, because P_1 has no knowledge of the positions and the initial states of decoy single photons in the sequence.
3. Participant Attack: The semi-honest wants to steal the participants' secret bit strings
   In our protocol, we assume that TP is semi-honest which means that it is required to loyally execute the protocol, and cannot cooperate with P_1 or P_2. The attack of TP is that he records all his intermediate computations and might try to derive the participants' private secret bit strings from the record. In this condition, TP can guess the partial secret bit strings provided by participants. However, he fails to obtain all the secret bit strings. In our protocol, we guarantee that TP cannot determinately steal all secret bit strings K_1 and K_2. Clearly, TP finally gets the summation result $r = k_1 \oplus k_2$. That is, TP only knows if the bit $k_1 = k_2$ or not. For instance, if TP knows that $k_1 = k_2$, he cannot determinately know $k_1 = k_2 = 0$ or $k_1 = k_2 = 1$.

3 Protocol of Multi-Party Quantum Summation

With current quantum techniques, single-photon states in both the polarization and the spatial-mode degrees of freedom are available. Following the basic idea from the two-party quantum summation protocol, we can easily design an n-party ($n > 2$) quantum summation protocol.

Like the two-party quantum summation protocol, TP and n participants agree on the encoding operations in (7). Suppose that the j-th participant has the secret bit string K_j ($j = 1, 2, \ldots, n$), TP prepares the sequence of single photons R and computes the summation $\oplus \sum_{j=1}^{n} K_j$. Here, $\oplus \sum$ represents the additions module 2. The process of the n-party quantum summation protocol is as follows.

(S1) TP prepares a sequence of ordered $\lceil \frac{L}{2} \rceil$ ($\lceil$ denotes the ceiling function) single photons R. Each single photon is in one of the 16 quantum states $|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$. Here $|\phi\rangle_P \in \{|H\rangle, |V\rangle, |S\rangle_P, |A\rangle_P\}$ and $|\phi\rangle_S \in \{|a_1\rangle, |a_2\rangle, |s\rangle_S, |a\rangle_S\}$. TP keeps the sequence R secret. Like the Two-party quantum summation protocol, TP inserts decoy single photons into the sequence R to form a new one denoted by R^1. And then he sends R^1 to P_1.

(S2) For $i = 1, 2, \ldots, n-1$
{
P_i checks if the transmission is secure using decoy single-photon technique. If the transmission is secure, he removes the decoy single photons and performs unitary operations on the sequence R depending on his secret bit string. He then inserts decoy single photons into this operated R to form a new one denoted by R^{i+1} and sends it to P_{i+1}. The positions and initial states of the decoy single photons are kept secret. Otherwise, they abort the protocol and repeat step (S1). This procedure will continue until $i = n-1$.
}

(S3) P_n checks if the transmission is secure using decoy single-photon technique as before. If the transmission is secure, he removes the decoy single photons and performs unitary operations on the sequence R in the light of his secret bit string. Then he inserts decoy single photons into this operated R to form a new one denoted by R^{n+1} and sends it to TP. The positions and initial states of the decoy single photons are kept secret. Otherwise, they abort the protocol and repeat step (S1).

(S4) TP checks whether or not the transmission is secure using the method as before. If the transmission is secure, TP will obtain the summation result, but he cannot get the secret bit string of each participant. Otherwise, they will abort the communication and repeat the step (S1).

The security of the multi-party quantum summation protocol is the same as that of the two-party quantum summation protocol, because we also use the decoy single-photon technique for eavesdropping detection.

4 Conclusions

In this paper, we present a quantum summation protocol using single photons in both polarization and spatial-mode degrees of freedom. As the preparation and the measurement of single-photon quantum states in both the polarization and the spatial degrees of freedom are available with current quantum techniques, our protocol is feasible. In addition, our protocol doubles the capacity of quantum communication compared with those based on single photons in only one degree of freedom.

Acknowledgements This work is supported by the National Natural Science Foundation of China under Grants No. 61272013.

References

1. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. In: Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, p. 218. ACM, New York (1987)
2. Sheikh, R., Kumar, B., Mishra, D.K.: arXiv:1003.4071 (2010)
3. Prabhakaran, M.M., Sahai, A.: Secure Multi-Party Computation. IOS Press, Amsterdam (2013)
4. Boyle, E., Goldwasser, S., Tessaro, S.: Communication locality in secure multi-party computation. In: Theory of Cryptography, p. 356. Springer, Berlin (2013)
5. Lo, H.K.: Phys. Rev. A **56**, 1154 (1997)
6. Crépeau, C., Gottesman, D., Smith, A.: In: Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing, pp. 643–652. ACM, New York (2002)
7. Ben-Or, M., Crepeau, C., Gottesman, D., Hassidim, A., Smith, A.: In: 47th Annual IEEE Symposium on Foundations of Computer Science. FOCS'06, pp. 249–260. IEEE, New York (2006)
8. Chau, H.F.: Phys. Rev. A **61**, 032308 (2000)
9. Smith, A.: arXiv:quant-ph/0111030 (2010)
10. Heinrich, S.: J. Complex. **18**(1), 1 (2002)
11. Heinrich, S., Novak, E.: J. Complex. **19**(1), 1 (2003)
12. Heinrich, S., Kwas, M., Wozniakowski, H.: arXiv:quant-ph/0311036 (2003)
13. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Acta Phys. Sin. **56**(11), 6214 (2007)
14. Hillery, M., Ziman, M., Bužek, V., Bieliková, M.: Phys. Lett. A **349**(1–4), 75 (2006)
15. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: Int. J. Theor. Phys. **49**(11), 2793 (2010)
16. Wang, T.J., Li, T., Du, F.F., Deng, F.G.: Chin. Phys. Lett. **28**, 040305 (2011)
17. Liu, D., Zong, Z.C., Ma, W.: Int. J. Theor. Phys. **52**, 2245 (2013)
18. Wang, H., Huang, Y., Fang, X., Gu, B., Fu, D.: Int. J. Theor. Phys. **52**(4), 1043 (2013)
19. Gu, B., Huang, Y.G., Fang, X., Chen, Y.L.: Commun. Theor. Phys. **56**(4), 659 (2011)
20. Gu, B., Huang, Y.G., Fang, X., Zhang, C.Y.: Chin. Phys. B **20**(10), 100309 (2011)
21. Liu, D., Chen, J.L., Jiang, W.: Int. J. Theor. Phys. **51**(9), 2923 (2012)
22. Deng, F.G., Long, G.L.: Phys. Rev. A **69**, 052319 (2004)
23. Deng, F.G., Long, G.L.: Phys. Rev. A **70**, 012311 (2004)
24. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.X.: Opt. Commun. **283**(7), 1561 (2010)
25. Sun, Z., Zhang, C., Wang, B., Li, Q., Long, D.: Quantum Inf. Process. **12**, 3411 (2013)
26. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Chin. Phys. Lett. **22**(5), 1049 (2005)
27. Li, C.Y., Li, X.H., Deng, F.G., Zhou, P., Liang, Y.J., Zhou, H.Y.: Chin. Phys. Lett. **23**(11), 2896 (2006)
28. Bennett, C.H., Brassard, G.: Quantum cryptography: Public-key distribution and coin tossing. In: IEEE International Conference on Computer, System and Signal, p. 175. IEEE, New York (1984)
29. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
30. Bennett, C.H.: Phys. Rev. Lett. **68**, 3121 (1992)
31. Bennett, C.H., Brassard, G., Mermin, N.D.: Phys. Rev. Lett. **68**, 557 (1992)
32. Deng, F.G., Long, G.L.: Phys. Rev. A **68**, 042315 (2003)
33. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A **78**, 022321 (2008)
34. Long, G.L., Liu, X.S.: Phys. Rev. A **65**, 032302 (2002)
35. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**(4), 042317 (2003)
36. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Phys. Rev. A **71**, 044305 (2005)
37. Li, X.H., Li, C.Y., Deng, F.G., Zhou, P., Liang, Y.J., Zhou, H.Y.: Chin. Phys. B **16**(8), 2149 (2007)
38. Shi, J., Gong, Y.X., Xu, P., Zhu, S.N., Zhan, Y.B.: Commun. Theor. Phys. **56**(5), 831 (2011)
39. Sun, Z.W., Du, R.G., Long, D.Y.: Int. J. Theor. Phys. **51**(6), 1946 (2012)
40. Ren, B.C., Wei, H.R., Hua, M., Li, T., Deng, F.G.: Eur. Phys. J. D **67**(2), 1 (2013)
41. Hillery, M., Buzek, V., Berthiaume, A.: Phys. Rev. A **59**(3), 1829 (1999)
42. Karlsson, A., Koashi, M., Imoto, N.: Phys. Rev. A **59**, 162 (1999)
43. Cleve, R., Gottesman, D., Lo, H.K.: Phys. Rev. Lett. **83**, 648 (1999)
44. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Phys. Rev. A **69**, 052307 (2004)
45. Zhang, Z.J., Li, Y., Man, Z.X.: Phys. Rev. A **71**, 044301 (2005)
46. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Eur. Phys. J. D **39**(3), 459 (2006)
47. Deng, F.G., Li, X.H., Zhou, H.Y.: Phys. Lett. A **372**(12), 1957 (2008)
48. Chen, X.B., Niu, X.X., Zhou, X.J., Yang, Y.X.: Quant. Inf. Process. **12**, 365 (2013)
49. Chen, X.B., Yang, S., Xu, G., Su, Y., Yang, Y.X.: Int. J. Quantum Inf. **11**(01), 1350010 (2013)

50. Chen, X.B., Yang, S., Su, Y., Yang, Y.X.: Phys. Scr. T **86**(5), 055002 (2012)
51. Shor, P.W., Preskill, J.: Phys. Rev. Lett. **85**, 441 (2000)
52. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Phys. Rev. A **72**, 044302 (2005)
53. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Phys. Rev. A **73**, 022320 (2006)
54. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A **74**, 054302 (2006)