Quantum Inf Process (2014) 13:1457–1465
DOI 10.1007/s11128-014-0740-z

Authenticated semi-quantum key distribution protocol using Bell states

Kun-Fei Yu · Chun-Wei Yang · Ci-Hong Liao · Tzonelih Hwang

Received: 24 June 2013 / Accepted: 4 February 2014 / Published online: 18 March 2014

Abstract This study presents the first authenticated semi-quantum key distribution (ASQKD) protocols without using authenticated classical channels. By pre-sharing a master secret key between two communicants, a sender with advanced quantum devices can transmit a working key to a receiver, who can merely perform classical operations. The idea of ASQKD enables establishment of a key hierarchy in security systems that also eases the key management problem. The proposed protocols are free from several well-known attacks

Keywords Authentication · Bell state · Quantum cryptography · Semi-quantum key distribution

1 Introduction

Quantum key distribution (QKD) is the first concerned protocol in quantum cryptography. The main goal of a QKD protocol is to distribute a secret key among two communicants using techniques based on quantum mechanics. In these QKD protocols [1–16], two communicants perform quantum operations on their qubits. Both

K.-F. Yu · C.-W. Yang · C.-H. Liao · T. Hwang (✉)
Department of Computer Science and Information Engineering, National Cheng Kung University, No. 1, University Rd., Tainan City 70101, Taiwan, ROC
e-mail: hwangtl@ismail.csie.ncku.edu.tw

K.-F. Yu
e-mail: mrkunfei@gmail.com

C.-W. Yang
e-mail: waywei.yang@gmail.com

C.-H. Liao
e-mail: eddy78731@gmail.com

communicants need to be equipped with advanced quantum devices such as quantum memory, quantum generator, and quantum unitary operations.

Different from the above QKD protocols, Boyer et al. [17,18] proposed two novel semi-quantum key distribution (SQKD) protocols using single photons. According to their definition, the term "semi-quantum" implies that the sender, Alice, is a powerful quantum communicant, whereas the receiver, Bob, has only *classical* capabilities. More precisely, the sender (Alice) has the ability to perform following operations: (1) prepare any quantum state, such as single photons and Bell states, (2) perform any quantum measurement, such as Bell measurement and multi-qubit joint measurement, and (3) store qubits in a quantum memory. Conversely, the classical Bob is restricted to perform the following operations over the quantum channel: (1) prepare new qubits in the classical basis $\{|0\rangle, |1\rangle\}$ (i.e., Z basis), (2) measure qubits in the classical basis, (3) reorder the qubits via different delay lines, and (4) send or reflect the qubits without disturbance. As the classical basis only considers the qubits $|0\rangle$ and $|1\rangle$, the other quantum superpositions of single photons are not considered. Hence, the classical Bob's operations above are equivalent to the traditional $\{0, 1\}$ computation. Apparently, a semi-quantum protocol can reduce not only the computational burden of the communicants but also the cost of the quantum hardware devices in the practical implementation.

The two SQKD protocols proposed by Boyer et al. [17,18] are the randomization-based SQKD and the measure-resend SQKD. The only difference between these two schemes is in the capability of the classical Bob. In the randomization-based SQKD protocol, classical Bob is limited to performing operations (2), (3), and (4), whereas in the measure-resend SQKD protocol, classical Bob is limited to performing operations (1), (2), and (4). After that, Zou et al. [19] presented five SQKD protocols to improve Boyer et al.'s [18] SQKD protocol by using less than four quantum states. In 2011, Wang et al. [20] proposed an SQKD protocol to enhance the qubit efficiency by using maximally entangled states.

To ease the design, however, all the above-mentioned SQKD protocols [17–20] assume the existence of an authenticated classical channel between the sender and receiver (i.e., the transmitted information can be eavesdropped, but cannot be modified), within which both the information integrity and originality can be guaranteed. That is, they assume the availability of authenticated classical channels to provide authentication, which further can be used to detect eavesdropping. Without this assumption, the above SQKD protocols [17–20] would suffer from the impersonation attack, the man-in-the-middle attack or the modification attack [21–23]. That is, an outsider can impersonate the receiver to obtain a secret key or impersonate the sender to send a secret key. In the man-in-the-middle attack, the outsiders can interrupt the information in both public classical channels and quantum channels to impersonate the receiver and reveal the secret key. Furthermore, outsiders can impersonate the sender and send a fake key to the receiver.

In this paper, we propose the first authenticated SQKD protocol (or call ASQKD in short). ASQKD can do without the existence of an authenticated classical channel. A pre-shared master secret key is required between the communicants. This can be done by performing an SQKD (or a QKD) protocol. Once a master key has been shared between two communicants, many session keys can be generated by running

the proposed ASQKD for many communication sessions as long as no eavesdropper is identified. Without using the ASQKD, an SQKD (or a QKD) has to be performed each time whenever a communication session is initiated, which implies that both communicants have to be always in an environment where an authenticated classical channel is available, which could be a restriction for some applications. The proposed ASQKD protocols have been designed to resolve the situation. By using the quantum entanglement of Bell states as well as a pre-shared master secret key, the proposed protocol enables a sender to distribute many session keys to a receiver for many communication sessions via a quantum channel and a public classical channel. Hence, the proposed ASQKD protocol together with an SQKD or a QKD is more effective to implement than merely performing an SQKD or a QKD to solve the above-mentioned scenario. The idea of ASQKD facilitates establishment of a key hierarchy in security systems that also eases the key management problem. Furthermore, the proposed protocols are free from various well-known attacks.

The rest of this paper is organized as follows: Sect. 2 proposes the authenticated semi-quantum key distribution (ASQKD) protocols. Section 3 presents a security analysis of the proposed ASQKD protocols. Section 4 summarizes our results.

2 Proposed ASQKD protocol

This section presents two ASQKD protocols: one is a randomization-based protocol and the other, a measure-resend one.

2.1 Randomization-based ASQKD protocol

Let Alice and Bob be two communicants in an ASQKD protocol, who pre-share a master secret key, which is divided into three parts: K_1, K_2 and K_3, where $K_1 \epsilon \{0,1\}^{2n}$, $K_2 \epsilon \{0,1\}^{2n}$ and $K_3 \epsilon \{0,1\}^{n}$. K_1 is used to decide the initial states of the prepared Bell states, K_2 is used to select either measurement or reflection, and K_3 is used to select the positions of the check values. The procedure of the randomization-based ASQKD is described in the following steps (see also Fig. 1):

Step 1 Alice generates a sequence of Bell states, $S = \{s_1, s_2, \ldots, s_{2n}\}$, according to the secret key K_1, where $s_i = \left\{q_1^i, q_2^i\right\}$ for $i = 1, 2, \ldots, 2n$. If the ith bit of the secret key K_1 is zero, i.e., $K_1^i = 0$, Alice produces s_i in $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Otherwise, Alice produces $\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Then, she divides these $2n$ Bell states into two ordered sequences, $S_A = \{q_1^i\}$ and $S_B = \{q_2^i\}$, which include the first and second particles of all Bell states, respectively. After the above preparation, Alice retains the sequence S_A and sends the sequence S_B to Bob.

Step 2 When Bob receives the qubits in S_B, he chooses to adopt either the SHARE mode or the CHECK mode on each qubit according to the secret key K_2. If the ith bit of the secret key $K_2^i = 0$, Bob chooses the SHARE mode. Otherwise, Bob chooses the CHECK mode. In the SHARE mode, Bob performs a Z-basis measurement on the qubit and obtains the measurement result MR_B, whereas

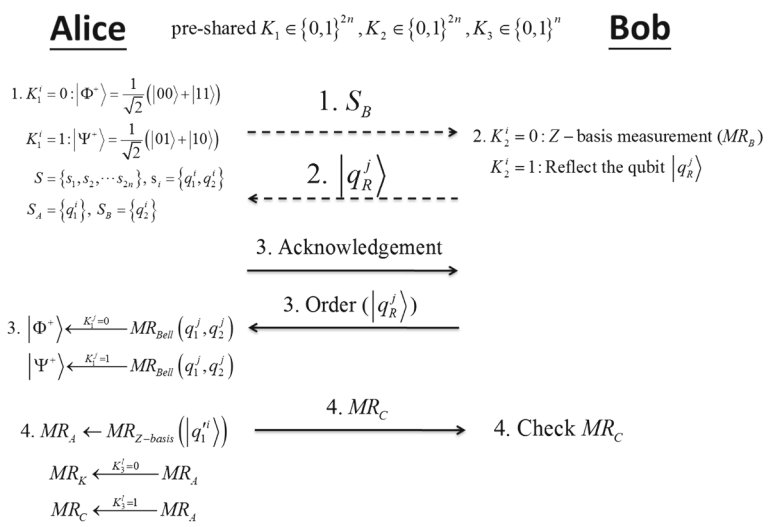

Fig. 1 The proposed randomization-based ASQKD protocol

in the CHECK mode, Bob reflects the qubit (i.e., $|q_{\mathrm{R}}^j\rangle$ for $j = 1, 2, \ldots, n$) back to Alice. Note that the returned qubits in the CHECK mode are reordered via different delay lines.

Step 3 Alice stores the reflected qubits in a quantum memory and publicly announces an acknowledgment. Next, Bob publishes the correct order of the reflected qubits to Alice. According to the Bob's report, Alice can recover the reflected qubits in the correct order. Then, Alice can perform Bell measurement on $\{q_1^j, q_2^j\}$ to check whether each corresponding set of two qubits is consistent with the correlation of a Bell state, $|\Phi^+\rangle$ or $|\Psi^+\rangle$. If there is no eavesdropper, then the protocol will continue to the next step, otherwise they will terminate the protocol and start it again.

Step 4 Alice performs the Z-basis measurement on the remaining qubits $|q_1'^i\rangle$ and obtains the measurement result MR_A. According to the secret key K_3, Alice chooses to share the raw key to form the key sequence MR_K or to check eavesdroppers to form the check sequence MR_C. If the ith bit of the secret key $K_3^i = 0$, Alice chooses to share the raw key. Otherwise, Alice chooses to check eavesdroppers. After Alice announces the check sequence MR_C to Bob, he can verify the entanglement correlation of Bell states for eavesdropping check. Finally, if the transmission between Alice and Bob is secure, then they can distill a private key with the privacy amplification process [24,25] on the raw key. Otherwise, they abort this protocol.

The randomization-based ASQKD protocol uses the entanglement correlation of the Bell states, $|\Phi^+\rangle$ and $|\Psi^+\rangle$, to achieve the goal of quantum key distribution. Here, Bob directly performs the Z-basis measurement on the qubits in the SHARE mode.

2.2 Measure-resend ASQKD protocol

Here, a measure-resend ASQKD protocol, which modifies the operations that Bob is allowed to perform in the randomization-based ASQKD described in Sect. 2.1, is as follows. The modified steps (*) are listed in detail, as follows. The others are the same as those described in Sect. 2.1.

Step 2* Based on the secret key K_2, Bob decides to perform either SHARE or CHECK on each received qubit. If the ith bit of the secret key $K_2^i = 0$, Bob chooses the SHARE mode. Otherwise, Bob chooses the CHECK mode. In the CHECK mode, Bob reflects the qubit back to Alice. However, in the SHARE mode, Bob measures the received qubit using the Z basis and returns a qubit of the same state to Alice.

Step 3* According to the secret key K_2, Alice performs Bell measurement on $\left\{q_1^j, q_2^j\right\}$ to check whether each corresponding set of two qubits is consistent with the correlation of a Bell state, $|\Phi^+\rangle$ or $|\Psi^+\rangle$, where $j = 1, 2, \ldots, n$. If there is no eavesdropper, then the protocol will continue to the next step, otherwise they will terminate the protocol and start it again.

Step 4* According to the secret key K_3, Alice chooses to share the raw key or to check eavesdroppers. If the ith bit of the secret key $K_3^i = 0$, Alice performs the Z-basis measurement on the corresponding qubits to form the key sequence MR_K. Otherwise, Alice chooses to check eavesdroppers as follows. Alice further divides the secret key of value 1 (i.e., $K_3^i = 1$) into the first half and the second half, which represent to check the entanglement correlation and to form the check sequence MR_C on the remaining qubits, respectively. To check the entanglement correlation, Alice performs Bell measurement on $\left\{q_1^l, q_2^l\right\}$ to prevent a directly reflecting attack from Eve, where $l = 1, 2, \ldots, \frac{n}{4}$. If the initial state is $|\Phi^+\rangle$ (or $|\Psi^+\rangle$), then the measurement result is one of $\{|\Phi^+\rangle, |\Phi^-\rangle\}$ (or $\{|\Psi^+\rangle|\Psi^-\rangle\}$). If the measurement results are all the same as their initial states (i.e., $|\Phi^+\rangle$ or $|\Psi^+\rangle$), then it indicates a reflecting attack, and hence, Alice and Bob will terminate the protocol and start it again. However, to form the check sequence MR_C, Alice performs the Z-basis measurement on the corresponding qubits in the second half. After Alice announces the check sequence MR_C to Bob, he can verify the entanglement correlation of Bell states for eavesdropping check. Finally, if the transmission between Alice and Bob is secure, then they can distill a private key with the privacy amplification process [24,25] on the raw key MR_K. Otherwise, they abort this protocol.

The measure-resend ASQKD protocol is also based on the entanglement correlation of the Bell state. The only difference between these two protocols (the randomization-based ASQKD and the measure-resend ASQKD) is in the type of operations that Bob is allowed to perform in the SHARE mode. To detect the presence of eavesdroppers, both schemes use the measurement result of each qubit in the Bell state.

In the proposed ASQKD protocols, the pre-shared master secret key is divided into three parts (i.e., K_1, K_2, and K_3, which are $2N$, $2N$, and N-bit in length, respectively). These master secret keys are used for user authentication and key generation of an

$\frac{N}{2}$-bit raw key as a working key or a session key. The length of the generated raw key is obviously shorter than the master secret key. However, it should be noted that the master secret key can be reused if no eavesdropper is detected. Therefore, a fresh raw key can always be generated between the communicants if needed. Consequently, the communicants do not have to renew the master secret key, which is a tedious work, after completing a protocol execution. Only when a failure occurs in the eavesdropping check or when the master key is used for a long period of time does a new master secret key have to be shared again between Alice and Bob.

3 Security analysis

In this section, the security of the proposed ASQKDs is analyzed from two directions: (1) the impersonation attack and (2) the modification attack. It should be noted that only the security of the randomization-based ASQKD protocol is analyzed in detail. As for the security of the measure-resend ASQKD protocol, the same analysis can be performed.

3.1 Security against impersonation attack

An attacker, Eve, may try to impersonate Alice to send a forged key to Bob. Without knowing the pre-shared key K_1, K_2 and K_3, however, Eve will be caught by Bob with a very high probability. In the randomization-based ASQKD protocol, since Eve does not know the initial states of Bell states, the decision of measurement or the reflection on each qubit, and the positions of the check values (i.e., K_1, K_2, and K_3 respectively), she may try to generate a sequence of single photons, $Q_E = \{|0\rangle_1, |0\rangle_2, \ldots, |0\rangle_{2n}\}$, and send them to Bob in Step 1. If Eve can pass the eavesdropping check in Step 4, then she is able to successfully impersonate Alice to share a secret key with Bob. However, without knowing the pre-shared key K_1, K_2 and K_3, Eve cannot compute the check sequence MR_C. The probability for a random guess on each bit of MR_C is $\frac{1}{2}$. Hence, the probability for Eve to be detected in the randomization-based ASQKD protocol is $1-\left(\frac{1}{2}\right)^{\frac{n}{2}}$. While n is large enough, the detection probability is approximately 100 %. Similarly, in the measure-resend ASQKD protocol, the probability for Eve to be detected is $1-\left(\frac{1}{2}\right)^{\frac{n}{4}}$.

On the other hand, Eve may try to impersonate Bob to communicate with Alice. In the randomization-based ASQKD protocol, Eve may intercept the sequence S_B sent from Alice to Bob in Step 1. Since Eve does not know the decision of measurement or the reflection on each qubit (i.e., K_2), she may try to randomly reflect a sequence of qubits back to Alice in Step 2. In this case, if Eve reflects the correct qubits back to Alice, then she is able to successfully impersonate Bob. The probability for a random guess on each bit of K_2 is $\frac{1}{2}$. If, however, Eve reflects the wrong qubits back to Alice, then Eve can successfully pass the verification process of Alice with a probability of $\frac{1}{4}$ for each qubit. For example, if the initial state is $|\Phi^+\rangle$ (or $|\Psi^+\rangle$), then Alice performs the Bell measurement on the wrong qubit to obtain the measurement result $|\Phi^+\rangle$ (or $|\Psi^+\rangle$) with a probability of $\frac{1}{4}$ because she will randomly obtain one of

the four measurement results from $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$. As a result, Eve has a probability of $\frac{5}{8}\left(=\frac{1}{2}+\frac{1}{2}\times\frac{1}{4}\right)$ to pass the verification for each qubit. Hence, the probability for Eve to be detected in the randomization-based ASQKD protocol is $1-\left(\frac{5}{8}\right)^n$. The detection probability would converge to 1 when n is large enough.

In the measure-resend ASQKD protocol, Eve may try to impersonate Bob as follows. Eve intercepts the sequence S_B from Alice to Bob in Step 1. She then reflects the original qubits back to Alice in Step 2. If Eve can pass the eavesdropping check in Step 4, then she is able to successfully impersonate Bob (though she cannot share a key with Alice). However, Eve will be detected because she does not measure the qubits in Step 2. In Step 4, Alice uses the entanglement correlation check to detect this type of attack (the reflecting attack). Because Eve only sends the original qubits back to Alice without measuring them, the measurement results are all the same as their initial states. Hence, Eve will be detected by Alice.

3.2 Security against modification attack

In the modification attack, Eve may try to modify the contents of the transmitted qubits to make the communicants obtain a wrong secret key without being detected. Although adding checksum could also solve this problem [21,23], this protocol tries to avoid this attack based on quantum mechanism (i.e., based on the entanglement correlation of the Bell state). In Step 1, Eve intercepts the sequence S_B and then performs the unitary operation $\sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|$ on a qubit to form a sequence Q'_E and sends it to Bob. That is, the Bell state $|\Phi^+\rangle$ (or $|\Psi^+\rangle$) will be changed to $|\Psi^+\rangle$ (or $|\Phi^+\rangle$). An arbitrary modification to a qubit, however, could lead to the wrong measurement results and therefore would be probably detected by Alice (or Bob). Suppose that the SHARE mode and the CHECK mode are chosen equally likely. If Bob chooses the CHECK mode for that modified qubit (i.e., Bob reflects the modified qubit back to Alice), then Eve cannot pass the verification process of Alice because the measurement result cannot be equal to the initial state. If, however, Bob chooses the SHARE mode, then Alice can choose to share the raw key or to check eavesdroppers according to K_3 in Step 4. Hence, once Bob chooses to share the raw key, Eve can successfully modify a qubit with a probability of $\frac{1}{4}\left(=\frac{1}{2}\times\frac{1}{2}\right)$. Thus, the detection probability is $1-\left(\frac{1}{4}\right)^{\frac{n}{2}}$ if n bits are modified. If n is large enough, the detection rate would converge to 1. To avoid the low detection rate with small number of modifications, quantum error correction codes can be applied to correct or detect small number of errors. However, this is not the focus of this paper.

4 Conclusions

This study proposes two new ASQKD protocols via Bell states without using authenticated classical channels. The security analysis shows that the proposed protocols are free from the impersonation attack and the modification attack. It should also be noted here that, the same as all semi-quantum scheme, the proposed protocols suffer from

the Trojan-horse attacks [26–28]. To prevent this kind of attacks, the photon number splitter device and wavelength filter device could be adopted [29–31].

Acknowledgments We would like to thank the National Science Council of the Republic of China, Taiwan for partially supporting this research in finance under the Contract No. NSC 100-2221-E-006-152-MY3.

References

1. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121–3124 (1992)
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
3. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chinese Phys. Lett. **21**(11), 2097–2100 (2004)
4. Long, G., Liu, X.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**(3), 032302 (2002)
5. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050–2056 (1999)
6. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
7. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984)
8. Zhang, Z.J., Man, Z.X., Shi, S.H.: An efficient multiparty quantum key distribution scheme. Int. J. Quantum Inf. **3**(3), 555–560 (2005)
9. Chen, P., Li, Y.-S., Deng, F.-G., Long, G.-L.: Measuring-basis encrypted quantum key distribution with four-state systems. Commun. Theor. Phys. **47**(1), 49–52 (2007)
10. Li, X.-H., Deng, F.-G., Zhou, H.-Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**(2), 022321 (2008)
11. Li, X.-H., Duan, X.-J., Deng, F.-G., Zhou, H.-Y.: Error-rejecting Bennett–Brassard–Mermin quantum key distribution protocol based on linear optics over a collective-noise channel. Int. J. Quantum Inf. **8**(7), 1141–1151 (2010)
12. Li, X.-H., Zhao, B.-K., Sheng, Y.-B., Deng, F.-G., Zhou, H.-Y.: FAULT tolerant quantum key distribution based on quantum dense coding with collective noise. Int. J. Quantum. Inf. **7**(8), 1479–1489 (2009)
13. Zhao, B.-K., Sheng, Y.-B., Deng, F.-G., Zhang, F.-S., Zhou, H.-Y.: Stable and deterministic quantum key distribution based on differential phase shift. Int. J. Quantum Inf. **7**(4), 739–745 (2009)
14. Hwang, T., Hwang, C.C., Tsai, C.W.: Quantum key distribution protocol using dense coding of three-qubit W state. Eur. Phys. J. D **61**(3), 785–790 (2011)
15. Hwang, T., Lee, K.C., Li, C.M.: Provably secure three-party authenticated quantum key distribution protocols. IEEE Trans Depend Secur **4**(1), 71–80 (2007)
16. Hwang, T., Tsai, C.W., Chong, S.K.: Probabilistic quantum key distribution. Quantum Inf. Comput. **11**(7–8), 615–637 (2011)
17. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. Phys. Rev. Lett. **99**(14), 140501 (2007)
18. Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Phys. Rev. A **79**(3), 032341 (2009)
19. Zou, X., Qiu, D., Li, L., Wu, L., Li, L.: Semiquantum-key distribution using less than four quantum states. Phys. Rev. A **79**(5), 052312 (2009)
20. Wang, J., Zhang, S., Zhang, Q., Tang, C. J.: Semiquantum key distribution using entangled states. Chinese Phys. Lett. **28**(10), 100301 (2011)
21. Yang, C.-W., Hwang, T.: Improved QSDC protocol over a collective-dephasing noise channel. Int. J. Theor. Phys. **51**(12), 3941–3950 (2012)
22. Lin, J., Yang, C.-W., Tsai, C.-W., Hwang, T.: Intercept-resend attacks on semiquantum secret sharing and the improvements. Int. J. Theor. Phys. **52**(1), 156–162 (2013)

23. Yang, C.-W., Hwang, T., Lin, T.-H.: Modification Attack on QSDC with Authentication and the Improvement. Int. J. Theor. Phys. **52**(7), 2230–2234 (2013)
24. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM J. Comput. **17**(2), 210–229 (1988)
25. Bennett, C.H., Brassard, G., Crepeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inf. Theory **41**(6), 1915–1923 (1995)
26. Yang, C.-W., Hwang, T., Luo, Y.-P.: Enhancement on "quantum blind signature based on two-state vector formalism". Quantum Inf. Process. **12**(1), 109–117 (2013)
27. Deng, F.G., Zhou, P., Li, X.H., Li, C.Y., Zhou, H.Y.: Robustness of two-way quantum communication protocols against trojan horse attack. Quantum Phys. (2005) arXiv:quant-ph/0508168v1z
28. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**(1–2), 23–25 (2006)
29. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**(4), 044302 (2005)
30. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**(5), 054302 (2006)
31. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack (vol 72, art no 044302, 2005). Phys. Rev. A **73**(4), 049901 (2006)