Int J Theor Phys (2016) 55:98–106
DOI 10.1007/s10773-015-2636-9

Quantum Key Distribution Based on Interferometry and Interaction-Free Measurement

Yan-Bing Li[1,2,3] · Sheng-Wei Xu[1] · Qing-Le Wang[2] · Fang Liu[1] · Zong-Jie Wan[1]

Received: 1 February 2015 / Accepted: 27 March 2015 / Published online: 16 April 2015

Abstract We propose a quantum key distribution based on Mach-Zehnder (MZ) interferometry and interaction-free measurement on single photon. The raw key comes from the photons on which MZ interferometry happened. And the interaction-free measurements are used to detect eavesdroppers. The analysis indicates that the protocol is secure, and can prevent some familiar attacks, such as photon number splitting (PNS) attack. This scheme is easy to be realized in current experiments.

Keywords Quantum key distribution · MZ interferometry · Interaction-free measurement

1 Introduction

Quantum cryptography allows higher security than classical cryptography as it is based on the laws of physics instead of the difficulty of solving mathematical problems. Quantum key distribution (QKD) [1], which is to provide secure means of distributing secret keys between two participants, the sender (Alice) and the receiver (Bob), in fact is the most important protocol of quantum cryptography, and has been researched and developed in both theoretics and experiments [2–13].

Mach-Zehnder (MZ) interferometer is a basic phenomenon in optical physics, and has been used to design QKD. Such as in the QKD schemes in Ref. [3, 4], one single photon

✉ Yan-Bing Li
liyanbing1981@gmail.com

[1] Beijing Electronic Science and Technology Institute, Beijing, 100070, China

[2] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China

[3] Department of Electrical Engineering and Computer Science, Northwestern University, Evanston, IL 60208, USA

carrying a bit secret information was split into two wave packets transmitted in different times, by which Eve cannot cheat the bit without being detected. Interaction-free measurement which can be produced with same equipments as MZ interferometer also has been used to design QKD. Such as in the QKD schemes in Ref. [5, 8], the single photon carrying secret information is transmitted through part of quantum channels, by which Eve cannot cheat the bit without being detected.

In this paper, we report a quantum key distribution based on interferometry and interaction-free measurement together. The raw key comes from the photons on which interferometry happened. And the interaction-free measurements are used to detect eavesdroppers. Since interferometry and interaction-free measurement are easy to realized in one system, the scheme is simple and realizable in experiment. We also analyze its security both in the ideal setting and the practical setting.

The rest of this paper is constructed as follows. Section 2 shows our quantum key distribution protocol. Some analysis about its security in the ideal setting and the practical setting are given in Section 3. In Section 4, we analyze the protocol's efficiency and compare it with some other QKD protocols briefly. Finally, Section 5 is a short conclusion.

2 The Quantum Key Distribution Protocol

Let we first introduce MZ interferometry and interaction-free with a single-photon.

Figure 1 is the schematic of interferometry with a single-photon. S denotes the single particle source, D_1 and D_2 are detectors, M is a mirror and BS is a 50/50 beam splitter. When a particle enters a MZ interferometer, detector D_1 should be dark and detector D_2 clicks because of constructive interference.

The input state can be described as $|0\rangle_a|1\rangle_b$, where the subscript means which path the state is in. The first beam splitter transforms the input as

$$|1\rangle_a|0\rangle_b \rightarrow \frac{1}{\sqrt{2}}(|1\rangle_c|0\rangle_d + i|0\rangle_c|1\rangle_d). \tag{1}$$

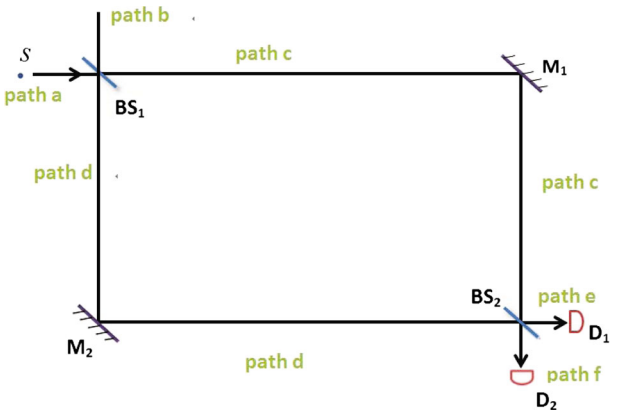

Fig. 1 (color online).The schematic of interferometry with a single-photon

The mirrors contribute a factor of $e^{i\pi/2}$ to each term, amounting to an irrelevant phase, which we omit. At the second beam splitter we have the following transformations

$$|1\rangle_c|0\rangle_d \rightarrow \frac{1}{\sqrt{2}}(|1\rangle_e|0\rangle_f + i|0\rangle_e|1\rangle_f), \tag{2a}$$

$$|0\rangle_c|1\rangle_d \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_e|1\rangle_f + i|1\rangle_e|0\rangle_f). \tag{2a}$$

Thus the transformation on the total state due to the second beam splitter is

$$\frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b + i|1\rangle_a|0\rangle_b) \rightarrow i|0\rangle_e|1\rangle_f. \tag{3}$$

So the detector D_2 clicks.

When there is an absorber (opaque object) present in path c or d, it becomes an interaction-free measurement with a single-photon. Figure 2 gives the example that the absorber blocks path d. Then the state is collapsed to $|0\rangle_c|1\rangle_d$ or $|1\rangle_c|0\rangle_d$ with equal probability $1/2$. In the first case, $|0\rangle_c$, i.e., vacuum state will not click any detectors. In the second case, because there is no longer an open path to cause interference, at the second beam splitter the photon $|1\rangle_c$ has a $50:50$ chance of being transmitted to detectors D_1 and D_2. So they click with equal probability. In other words, when the absorber presents in path c or d, totally D_1 and D_2 clicks with equal probability $1/4$. (If the absorber was replaced by a detector, it would click with remaining probability $1/2$.) Thus one can deduce that an absorber is present in path c or d.

With the above in mind, we now proceed to describe a model for quantum key distribution. The scheme is shown in Fig. 3.

In this protocol, Alice sends some random secret information to Bob. Let us consider the case of error-free channels and perfect devices. The details are proposed as following.

(1) Alice's source produces a sequence of N single photons. Alice sends single photon from path a (i.e., the state is $|1\rangle_a|0\rangle_b$) representing bit 0, or b (i.e., the state is $|0\rangle_a|1\rangle_b$) representing bit 1. So Alice has bit sequence $S = \{s_1, s_2, \ldots, s_N\}$.

(2) Before transferring the ith photon, both Alice and Bob have a chance to insert a detector to block path c or d. In other words, they detect the state in one of path c or d

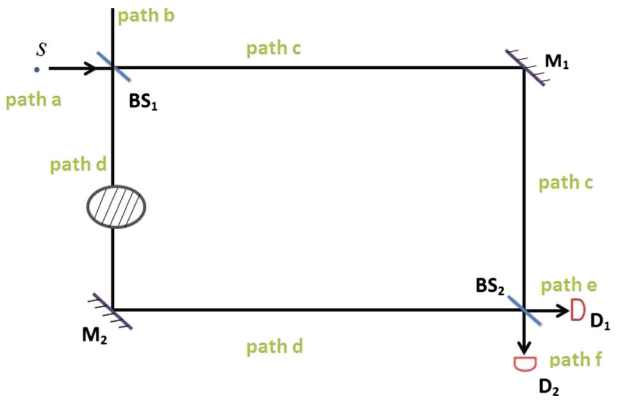

Fig. 2 (color online). An interaction-free measurement with a single-photon

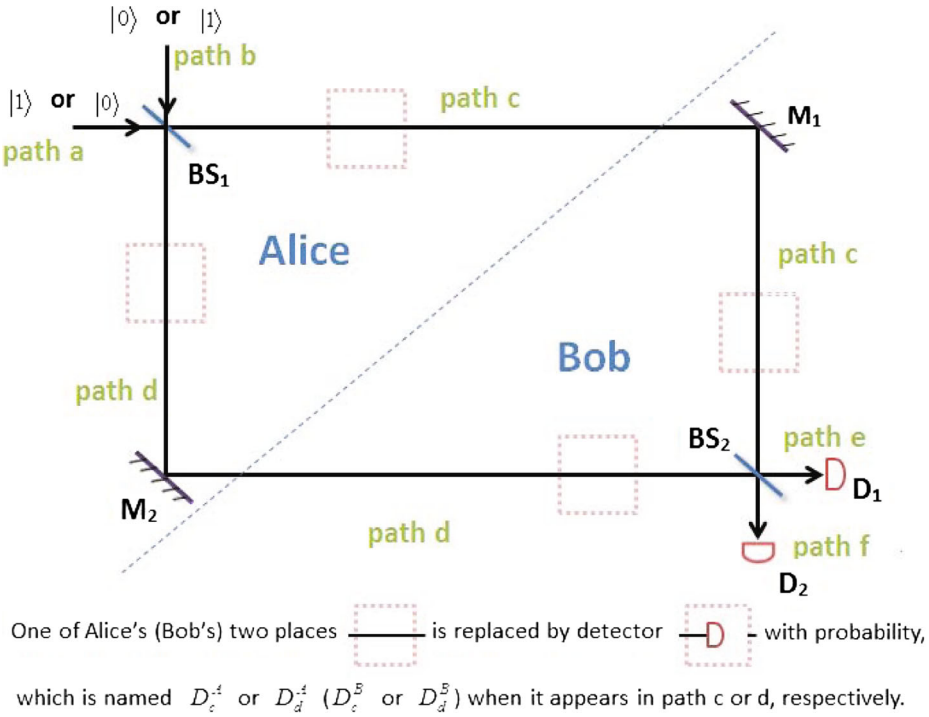

Fig. 3 (color online). The QKD based on interferometry and interaction-free detection

with some probabilities. The detectors are named as D_c^A, D_d^A, D_c^B and D_d^B, where D_j^X means $X(= A \text{ or } B)$'s detector is inserted on path $j(= c \text{ or } d)$.

(3) After all the N photons have been transmitted, both of Alice and Bob announce the orders in which they have detected in paths c and d respectively. And they also announce the orders in which the detectors have clicked. There are three restrictions as following. (i) If both of paths c and d have been blocked, detectors D_1 and D_2 should not click. (ii) If only one of paths c and d has been blocked, detectors D_1 and D_2 should click with probability $1/4$, respectively. (iii) To ith transmission, only one of D_1, D_2, the detectors in path c (i.e., D_c^A and D_c^B) and the detectors in path d (i.e., D_d^A and D_d^B) should click. Alice and Bob use these to check eavesdropper.

(4) When both of path c and d have not been blocked, Bob can make sure Alice's bit s_i as following. D_1 clicks means $s_i = 1$, D_2 clicks means $s_i = 0$. He announces some of them to check eavesdropper and estimate the bit error rate e with Alice. Subsequently, the other bits were used as raw key bits.

(5) Alice and Bob use classical error correction method [22] to correct errors in the raw key and then execute privacy amplification [23] to eliminate the information leakage of the raw key. Finally, Alice and Bob share a secure key.

3 Security Analysis

In this section, we analyze the protocol's security both in ideal setting and practical setting.

3.1 Security Analysis in Ideal Setting

In the proposed QKD, after the possible block in path c or d, the ith state Alice sends out evolves to one of the four states

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle_c|1\rangle_d + i|1\rangle_c|0\rangle_d), \tag{4a}$$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|1\rangle_c|0\rangle_d + i|0\rangle_c|1\rangle_d), \tag{4b}$$

$$|\phi_+\rangle = |1\rangle_c|0\rangle_d, \tag{4c}$$

$$|\phi_-\rangle = |0\rangle_c|1\rangle_d, \tag{4d}$$

randomly. And what Bob does is making a measurement in basis $\{|0\rangle|1\rangle, |1\rangle|0\rangle\}$ or $\{|\phi_0\rangle, |\phi_1\rangle\}$. These states and measurements like that in BB84 QKD. The difference are that the secure information are only represented by the states in basis $\{|\phi_0\rangle, |\phi_1\rangle\}$, and the states are transferred from two paths.

Because the states are transferred from two paths, Eve could intercept only one or both of the two path and measure it. First, we will indicate that Eve cannot obtain any information about the raw key if she only measures on one path. Without loss of generality, we suppose that she makes a measurement on path c. Regardless of the state Alice sent out is $|\phi_0\rangle$ or $|\phi_1\rangle$, the reduced density operators of the sub-state which passes through path c is $\begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$ all the time. According to the conclusion of discriminating two density operators [14], one cannot distinguish two states whose reduced density operators are identical. So Eve cannot distinguish them with any strategies if she only cheats from one path.

Next, we analyze the case that Eve cheats from paths c and d simultaneously. Eve has a lot of possible strategies. For example, an eavesdropper could place two special equipments in the paths c and d, which does nothing when facing the vacuum, and emits a photon after absorbing a signal photon. Since Eve's strategies are performed on both of the two paths, we should analyze the system state composed by the sub-system state in path c and the sub-system state in path d.

In the proposed QKD, the system states sent out from Alice's site are randomly in one of $\{|\phi_0\rangle, |\phi_1\rangle, |\phi_+\rangle, |\phi_-\rangle\}$, which satisfy

$$\langle\phi_0|\phi_1\rangle = \langle\phi_+|\phi_-\rangle = 0, \tag{5a}$$

$$||\langle\phi_0|\phi_+\rangle||^2 = ||\langle\phi_0|\phi_-\rangle||^2 = ||\langle\phi_1|\phi_+\rangle||^2 = ||\langle\phi_1|\phi_-\rangle||^2 = \frac{1}{2}. \tag{5b}$$

Then Bob randomly performs measurement in basis $\{|\phi_0\rangle, |\phi_1\rangle\}$ or $\{|\phi_+\rangle, |\phi_-\rangle\}$. Alice and Bob detect cheat strategies by comparing the state and the measurement result. In the security analysis of BB84 QKD [15], without the knowledge of whether the state's basis is $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$, Eve's any cheat strategies, such as measurement-resend attack, entangle-resend attack will disturb the state and be detected with some probability. In the

proposed QKD, the system states and detection strategy are similar to the four BB84 states and the detection strategy in BB84 QKD. Any measurements performed on both of the two paths together could be considered as global measurements on the system state. In the same way, Eve's any cheat strategies, such as measurement-resend attack, entangle-resend attack will disturb the states and be detected with some probability. When the cheat strategies are performed on a large amount of states, they will be detected with certainty. So the proposed scheme is secure in ideal setting.

3.2 Security in Practical Setting

But due to the limitations of real-life setting [16], such as the imperfect sources, imperfect detectors, loss and noise in channels, practical QKD has security loopholes and has suffered some attacks. The most familiar attack of them is photon number splitting (PNS) attack [17].

Usually, Eve performs the PNS attack by replacing the high loss channel between Alice and Bob with a lossless channel first. Then she performs a quantum non-demolition (QND) measurement on each pulse to obtain number information without disturbing the states. If only one single photon is present in a pulse, she blocks a fraction of these pulses to simulate the loss. Else if multiple photons are present in a pulse, she catches one photon and stores it in her quantum memory, then sends a fraction of the remaining photons to Bob for simulating the loss. After Alice and Bob announced the based of each pulse and discussed the measurement outcomes, Eve can measure the photons in her memory in correct bases and obtain a significant fraction of the raw key without being detected.

In the presented scheme, the secret information is encoded in states $|\phi_0\rangle = \frac{1}{\sqrt{2}}|0\rangle_c|1\rangle_d + \sqrt{R}|1\rangle_c|0\rangle_d$ and $|\phi_1\rangle = \frac{1}{\sqrt{2}}|1\rangle_c|0\rangle_d + \sqrt{R}|0\rangle_c|1\rangle_d$, which are the entangled states of $|1\rangle$ and vacuum state $|0\rangle$. If Eve makes a number measurement on the state after it leaves Alice' site, the state will no longer be an entangled states of $|1\rangle$ and vacuum state $|0\rangle$. Eves measurement will collapse the entangled state into $|1\rangle_c|0\rangle_d$ or $|0\rangle_c|1\rangle_d$. When Alice and Bob detect by comparing a part of secret information, the PNS attack will be detected.

Beside PNS attack, the non-ideal cases will also bring some risks to the proposed QKD. Any imperfection in the channels, such as unbalanced loss in the paths c and d, and imperfect detection efficiency of the detectors, may change the detection probability $(1/4)$ of the detector D_1 and D_2 to an unexpected probability, which makes the detection of the eavesdropper fail. Generally, a upper bound of error bits is existent in a practical setting, which indicates that the error bits come from the practical setting including imperfect channel, imperfect source and detections should not exceed a threshold. The threshold will be used to improve the presented QKD's security when it is actualized. If the error rate exceeds the threshold, an eavesdropper is likely to cheat the information. Then the protocol should be re-start which lets the leaked information be discarded. On the other hand, if the eavesdropper only cheat a small portion of the information the error rate comes from which did not exceed the error threshold, she will not be detected. However, because the information leakage of the raw key is small, valid information will be eliminated to zero with privacy amplification processes in step (5).

Some other attacks also have been proposed in practical setting, such as Trojan-horse attack [18–20], faked state attack [21]. They are based on the imperfect devices in practical setting, and use illegal wave pulse or resend the intercepted state in detector's mismatch time window to cheat. In order to limit these attacks, the system should be designed in such a way

that (1) using filters to only permit light at appropriate wavelength enter, (2) the "doors" of operation device and detector should be open only during short times, i.e., the encoding optical components should be active only during short times, and activate phase modulators only when the qubits is there, and (3) making a counter measures on the possible leak to Eve, then using privacy amplification (PA) [22, 23] on raw key to compress the leak to zero.

4 Discussion

In this section, we will analyze the above QKD scheme's efficiency, and compare the scheme with some other QKD schemes which are based on interferometry or interaction-free measurement briefly.

Let $\eta = c/q$ be the qubit efficiency of a quantum protocol, where c denotes the total number of transmitted classical bits and q denotes the total number of photons generated in the protocol. We suppose that Alice's actions of blocking path c, blocking path d, and unblocking neither path c or d will happen with probabilities p_c^A, p_d^A and $p_{no}^A = 1 - p_c^A - p_c^A$ respectively. And suppose that Bob's actions of blocking path c, blocking path d, and unblocking neither path c or d will happen with probabilities p_c^B, p_d^B and $p_{no}^B = 1 - p_c^B - p_c^B$ respectively. Then interferometry will happen with probability $o_{no}^A \times o_{no}^B$. So the qubit efficiency of the proposed protocol is $o_{no}^A \times o_{no}^B$ in an ideal setting (shown in Fig. 4). Alice and Bob could adjust these parameters o_{no}^A and o_{no}^B respectively to have a best balance between key rate and security. When they want higher key rate, they can increase the values. But we should point out that the protocol's capability of detecting eavesdropper

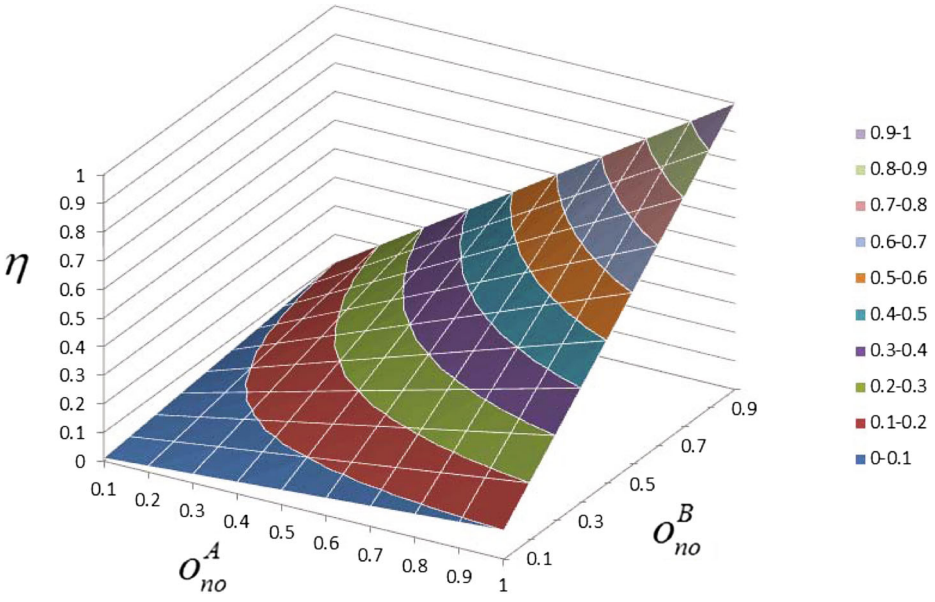

Fig. 4 (color online). The qubit efficiency of the proposed QKD related with Alice's no blocking probability o_{no}^A and Bob's no blocking probability o_{no}^B

will decrease with increasing of raw key rate. So both of o_{no}^{A} and o_{no}^{B} should be more less than 1 for let some interaction-free measurement to detect the Eve.

There are some QKD schemes which are based on MZ interferometry or interaction-free measurement have been proposed previously. In the QKD schemes based on interferometry [3, 4], the advantage is that the qubit efficiency in ideal setting could be close to 1. But the disadvantage is that optical delay lines should be used to delay one split wave packet, which will decrease the actual transmission distance of information. In the QKD schemes based on interaction-free measurement [5, 8], the advantage is that the qubits carrying secret information will not transfer between the whole channel which can increase the protocol's security. But the disadvantage is that the qubit efficiency is low, which are $1/8$ and $1/4$ respectively even in an ideal setting. Compared with these QKD protocols, the proposed QKD is flexible as its qubit efficiency and security degree could be adjusted by choosing suitable blocking probabilities. Further, we will study the suitable blocking probabilities in some different settings.

5 Conclusion

In conclusion, this paper proposes a quantum key distribution based on interferometry and interaction-free measurement. The raw key comes from the photons on which interferometry happened. And the photons on which interaction-free happened are used to detect eavesdropper. The analysis shows that the protocol is secure in the ideal setting, and can prevent some familiar attacks in practical settings. In practice, the scheme needs only two sources, some switches and detectors, which are easy to be constructed.

Acknowledgments This work is supported by NSFC (Grant Nos. 61272057, 61170270, 61370188), Beijing Higher Education Young Elite Teacher Project (Grant Nos. YETP0475, YETP0477), the Fundamental Research Funds for the Central Universities (Grant No. 328201506), China scholarship council.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: IEEE International Conference on Computers, Systems and Signal Processing, p. 175C179. IEEE, New York, Bangalore, India (1984)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
3. Goldenberg, L., Vaidman, L.: Quantum cryptography based on orthogonal states. Phys. Rev. Lett. **75**, 1239–1243 (1995)
4. Koashi, M., Imoto, N.: Quantum cryptography based on split transmission of one-bit information in two steps. Phys. Rev. Lett. **79**, 2383–2386 (1997)
5. Guo, G.C., Shi, B.S.: Quantum cryptography based on interaction-free measurement. Phys. Lett. A **256**, 109–112 (1999)
6. Yuen, H.P.: In: Tombesi, P., Hirota, O. (eds.) Proceedings of QCMC00, Capri, 2001. Plenum Press, New York (2001)
7. Hwang, W.Y.: Quantum key distribution with high loss: Toward global secure communication. Phys. Rev. Lett. **91**, 057901 (2003)
8. Noh, T.G.: Counterfactual quantum cryptography. Phys. Rev. Lett. **103**, 230501 (2009)
9. Allati, A.E., Baz, M.E., Hassouni, Y.: Quantum key distribution via tripartite coherent states. Quantum Inf. Process **10**(5), 589–602 (2011)
10. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)

11. Lin, S., Liu, X.F.: A modified quantum key distribution without public announcement bases against photon-number-splitting attack. Int. J. Theor. Phys. **51**, 2514–2523 (2012)
12. Mishra, M.K., Prakash, H.: Bipartite coherent-state quantum key distribution with strong reference pulse. Quantum Inf. Process **12**(2), 907–920 (2013)
13. Li, Y.B.: Analysis of counterfactual quantum key distribution using error correcting theory. Quantum Inf. Process **13**(10), 2325–2342 (2014)
14. Fuchs, C.A.: Information gain vs. state disturbance in quantum theory. Fortschr. Phys. **46**, 535–565 (1998)
15. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**, 2050 (1999)
16. Brassard, G., Lütkenhaus, N., Mor, T., Sanders, B.C.: Limitations on practical quantum cryptography. Phys. Rev. Lett. **85**, 1330–1333 (2000)
17. Huttner, B., Imoto, N., Gisin, N., Mor, T.: Quantum cryptography with coherent states. Phys. Rev. A **51**, 1863 (1995)
18. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**, 022320 (2006)
19. Wang, T.Y., Wen, Q.Y.: Security of a kind of quantum secret sharing with single photons. Quantum Inf. Comput. **11**(5–6), 0434–0443 (2011)
20. Yang, Y.G., Teng, Y.W., Chai, H.P., Wen, Q.Y.: Revisiting the security of secure direct communication based on ping-pong protocol. Quant. Inf. Proc. **10**(3), 317–323 (2011)
21. Makarov, V., Anisimov, A., Skaar, J.: Effects of detector efficiency mismatch on security of quantum cryptosystems. Phys. Rev. A **74**, 022313 (2006)
22. Brassard, G., Salvail, L.: Secret-key reconciliation by public discussion. Lect. Notes Comput. Sci. **765**, 410 (1994)
23. Bennett, C.H., Brassard, G., Crépeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inf. Theory **41**, 1915 (1995)