Int J Theor Phys (2013) 52:3915–3921
DOI 10.1007/s10773-013-1702-4

Three-Party Quantum Key Agreement with Two-Photon Entanglement

Xun-Ru Yin · Wen-Ping Ma · Wei-Yan Liu

Received: 23 March 2013 / Accepted: 11 June 2013 / Published online: 3 July 2013
© Springer Science+Business Media New York 2013

Abstract A three-party quantum key agreement protocol with two-qubit entangled states is proposed. In this paper, the three parties are entirely peer entities and each party has a equal contribution to the establishment of the shared secret key. Moreover, any subset of the three participants except the universal set can not determine the shared key alone. Finally, the security analysis shows that the present protocol can resist against both the outsider attack and the insider attack.

Keywords Quantum cryptography · Quantum key agreement · Two-qubit entangled states

1 Introduction

Quantum cryptography has made great progress since the first quantum key distribution protocol (QKD) was proposed by Bennett and Brassard in 1984 [1]. The main goal of this field is to take advantage of quantum effects to provide unconditionally secure information exchange. People have proposed many kinds of quantum cryptographic protocols [2–28], including quantum key distribution, quantum secure direct communication, quantum secret sharing, quantum signature, and so on.

Different from the key distribution, the key agreement protocol is a key establishment technique whereby a shared secret key is derived by two or more specified parties as a function of information contributed by, or associated with, each of these, such that all of them

X.-R. Yin (✉) · W.-P. Ma
State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China
e-mail: xryin@outlook.com

X.-R. Yin
e-mail: yxr03@yahoo.com.cn

X.-R. Yin
School of Mathematics, Taishan University, Tai'an 271021, China

W.-Y. Liu
School of Science, Northwestern Polytechnical University, Xi'an 710072, China

can not predetermine the value of the key [29, 30]. However, the security of classical key agreement based on the computation complexity is strongly challenged by the capability of computation or algorithms, especially since Shor [31] proposed two algorithms for quantum computation, i.e., discrete logarithms and factoring. Therefore, quantum key agreement (QKA) based on the principles of quantum mechanics is a subject worthy of study, in which both parties contribute information and jointly establish the shared secret key by using the quantum channels. In 2004, Zhou et al. [32] first proposed a QKA protocol based on quantum teleportation. However, Zhou et al.'s protocol was pointed out by Tsai et al. [33] that a user can fully determine the shared key alone without being detected. In 2010, Chong and Hwang [34] proposed a QKA protocol based on BB84 [1], in which two parties can negotiate a shared secret key by using the unitary operations and the delayed measurement technique. In 2011, Chong et al. [35] proposed an improvement on Hsueh et al.'s protocol [36] with maximally entangled states. But these QKA protocols [32–36] only involved two parties and can not be used in the multi-party situation. So, in 2013, Shi and Zhong [37] proposed a multi-party QKA based on entanglement swapping with bell states and bell measurements. Unfortunately, Liu et al. [38] pointed out that Shi et al.'s protocol can not be secure in the sense that the key can be totally determined by a dishonest participant alone. In the same paper, Liu et al. proposed a multi-party QKA with single particles, which was the first secure multi-party scheme declared by the authors.

In this paper, we propose a three-party quantum key agreement protocol with two-photon entanglement. We use the idea of quantum dense coding on the four EPR pairs. The three participants are peer entities and they first generate their respective secret keys randomly. Then one party can extract the other two parties' secret keys by performing Bell measurement on the initial particles in his site and the particles encoded by the other two parties. Thus the shared secret key can been established by using the XOR operation. The rest of our paper is structured as follows. Section 2 describes the present protocol in detail. The security analysis is discussed in Sect. 3. Finally, Sect. 4 concludes our scheme briefly.

2 Description of the Present Protocol

Let us introduce two-qubit entangled states. An EPR pair is one of the four Bell states, i.e., $|\psi^+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$, $|\psi^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$, $|\phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, and $|\phi^-\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$. Where $|0\rangle$ and $|1\rangle$ are the up and down eigenstates of Pauli operator σ_z. Let $|+\rangle$ and $|-\rangle$ be $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$ respectively. Suppose U_0, U_1, and U_2 are three local unitary operations. That is, $U_0 \equiv I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_1 \equiv \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $U_2 \equiv \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$. An EPR pair can be transformed into another EPR pair by performing the unitary operation U_i, $i = 0, 1, 2$ on the second particle. The transformation can be shown in Table 1. Furthermore, we perform two consecutive operations on the second qubit of $|\psi^+\rangle$, i.e., if we take U_0 or U_1 as the first unitary operation, U_0 or U_2 as the second unitary operation, then the transformation can be summarized in Table 2.

Table 1 The transformation of the four EPR pairs

	$I \otimes U_0$	$I \otimes U_1$	$I \otimes U_2$
$\|\phi^\pm\rangle$	$\|\phi^\pm\rangle$	$\|\psi^\pm\rangle$	$\|\phi^\mp\rangle$
$\|\psi^\pm\rangle$	$\|\psi^\pm\rangle$	$\|\phi^\pm\rangle$	$\|\psi^\mp\rangle$

Table 2 The transformation of $|\psi^+\rangle$ based on two operations

Initial state	The first operation	The second operation	Final state
$\|\psi^+\rangle$	$I \otimes U_0$	$I \otimes U_0$	$\|\psi^+\rangle$
	$I \otimes U_0$	$I \otimes U_2$	$\|\psi^-\rangle$
	$I \otimes U_1$	$I \otimes U_0$	$\|\phi^+\rangle$
	$I \otimes U_1$	$I \otimes U_2$	$\|\phi^-\rangle$

Suppose that there are three characters, say, Alice, Bob, and Charlie. Three parties want to establish a shared secret key K over the quantum channels. Alice, Bob, and Charlie first generate the random bit strings K_A, K_B, and K_C as their own secret keys, respectively. That is,

$$K_A = \{a_1 a_2 \cdots a_n\}, \tag{1}$$

$$K_B = \{b_1 b_2 \cdots b_n\}, \tag{2}$$

$$K_C = \{c_1 c_2 \cdots c_n\}, \tag{3}$$

where $a_i, b_i, c_i \in \{0, 1\}$, $i = 1, 2, \ldots, n$. In the following, we describe the present quantum key agreement.

Step 1 Each party prepares n entangled states $|\psi^+\rangle$ and divides these entangled states into two ordered qubit sequences. Let P_{A1} and P_{A2} be Alice's two sequences, where each particle in P_{A1} is the first qubit of $|\psi^+\rangle$ and that in P_{A2} is the second qubit. Similarly, P_{B1} and P_{B2} represent Bob's sequences, and P_{C1} and P_{C2} represent Charlie's. Moreover, each party prepares enough decoy photons which are randomly in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then Alice/Bob/Charlie inserts them into $P_{A2}/P_{B2}/P_{C2}$ randomly. After that, Alice/Bob/Charlie sends the mixed sequence to Bob/Charlie/Alice.

Step 2 After confirming Bob/Charlie/Alice has received the sequence, Alice/Bob/Charlie announces the positions and the corresponding basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ of the decoy particles. Then two parties check the quantum channel by comparing the measurement results. If the error rate exceeds the threshold, then this protocol is aborted. Otherwise, it is continued.

Step 3 Bob/Charlie/Alice first picks out the decoy particles, then performs the unitary operation on each particle in $P_{A2}/P_{B2}/P_{C2}$ according to $b_i/c_i/a_i$ $(i = 1, 2, \ldots, n)$, which forms a new sequence $P^1_{A2}/P^1_{B2}/P^1_{C2}$. The rule is described as following. If $b_i = 0/c_i = 0/a_i = 0$, Bob/Charlie/Alice chooses U_0; otherwise, chooses U_1. Moreover, Bob/Charlie/Alice prepares enough decoy particles which are chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts them into $P^1_{A2}/P^1_{B2}/P^1_{C2}$ randomly. Then Bob/Charlie/Alice sends the mixed photon sequence to Charlie/Alice/Bob.

Step 4 After confirming Charlie/Alice/Bob has received the sequence, 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. Otherwise, they continue this process.

Step 5 Charlie/Alice/Bob first picks out the decoy particles, then performs the unitary operation on each particle in $P^1_{A2}/P^1_{B2}/P^1_{C2}$ according to $c_i/a_i/b_i$ $(i = 1, 2, \ldots, n)$, which forms a new sequence $P^2_{A2}/P^2_{B2}/P^2_{C2}$. That is, if $c_i = 0/a_i = 0/b_i = 0$, Charlie/Alice/Bob chooses U_0; otherwise, chooses U_2. Moreover, Charlie/Alice/Bob prepares enough decoy particles which are chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts

them into $P^2_{A2}/P^2_{B2}/P^2_{C2}$ randomly. Then Charlie/Alice/Bob returns the mixed photon sequence to Alice/Bob/Charlie.

Step 6 After confirming Alice/Bob/Charlie has received the sequence, two parties perform the third security check. If they confirm the qubit transmission is insecure, this process is aborted. Otherwise, the protocol is continued.

Step 7 Alice/Bob/Charlie first picks out the decoy particles. Each party has two particle sequences so far. That is, Alice has P_{A1} and P^2_{A2}; Bob has P_{B1} and P^2_{B2}; Charlie has P_{C1} and P^2_{C2}. Each party performs Bell measurement orderly on the corresponding photon pair in his two sequences. According to Table 2 and measurement results, each party can obtain the other two parties' secret keys. Thus the shared secret key $K = K_A \oplus K_B \oplus K_C$.

From the above steps, we can see each party transmits his particle sequence to the other two parties simultaneously, which forms a cycle between them. For conciseness, we ignore the security check and illustrate the whole protocol in Fig. 1. Next, we take $n = 1$ for

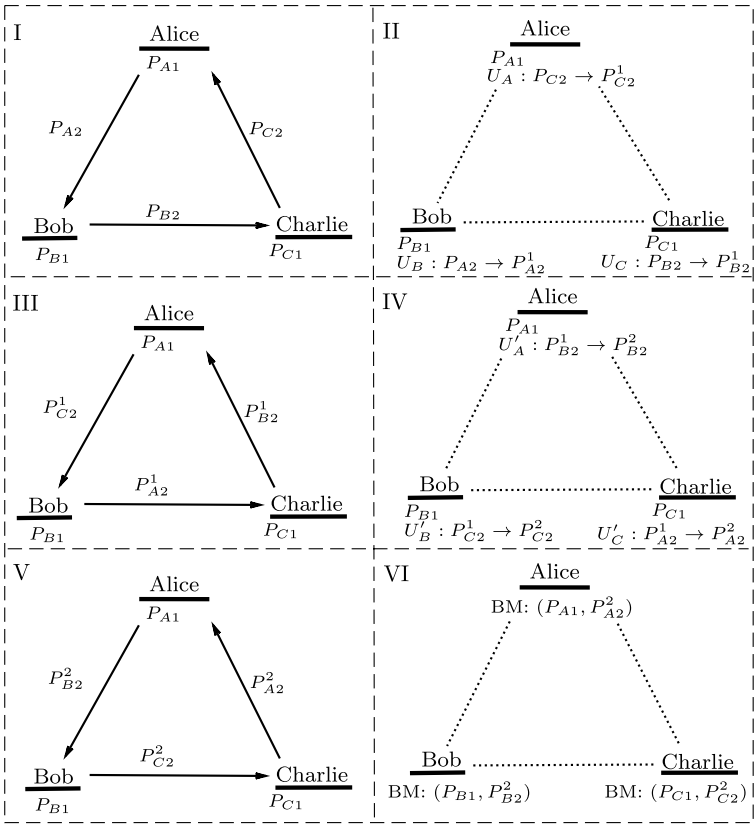

Fig. 1 Illustration of the present protocol. In Step II, U_A, U_B, U_C represent Alice's, Bob's, and Charlie's unitary operation respectively, and $U_A, U_B, U_C \in \{U_0, U_1\}$. "$U_A : P_{C2} \to P^1_{C2}$" represents Alice applies her unitary operation U_A on the particle sequence P_{C2} to form P^1_{C2} (the others are similar). In Step IV, three parties' operations $U'_A, U'_B, U'_C \in \{U_0, U_2\}$. "BM" in Step VI represents Bell measurement. The *solid arrows* denote the quantum channels and the *dotted lines* denote that the three parties execute the procedure simultaneously

example to explain the establishment of K. Suppose $K_A = 0$, $K_B = 1$, $K_C = 1$. We only consider Alice wants to extract Bob's secret key K_B and Charlie's secret key K_C. Alice prepares $|\psi^+\rangle_{12}$, and sends particle 2 to Bob. Bob performs U_1 on the particle according to Step 3 and therefore $|\psi^+\rangle_{12}$ is transformed into $|\phi^+\rangle_{12}$ (Table 1). Then he sends this particle to Charlie. Charlie performs U_2 according to Step 5 and therefore $|\phi^+\rangle_{12}$ is transformed into $|\phi^-\rangle_{12}$ (Table 1). Finally, Charlie sends this particle to Alice. Then Alice performs Bell measurement on this particle and particle 1. The measurement result must be $|\phi^-\rangle_{12}$. Thus Alice can extract K_B and K_C from Table 2. In the same way, if Bob and Charlie prepare $|\psi^+\rangle_{12}$ respectively, they can also obtain the other two parties' secret keys. So three parties can establish a shared secret key 0 by computing $K_A \oplus K_B \oplus K_C$.

3 Security Analysis and Discussion

In this section, we will demonstrate the security of our protocol. A secure quantum key agreement protocol can not only prevent the outside eavesdroppers from getting some information about the shared secret key, but also deter the dishonest participants from determining the shared key alone. That is, a PKA protocol can resist against the outsider attack and the insider attack.

We first consider the outsider attack. Suppose Eve is an evil attacker who wants to steal the shared secret key between the three parties. From the seven steps, we can see that the direction of qubit transmission is one-way and it is a separate process that one party obtains the secret keys of the other two parties. Without loss of generality, we consider Alice is a particle generators, and Bob and Charlie are receivers. When the particles are sent form Alice to Bob, Bob to Charlie, and Charlie to Alice, Eve can take an intercept-resend attack. For example, she captures the particles that Alice sent to Bob and replaces her own particles to resend them. However, the decoy particles are randomly inserted into the sequence and Eve can not possibly know the positions and the corresponding measurement basis of decoy particles before Alice announces the relevant information. In addition, each decoy particle is chosen from the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ randomly. Let m be the number of decoy particles, then the probability that Eve could not been detected is $1/4^m$. Thus, Eve can not pass the eavesdropping check in the condition that the errors occur. The other attack that Eve may employ is the entangle-measure attack. We take the particle 2 of $|\psi^+\rangle_{12}$ for example. Suppose that Eve prepares an ancilla E, and performs a unitary operation U on the particle E and 2 when the particle 2 passes by. Then we have

$$U: \quad |0\rangle|\epsilon\rangle \to |0\rangle|\epsilon_{00}\rangle + |1\rangle|\epsilon_{01}\rangle \tag{4}$$

$$|1\rangle|\epsilon\rangle \to |0\rangle|\epsilon_{10}\rangle + |1\rangle|\epsilon_{11}\rangle, \tag{5}$$

where $|\epsilon_{ij}\rangle$ $(i, j \in \{0, 1\})$ are pure ancilla states uniquely determined by U. The whole quantum system is in the state

$$U\big|\psi^+\big\rangle_{12}|\epsilon\rangle_E = U\left(\frac{1}{\sqrt{2}}\big(|10\rangle + |01\rangle\big)_{21}\right)|\epsilon\rangle_E \tag{6}$$

$$\to \frac{1}{\sqrt{2}}\big(|1\rangle_2|u\rangle_{1E} + |0\rangle_2|v\rangle_{1E}\big), \tag{7}$$

where $|u\rangle \to |0\rangle|\epsilon_{00}\rangle + |1\rangle|\epsilon_{01}\rangle$, $|v\rangle \to |0\rangle|\epsilon_{10}\rangle + |1\rangle|\epsilon_{11}\rangle$. If Eve wants to avoid introducing error, then $\langle 1|u\rangle = 0$ and $\langle 0|v\rangle = 0$ should be satisfied, i.e., $\epsilon_{01} = 0$ and $\epsilon_{10} = 0$. On the other hand, if two parties check the quantum channel by using the basis $\{|+\rangle, |-\rangle\}$, then we have

$$U: \quad |+\rangle|\epsilon\rangle \to \frac{1}{2}\big(|+\rangle\big(|\epsilon_{00}\rangle + |\epsilon_{11}\rangle\big) + |-\rangle\big(|\epsilon_{00} - |\epsilon_{11}\rangle\big)\big) \tag{8}$$

$$|-\rangle|\epsilon\rangle \to \frac{1}{2}\big(|+\rangle\big(|\epsilon_{00}\rangle - |\epsilon_{11}\rangle\big) + |-\rangle\big(|\epsilon_{00} + |\epsilon_{11}\rangle\big)\big). \tag{9}$$

Thus the quantum system is in the state

$$U\big|\psi^+\big\rangle_{12}|\epsilon\rangle_E = U\left(\frac{1}{\sqrt{2}}\big(|++\rangle - |--\rangle\big)_{21}\right)|\epsilon\rangle_E \tag{10}$$

$$\to \frac{1}{2\sqrt{2}}\big(|+\rangle_2\big(|+\rangle_1\big(|\epsilon_{00}\rangle + |\epsilon_{11}\rangle\big)_E + |-\rangle_2\big(|\epsilon_{00}\rangle - |\epsilon_{11}\rangle\big)_E\big) \tag{11}$$

$$- |-\rangle_2\big(|+\rangle_1\big(|\epsilon_{00}\rangle - |\epsilon_{11}\rangle\big)_E + |-\rangle_2\big(|\epsilon_{00}\rangle + |\epsilon_{11}\rangle\big)_E\big)\big). \tag{12}$$

Similarly, Eve must ensure that the measurement results $|+\rangle_2|-\rangle_1$ and $|-\rangle_2|+\rangle_1$ cannot appear if she wants to avoid introducing error. Thus we have $\varepsilon_{00} = \epsilon_{11}$ and the whole quantum system is in the state $|\psi^+\rangle_{12}|\epsilon_{00}\rangle_E$. That is, Eve can not obtain any useful information from observing the ancilla. Therefore our protocol can resist against the outsider attack from the above discussion.

Next, we consider the insider attack. In our protocol, the three random bit strings K_A, K_B, and K_C are generated as Alice's, Bob's, and Charlie's secret key respectively which are only known to themselves and can not be determined by any part of them alone. Each party has a equal contribution to the establishment of the shared secret key and the three parties are entirely peer entities. The way that all the participants share a secret key by combining each participant's key is similar to that in Liu et al.'s protocol [38] which is based on single particles. The difference is that the qubit transmission between all the participants is multi-way in Liu et al.'s protocol. Suppose that Alice is honest without loss of generality, and the dishonest parties Bob and Charlie want to determine the shared key alone. To realize this purpose, the dishonest parties need to obtain Alice's secret key. Thus Bob and Charlie should be particle producers and receive the encoded particles sent from Alice. In Bob's site he directly sends the particles prepared by himself to Alice with the help of Charlie after performing his unitary operation on the particles instead of Charlie's operation. After Alice returns the encoded particles, Bob can get Alice's secret key. In Charlie's site, when he has sent the particle sequence to Alice, Charlie directly receives Alice's encoded particles with the help of Bob to get her secret key by performing the unitary operation himself. However, on the other hand, the procedures are executed simultaneously by the three parties. That is, Alice would not extract Bob's or Charlie's secret key if the two dishonest parties colluded to cheat her. Therefore, our three-party protocol is secure against the outsider attack and insider attack from the above analysis.

4 Conclusion

In this paper, we propose a three-party quantum key agreement protocol based on EPR pairs. Three parties can establish a shared key in such a way that one party extracts the other two parties' secret key and all parties perform XOR operations on their secret keys. Moreover, the security analysis shows that our protocol is security against the outsider attack and insider attack. The security of our scheme is considered under the condition of ideal quantum channels. Since noise cannot be disregarded in a practical transmission process, the success probability of quantum communication would be decreased in a noisy channel. This problem may be solved perfectly in the future research.

Acknowledgements This work was supported by National Science Foundation of China under grant No. 61072140, the 111 Project under grant No. B08038, the Specialized Research Fund for the Doctoral Program of Higher Education under grant No. 20100203110003, and the Project of Shandong Province Higher Educational Science and Technology Program under Grant No. J13LN60.

References

1. Bennett, C.H., Brassard, G.: In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, p. 175. IEEE Press, New York (1984)
2. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
3. Bennett, C.H., Brassard, G., Mermin, N.D.: Phys. Rev. Lett. **68**, 557 (1992)
4. Long, G.L., Liu, X.S.: Phys. Rev. A **65**, 032302 (2002)
5. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Phys. Lett. A **355**, 172 (2006)
6. Huang, W., Guo, F.Z., Huang, Z., Wen, Q.Y., Zhu, F.C.: Opt. Commun. **284**, 536 (2011)
7. Huang, P., He, G.Q., Fang, J., Zeng, G.H.: Phys. Rev. A **87**, 012317 (2013)
8. Zhang, H., Fang, J., He, G.Q.: Phys. Rev. A **86**, 022338 (2012)
9. Zeng, G.H., Keitel, C.: Phys. Rev. A **65**, 042312 (2002)
10. Zeng, G.H.: Phys. Rev. A **78**, 016301 (2008)
11. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**, 042317 (2003)
12. Zeng, G.H., Lee, M., Guo, Y., He, G.Q.: Int. J. Quantum Inf. **5**, 553–573 (2007)
13. Deng, F.G., Long, G.L.: Phys. Rev. A **69**, 052319 (2004)
14. Gao, G.: Int. J. Theor. Phys. **49**, 1870 (2010)
15. Yang, Y.G., Wen, Q.Y.: Sci. China Ser. G **50**, 558 (2007)
16. Gao, F., Guo, F.Z., Wen, Q.Y., et al.: Sci. China Ser. G **51**, 559 (2008)
17. Man, Z.X., Zhang, Z.J., Li, Y.: Chin. Phys. Lett. **22**, 22–24 (2005)
18. Nguyen, B.A.: Phys. Lett. A **328**, 6–10 (2004)
19. Man, Z.X., Xia, Y.J., Zhang, Z.J.: Int. J. Quantum Inf. **4**, 739 (2006)
20. Guo, Y., Chen, Z.G., Zeng, G.H.: Chin. Phys. **16**, 2549 (2007)
21. Guo, Y., Huang, D.Z., Zeng, G.H.: Chin. Phys. Lett. **25**, 16 (2008)
22. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Phys. Rev. A **76**, 062324 (2007)
23. Shi, R.H., Zhong, H.: Quantum Inf. Process. **11**, 161 (2012)
24. Gottesman, D., Chuang, I.: (2001) arXiv:quant-ph/0105032v2
25. Yang, Y.G., Wen, Q.Y.: Opt. Commun. **283**, 3198 (2010)
26. Liu, B., Gao, F., Wen, Q.Y.: IEEE J. Quantum Electron. **47**, 1383 (2011)
27. Yin, X.R., Ma, W.P., Liu, W.Y.: Int. J. Theor. Phys. **51**, 455 (2012)
28. Lin, S., et al.: Phys. Rev. A **78**, 064304 (2008)
29. Mitchell, C.J., Ward, M., Wilson, P.: Electron. Lett. **34**, 980 (1998)
30. Ateniese, G., Steiner, M., Tsudik, G.: IEEE J. Sel. Areas Commun. **18**, 628 (2000)
31. Shor, P.W.: In: Proceedings of 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. IEEE Comput. Soc., Los Alamitos (1994)
32. Zhou, N., Zeng, G., Xiong, J.: Electron. Lett. **40**, 1149 (2004)
33. Tsai, C.W., Hwang, T.: Technical Report, C-S-I-E, NCKU, Taiwan, R.O.C. (2009)
34. Chong, S.K., Hwang, T.: Opt. Commun. **283**, 1192 (2010)
35. Chong, S.K., Tsai, C.W., Hwang, T.: Int. J. Theor. Phys. **50**, 1793 (2011)
36. Hsueh, C.C., Chen, C.Y.: In: Proceedings of the 14th Information Security Conference, National Taiwan University of Science and Technology, Taipei, pp. 236–242 (2004)
37. Shi, R.H., Zhong, H.: Quantum Inf. Process. **12**, 921 (2013)
38. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Quantum Inf. Process. **12**, 1797 (2013)