Int J Theor Phys (2016) 55:55–61
DOI 10.1007/s10773-015-2632-0

Participant Attack on Three-party Quantum key Agreement with Two-photon Entanglement

Zhen-Chao Zhu[1] · Ai-Qun Hu[1] · An-Min Fu[2,3]

Received: 27 October 2014 / Accepted: 27 March 2015 / Published online: 15 April 2015

Abstract In a recent study (Yin et al. Int. J. Theor. Phys. **52**, 3915-3921, 2013), Yin et al. proposed a three-party quantum key agreement protocol based on two-qubit entangled states, they claimed that the protocol could resist against the insider attack and each party in the protocol had an equal contribution to the establishment of the final shared secret key. However, in this study, we will show that the protocol is not secure, two dishonest participants can conclude to determine the shared key alone. To avoid this flaw, a further improved protocol is proposed.

Keywords Quantum key agreement · Two-qubit entangled states · Participant attack

How to establish a security key is an important critical issue in cryptography, early cryptologists usually assumed that there was a secure channel, the key could be exchanged through in this channel. However, this assumption becomes unmanageable when the number of participants increases greatly, or when secure channel is not available. To get rid of this awkward problem, in 1976, Diffie and Hellman introduced a kind of protocol [1], key agreement (KA) protocol. In a KA protocol, each party can contribute fairly her/his part to establish a shared secret key over an insecure public channel. Although the protocol [1] was later proven vulnerable to Man -in-Middle attack as it does not provide authentication of the communicating parties, the design philosophy of the protocol had fundamentally changed

✉ Zhen-Chao Zhu
zhuzc@seu.edu.cn

[1] Information Security Research Center, Southeast University, Nanjing 210096, China

[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

[3] School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China

the way cryptosystems might work. Since then, many researches have been focused on designing new KA protocols or formalizing the security model for KA protocols [2–10].

However, the securities of the proposed protocols above are often designed based on trapdoor functions. Cryptologists often suppose that it is easy to compute trapdoor function f(x) given the variable x but impossible to deduce x from f(x) without the trapdoor. However, so far, no one has proved the existence of any one-way function with a trapdoor. In other words, all the KA protocols above rely for their security on unproven mathematical assumptions, e.g. solving the discrete logarithm problem or factoring large numbers are difficult. In addition, the discovery in 1994 by Shor for fast factorization of integers [11] with a polynomial algorithm in a quantum computer and the discovery in 1996 by Grover for searching an unsorted database [12] with N entries in $O(N^{1/2})$ time and using O(log N) storage space in the linear quantum model cast more doubts on the existence of the trapdoor functions. The security of these KA protocols face serious challenges, how to design KA protocols which do not rely for their securities on unproven mathematical assumptions becomes urgent. Fortunately, in 2004, a new type of KA, quantum KA (QKA), was proposed by Zhou et al. [13], the protocol uses quantum teleportation and maximally entangled states to generate secret key over public channels, the security of the protocol is guaranteed by the principle of quantum mechanics. However, the study [14] showed that Zhou et al.'s protocol was not secure. In 2010, Chong et al. presented a QKA protocol [15] based on BB84 protocol [16]. In 2013, a multi-party QKA protocol, an extension of two-party QKA protocol [17], was proposed by Shi et al. However, Liu et al. pointed out that Shi et al.'s protocol was not secure, then they proposed a new multi-party QKA protocol using single particles [18]. Sun et al. gave an improvement to Liu et al.'s protocol by introducing two additional unitary operations [19], they claimed that the efficiency of the protocol could be raised for (N-1) times, where, N is the number of the participants in the protocol. Furthermore, they claimed that the improved protocol can overcome the privacy leakage problem existed in Liu et al.'s protocol. However, the study [20] showed that any participant's sub-key still could be deduced by other two participants next to him/her in Sun et al.'s improved protocol. Yin et al. proposed a three-party QKA protocol based on two-qubit entangled states [21], they claimed that each party in the protocol has an equal contribution to the establishment of the final shared secret key and the protocol can resist against both the outsider attack and the insider attack. In 2014, Shukla et al. proposed two QKA protocols based on Bell state and Bell measurement [22]. Huang et al. presented a QKA protocol with the block transmission of EPR pairs [23]. To solve the problem that QKA protocols cannot be immune to decoherence, Huang et al. proposed another QKA protocol [24] based on BB84 protocol. Recently, Xu et al. presented another three-party QKA protocol based on GHZ (Greenberger -Horne-Zeilinger) states [25].

Through analyzing the above introduction, we can see that QKA is being a new research hotspot in cryptography, more and more protocols were proposed. However, the cryptanalysis of QKA protocol has not drawn enough attention. As that described by Gao et al. in [26], cryptanalysis plays an important role in the development of cryptography, it estimates a protocol's security level, finds potential loopholes, and tries to overcome security issues. In the study of quantum cryptography, quite a few effective attack strategies have been proposed, such as entanglement-swapping attacks [27], channel-loss attacks [28], denial-of-service attacks [29], Trojan horse attacks [30], participant attacks [31] and so on. Understanding those attacks will be helpful for us to design new schemes with high security. In these kinds of attacks, we should pay more attention to the participant attacks. In contrast to an outside attacker, an inside participant, especially in a multi-party quantum cryptography protocol, usually has more power to attack the protocol for her/his participant identity. Later studies

showed that quite a number of quantum cryptographic protocols could not resist participant attacks [32–37].

In this paper, we will show that Yin et al.'s protocol [21] is not secure against participant attack. Through launching a special kind of attack, two dishonest participants can totally offset the third participant's role in the generation of the final key, they can determine the final shared key alone. To avoid the flaw, a further improved protocol is proposed. To maintain the integrity of the paper, let us give a brief review of the Yin protocol which is composed of the following 7 steps.

Step 1 Participant Alice (Bob, Charlie) generates a random string K_A (K_B, K_C), where, $K_J = \{j_1, ...j_n\}, J \in \{A, B, C\}, j \in \{a, b, c\}, a_i, b_i, c_i \in \{0, 1\}, i = 1, ...n$. In the meanwhile, Alice (Bob, Charlie) prepares n EPR pairs $\left|\psi^+\right\rangle_{A_1A_2}$ $\left(\left|\psi^+\right\rangle_{B_1B_2}, \left|\psi^+\right\rangle_{C_1C_2}\right)$ and then takes the first and the second particle from each pair to form sequences $S_{A_1}\left(S_{B_1}, S_{C_1}\right)$ and $S_{A_2}\left(S_{B_2}, S_{C_2}\right)$ respectively, where, $\left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. To check the security of the transmission, each participant prepares enough decoy photons which are randomly chosen from Z-basis $\{|0\rangle, |1\rangle\}$ or X-basis $\{|+\rangle, |-\rangle\}$ and then randomly inserts them into $S_{A_2}\left(S_{B_2}, S_{C_2}\right)$. Alice (Bob, Charlie) sends the mixed sequence $S_{A_2}\left(S_{B_2}, S_{C_2}\right)$ to Bob (Charlie, Alice).

Step 2 After having been confirmed that Bob (Charlie, Alice) has received the sequence $S_{A_2}\left(S_{B_2}, S_{C_2}\right)$, Alice (Bob, Charlie) announces the position and the basis of each decoy particle. Bob (Charlie, Alice) and Alice (Bob, Charlie) check the security of the channel. If the error rate exceeds the threshold, they restart the protocol.

Step 3 Bob (Charlie, Alice) picks out the decoy particles from the sequence $S_{A_2}\left(S_{B_2}, S_{C_2}\right)$ and then performs unitary operation $U_{b_i}\left(U_{c_i}, U_{a_i}\right)$ (i= 1,2,...,n) on the rest particles to form sequence $S^1_{A_2}\left(S^1_{B_2}, S^1_{C_2}\right)$, where,$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, U_1 = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$. In the meanwhile, Bob (Charlie, Alice) prepares enough decoy photons and then randomly inserts them into $S^1_{A_2}\left(S^1_{B_2}, S^1_{C_2}\right)$. Bob (Charlie, Alice) sends the mixed sequence $S^1_{A_2}\left(S^1_{B_2}, S^1_{C_2}\right)$ to Charlie (Alice, Bob).

Step 4 After having been confirmed that Charlie (Alice, Bob) has received the sequence $S^1_{A_2}\left(S^1_{B_2}, S^1_{C_2}\right)$, Bob and Charlie (Charlie and Alice, Alice and Bob) perform the second eavesdropping check. If the error rate exceeds the threshold, two parties abort this protocol.

Step 5 Charlie (Alice, Bob) first picks out decoy photons from the sequence $S^1_{A_2}\left(S^1_{B_2}, S^1_{C_2}\right)$ and then performs unitary operation $U_{2c_i}\left(U_{2a_i}, U_{2b_i}\right)$ (i= 1,2,...,n) on the rest particles to form sequence $S^2_{A_2}\left(S^2_{B_2}, S^2_{C_2}\right)$, where, $U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_2 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$. In the meanwhile, Charlie (Alice, Bob) prepares enough decoy photons and then randomly inserts them into $S^2_{A_2}\left(S^2_{B_2}, S^2_{C_2}\right)$. Charlie (Alice, Bob) sends the sequence to Alice (Bob, Charlie).

Step 6 After having been confirmed that Alice (Bob, Charlie) has received the sequence $S^2_{A_2}\left(S^2_{B_2}, S^2_{C_2}\right)$, two parties perform the third security check. If they confirm that the transmission is insecure, this process is aborted.

Step 7 Alice (Bob, Charlie) picks out the decoy particles from the sequence $S^2_{A_2}\left(S^2_{B_2}, S^2_{C_2}\right)$ and then performs Bell-state measurement on the corresponding particles in sequences $S_{A_1}\left(S_{B_1}, S_{C_1}\right)$ and $S^2_{A_2}\left(S^2_{B_2}, S^2_{C_2}\right)$. According to the measurement results, each party can obtain the other two parties' secret keys. Thus they can determine the final shared secret key $K = K_A \oplus K_B \oplus K_C$.

As that pointed out by Sun et al. in [19], one principle in the design of QKA protocol is that the protocol should have fairness property, that is, all involved participants are equally to influence the final shared key. In other words, no non-trivial subset of the participants can determine the shared key. Yin et al. claimed that each participant in their proposed protocol has an equal contribution to the establishment of the shared secret key and three participants are entirely peer entities [21]. However, we will show that two dishonest participants in Yin et al.'s protocol can conclude to determine the shared key alone, in the next, we will show how two dishonest participants can do this. Without loss of generality, we suppose that Alice and Bob are two dishonest participants. In step 3, Alice and Bob can disguised as legitimate participants to perform unitary operation on the corresponding particles. In step 5, it is obviously that Alice and Bob can deduce Charlie's unitary operations though measuring the particle pairs in which one particle has been performed unitary operation by Charlie. Then Bob can choose different unitary operations to perform on the particles and then send these particles to the honest participant Charlie. The role of the honest participant in the generation of the final key can be totally offset by this different unitary operations, the final key will be only determined by these two dishonest participants, so the protocol is not secure against the participant attack. In the next, we give the details of our proposed attack. In step 3, Bob (Charlie, Alice) first picks out the decoy photons and then performs unitary operation $U_{b_i}\left(U_{c_i}, U_{a_i}\right)$ on the rest particles in the sequence $S_{A_2}\left(S_{B_2}, S_{C_2}\right)$ to form sequence $S^1_{A_2}\left(S^1_{B_2}, S^1_{C_2}\right)$. Bob (Charlie, Alice) prepares enough decoy photons and then randomly inserts them into the sequence $S^1_{A_2}\left(S^1_{B_2}, S^1_{C_2}\right)$. Bob (Charlie, Alice) sends the mixed sequence $S^1_{A_2}\left(S^1_{B_2}, S^1_{C_2}\right)$ to Charlie (Alice, Bob). After checking the security of the quantum transmitting, Bob can deduce Charlie's unitary operation with the help of Alice through performing Bell-state measuring on the corresponding particles in sequences S_{B_1} and $S^1_{B_2}$. For example, if Bob and Alice get result $\left|\psi^+\right\rangle$, they can deduce that Charlie's unitary operation is U_0, which means that the corresponding bit of Charlie's sub key is 0. If Bob and Alice get result $\left|\phi^+\right\rangle$, they can deduce that Charlie's unitary operation is U_1, which means that the corresponding bit of Charlie's sub key is 1. After the Step 4 having been completed, Bob holds sequences S_{B_1} and $S^1_{C_2}$, Alice holds sequences S_{A_1} and $S^1_{B_2}$. If all the parties are honest, in the next, Bob will perform unitary operation U_{2b_i} on the corresponding particle in the sequence $S^1_{C_2}$ to form sequence $S^2_{C_2}$ and then send the sequence to Charlie, Alice will perform unitary operation U_{2a_i} on the corresponding particle in the sequence $S^1_{B_2}$ to form sequence $S^2_{B_2}$ and then send the sequence to Bob, Charlie performs U_{2c_i} on the corresponding particle in $S^1_{A_2}$ to form sequence $S^2_{A_2}$ and then send the sequence to Alice. Charlie (Alice, Bob) can deduce other two parties' sub keys through performing Bell-state measurement on the corresponding particles in sequences $S_{C_1}\left(S_{A_1}, S_{B_1}\right)$ and $S^2_{C_2}\left(S^2_{A_2}, S^2_{B_2}\right)$. We give the following Table 1 to show the relations among Alice's (Bob's, Charlie's) first unitary operations, Bob's (Charlie's, Alice's) second unitary operations and Charlie's (Alice's, Bob's) measurement results.

Table 1 Relations among Alice's (Bob's, Charlie's) first unitary operations, Bob's (Charlie's, Alice's) second unitary operations and Charlie's (Alice's, Bob's) measurement results. Alice's (Bob's, Charlie's) first unitary operations are listed in the first column, Bob's (Charlie's, Alice's) second unitary operations are listed in the first row

	U_0 (0)	U_2 (1)
U_0 (0)	$\left\|\psi^+\right\rangle$ (0 ⊕ 0)	$\left\|\psi^-\right\rangle$ (0 ⊕ 1)
U_1 (1)	$\left\|\phi^+\right\rangle$ (1 ⊕ 0)	$\left\|\phi^-\right\rangle$ (1 ⊕ 1)

However, if Bob chooses a different unitary operation $I \otimes U_{2c_i}$ $\left(I \otimes U_{2b_i}\right)$ to perform on the corresponding particle in sequence $S^1_{C_2}$ to form sequence $S^3_{C_2}$, through analyzing Yin et al.'s protocol, we can deduce that the corresponding particle pair in sequences S_{C_1} and $S^3_{C_2}$ is in state $I \otimes U_{2c_i}$ $\left(I \otimes U_{2b_i}\right) I \otimes U_{a_i} \left|\psi^+\right\rangle_{C_1C_2}$. We give the following Table 2 to show the relations among Alice's sub keys, Bob's sub keys, Charlie's sub keys and Charlie's measurement results after Bob has performed $I \otimes U_{2c_i}$ $\left(I \otimes U_{2b_i}\right)$ on the corresponding particle in sequence $S^1_{C_2}$. Bob prepares enough decoy photons and then inserts them into sequence $S^3_{C_2}$ randomly. Bob sends $S^3_{C_2}$ instead of $S^2_{C_2}$ to Charlie. After having confirmed the security of the quantum transmission, Charlie performs Bell-state measurement on the photon pairs in his two sequences to deduce the final shared key. However, the final key $K = K_A \oplus K_B \oplus K_C \oplus K_C = K_A \oplus K_B$ will be only determined by Alice and Bob, Charlie can't detect this kind of attack.

As seen in Table 2, through performing a different unitary operation on the corresponding particles in sequence $S^1_{C_2}$ according to his own sub key and Charlie's sub key, Bob can totally offset the role of Charlie in the generation of the final key, the final key is only determined by Bob and Alice, the protocol is not secure against the insider attack. We take a 4 bits key generation process as an example to show this attack, without loss of generality, we suppose that Alice and Bob want to generate a predetermined key $K = 1111$, they can randomly generate a 4 bits string $R = 0101$ as Alice's sub key $K_A = 0101$, $K_B = K \oplus K_A = 1111 \oplus 0101 = 1010$. After having received the sequence S_{C_2} from Charlie, Alice performs unitary operation U_{a_i} $(i = 1, 2, 3, 4)$ on the ith particle in sequence S_{C_2}, where, $a_1 = 0, a_2 = 1, a_3 = 0, a_4 = 1$. Without loss of generality, we suppose that Alice and Bob deduce that Charlie's sub key is 1101, after having received sequence $S^1_{C_2}$ from Alice, Bob performs unitary operation $I \otimes U_{2c_i}$ $\left(I \otimes U_{2b_i}\right)$ $(i = 1, 2, 3, 4)$ on the ith particle in sequence $S^1_{C_2}$ and then sends the sequence back to Charlie, where, $b_1 = 1, b_2 = 0, b_3 = 1, b_4 = 0, c_1 = 1, c_2 = 1, c_3 = 0, c_4 = 1$. Charlie performs Bell-state measurement on the corresponding photon pairs, he will get results $\left|\psi^+\right\rangle_{C_1C_2}$, $\left|\phi^-\right\rangle_{C_1C_2}$, $\left|\psi^-\right\rangle_{C_1C_2}$ and $\left|\phi^-\right\rangle_{C_1C_2}$, which means that the corresponding bits in Alice's and Bob's sub keys are 00, 11, 01, and 11 respectively. We know that Charlie's sub key is 1101, in this case, Charlie can deduce the final shared key through computing

Table 2 Relations among Alice's sub keys, Bob's sub keys, Charlie's sub keys and Charlie's measurement results after Bob has performed $I \otimes U_{2c_i}$ $\left(I \otimes U_{2b_i}\right)$ on the corresponding particles in $S^1_{C_2}$. Charlie's sub keys are listed in the first column, Alice's sub keys and Bob's sub keys are listed in the first row

	00	01	10	11
0	$\left\|\psi^+\right\rangle_{C_1C_2}$ (00)	$\left\|\psi^-\right\rangle_{C_1C_2}$ (01)	$\left\|\phi^+\right\rangle_{C_1C_2}$ (10)	$\left\|\phi^-\right\rangle_{C_1C_2}$ (11)
1	$\left\|\psi^-\right\rangle_{C_1C_2}$ (01)	$\left\|\psi^+\right\rangle_{C_1C_2}$ (00)	$\left\|\phi^-\right\rangle_{C_1C_2}$ (11)	$\left\|\phi^+\right\rangle_{C_1C_2}$ (10)

the equation $K = (0 \oplus 0 \oplus 1, 1 \oplus 1 \oplus 1, 0 \oplus 1 \oplus 0, 1 \oplus 1 \oplus 1) = 1111$, which in fact has been determined before the execution of the protocol.

The above analysis shows that two dishonest participants in Yin et al.'s protocol [21] can conclude to determine the shared key alone, the protocol can't resist against participant attack. Actually, to avoid the above attack, we should make sure that any two dishonest participants can't choose a suitable unitary operation to offset the role of the third parties' sub key in the generation of the final secret shared key. Inspired by the reference [22], we give an improved protocol as follows. In step 3, after having performed unitary operation U_{j_i} (i= 1,2,...,n) on each particle in the sequence S_{J_2} to form sequence $S^1_{J_2}$, each participant applies a permutation operator $(\Pi_n)_J$ on sequence $S^1_{J_2}$ to form a new sequence $S^{1*}_{J_2}$. In the meanwhile, each participant prepares enough decoy particles and then inserts them into sequence $S^{1*}_{J_2}$. Each participant sends the mixed sequence $S^{1*}_{J_2}$ to the next participant. In the end of the protocol, three participants publicly announce the details of their permutation operators. Alice (Bob, Charlie) can deduce the shared key according to the Bell-state measurement results and the details of Bob's (Charlie's, Alice's) permutation operator.

In summary, we show that the Yin et al.'s QKA protocol [21] is not secure against participant attack. Two dishonest participants can totally offset the third participant's role in the generation of the final shared key by launching a special kind of attack. In order to avoid this flaw, a further improved protocol is proposed.

Acknowledgments The authors would like to thank the anonymous reviewers and editor for their comments that improved the quality of this paper. This work is supported by the National Science Foundation of China (Grant Nos. 61202448 and 61202352), the National High-Tech Research and Development Program of China (Grant No. 2013AA014001) and Collaborative Innovation Center of Wireless Communication Technology.

References

1. Diffie, W., Hellman, M.: IEEE Trans. Inf. Theory **22**, 644–654 (1976)
2. Ingemarsson, I., Tang, D.T., Wong, C.K.: IEEE Trans. Inf. Theory **28**, 714–719 (1982)
3. Burmester, M., Desmedt, Y.: In: Advances in Cryptology-Eurocrypt'94, 275-286. Springer, Berlin (1994)
4. Steiner, M., Tsudik, G., Waidner, M.: IEEE Trans. Parallel Distrib. Syst. **11**, 769–780 (2000)
5. Bellare, M., Canetti, R., Krawczyk, H.: In: Proceedings of the 30th Annual Symposium on the Theory of Computing, 419–428. ACM, New York (1998)
6. Bellare, M., Pointcheval, D., Rogaway, P.: In: Advances in Cryptology-Eurocrypt'00, 139–155. Springer, Berlin (2000)
7. Bellare, M., Rogaway, P.: In: Advances in Cryptology-Crypto'94, 232–249. Springer, Berlin (1994)
8. Bellare, M., Rogaway, P.: In: Proceedings of the 27th Annual ACM Symposium on Theory of Computing, 57–66. ACM, New York (1995)
9. Blake-Wilson, S., Johnson, D., Menezes, A.: In: Proceedings of 6th IMA International Conference on Cryptography and Coding, 30–45. Springer, Berlin (1997)
10. Kudla, C., Paterson, K.G.: In: Advances in Cryptology-Asiacrypt'05, 549–565. Springer, Berlin (2005)
11. Shor, P.W.: In: Proceedings of 35th Annual Symposium on Foundations of Computer Science, 124–134. IEEE, New York (1994)
12. Grover, L.K.: In: Proceedings of 28th Annual ACM Symposium on the Theory of Computing, 212–219. ACM, New York (1996)
13. Zhou, N., Zeng, G., Xiong, J.: Electron. Lett. **40**, 1149 (2004)
14. Chong, S.K., Tsai, C.W., Hwang, T.: Int. J. Theor. Phys. **50**, 1793 (2011)
15. Chong, S.K., Hwang, T.: Opt. Commun. **283**, 1192 (2010)
16. Bennett, C.H., Brassard, G.: In: Proceedings IEEE International Conference on Computers, Systems and Signal Processing, 175–179. IEEE, New York (1984)
17. Shi, R.H., Zhong, H.: Quantum Inf. Process **12**, 921 (2013)

18. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Quantum Inf. Process **12**, 1797 (2013)
19. Sun, Z.W., Zhang, C., Wang, B.H., Li, Q., Long, D.Y.: Quantum Inf. Process **12**, 3411 (2013)
20. Huang, W., Wen, Q.Y., Liu, B., Su, Q., Gao, F.: arXiv:2777.1308 (2013)
21. Yin, X.R., Ma, W.P., Liu, W.Y.: Int. J. Theor. Phys. **52**, 3915 (2013)
22. Shukla, C., Alam, N., Pathak, A.: Quantum Inf. Process **13**, 2391 (2014)
23. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Quantum Inf. Process **13**, 649 (2014)
24. Huang, W., Su, Q., Wu, X., Li, Y.B., Sun, Y.: Int. J. Theor. Phys. **53**, 2891 (2014)
25. Xu, G.B., Wen, Q.Y., Gao, F., Qin, S.J.: Quantum Inf. Process **13**, 2587 (2014)
26. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Phys. Rev. A **84**, 022344 (2011)
27. Zhang, Y.S., Li, C.F., Guo, G.C.: Phys. Rev. A **63**, 036301 (2001)
28. Wójcik, A.: Phys. Rev. Lett. **90**, 157901 (2003)
29. Cai, Q.Y.: Phys. Rev. Lett. **91**, 109801 (2003)
30. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Phys. Rev. A **72**, 044302 (2005)
31. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: Quantum Inf. Comput. **7**, 329 (2007)
32. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: Phys. Rev. A **76**, 062324 (2007)
33. Gao, F., Wen, Q.Y., Zhu, F.C.: Phys. Lett. A **360**, 748 (2007)
34. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Phys. Rev. Lett. **101**, 208901 (2008)
35. Song, T.T., Zhang, J., Gao, F., Wen, Q.Y., Zhu, F.C.: Chin. Phys. B **18**, 1333 (2009)
36. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: Opt. Commun. **283**, 192 (2010)
37. Guo, F.Z., Qin, S.J., Gao, F., Lin, S., Wen, Q.Y., Zhu, F.C.: Eur. Phys. J. D **56**, 445 (2010)