Design and Simulation of a Quantum Key Distribution Protocol Based on Single-Particle and EPR Entanglement

Leilei Li[1], Jian Li[1(✉)], Hengji Li[1], Chaoyang Li[1], Yan Zheng[1], and Yuguang Yang[2]

[1] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
buptlijian@126.com

[2] College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

Abstract. Based the idea of original "Ping-pong" protocol, an improved "Ping-pong" protocol based on single-particle and Einstein-Podolsky-Rosen (EPR) entanglement is presented. The EPR entanglement is used to detect the eavesdropping and the single particle is used to transmit the information. During the protocol, the sender Alice transmits an EPR entanglement pairs and a single particle to the receiver Bob at the same time. The bit error is caused by the random position of the single particle. In our security analysis, an eavesdropping will cause at least a bit error rate of 16.7%, and the probability of detecting eavesdropping with bit error rate is 50.0%. We also give a simulation which is based on law of large numbers and Monte Carlo method. In our simulation, we use mean square error (the value is 1.8115×10^{-5}) to indicate that the simulation data is approach to the theoretical value. Compared with the original "Ping-pong" protocol, the presented protocol doesn't need the control mode, and it doesn't need to store the quantum state.

Keywords: Single-particle · EPR entanglement · The "Ping-pong" protocol · Security analysis · Monte Carlo method

1 Introduction

Cryptography is the basis of information security, the task of cryptography is to ensure that only legitimate users like Alice and Bob can read a secret message in a secure communication, while unauthorized users like Eve cannot. To accomplish this task, the communication protocol must ensure that only the key can encrypt and decrypt the secret message. In 1949, Shannon proved the one-time pad (OTP) [19] is perfectly secure with equal length of the key and secret message

This work is supported by the National Natural Science Foundation of China (Grant No. U1636106, No. 61472048, No. 61572053).

H. Song et al. (Eds.): SIMUtools 2019, LNICST 295, pp. 278–287, 2019.
https://doi.org/10.1007/978-3-030-32216-8_27

[17], that means the key can protect the secret message during transmission, but how to protect the key during distribution is still a tricky problem. [13,23,27].

Different from the classical communication, quantum communication and quantum cryptography is based on the theory of quantum physics and quantum entanglement which have attracted the interest of researchers in past decade, especially Quantum key distribution (QKD) [1,14,16,18] and quantum secure direct communication (QSDC) [9,21,22,25]. In QKD, the quantum particles is used to transmit the key while the classical bit is used to transmit the secret message. The key is determined until the end of the transmission, and the incompleteness of the quantum bits can be tolerated [4,5,11,20]. In QSDC, not only the key but also the secret message is transmitted in quantum channel, that means every qubits is useful, and QSDC cannot tolerate the incompleteness of the qubits [7,24].

In 2002, Long et al. proposed the first QSDC protocol with EPR entanglement [15]. In this protocol, the method of quantum data block transmission for security based on bit error rate analysis is introduced, before transmitting the secret message, the protocol sends a block of quantum data to make sure whether the quantum channel is security. It's an excellent method of QSDC, but it cannot detect the eavesdropping after starting transmit the secret message.

At the same year, Bostrom and Felbinger presented an excellent two-step deterministic QKD protocol which called the "Ping-pong" protocol [2]. This protocol contains two modes: the message mode is used to transmit the security message while the control mode is used to detect eavesdropper's (Eve) eavesdropping. During the protocol, the sender Alice randomly chooses the control mode or the message mode, means this protocol can detect the eavesdropping during the whole transmission process. But the "Ping-pong" protocol cannot transmit the security message in control mode, that means the more effective of detecting eavesdropping, the less effective of transmitting security message.

Based the idea of the original "Ping-pong" protocol (OPP) [2,10,11], we present an improved "Ping-pong" protocol based on a single-particle and an EPR entanglement which is called TPP. The receiver Bob randomly puts the single-particle in the first, second or third position of the three-particle group, that means only Bob knows the position of the single-particle, but the sender Bob and the eavesdropper Eve not. Eve can only randomly chooses the particle as the single-particle, that means the Eve will caused a bit error rate.

In 2016, we presented a QKD protocol based the idea of the BB84 protocol, which is called MEQKD [10]. In MEQKD, Alice sends two EPR entanglement pairs to Bob at one time, Bob randomly chooses the position of EPR pairs, if there is no eavesdropping, the bit error rate only caused by Bob's incorrect choice, which is the same as the BB84 protocol. But the MEQKD protocol has a higher efficiency of detecting eavesdropping. Compared with MEQKD, TPP only sends three particles at one time, which is one particle less than MEQKD, in other words, TPP is easier to application.

Compared with the OPP, TPP sends one single-particle and one EPR Entanglement every time, in other words, it sends totally three qubits once, which is

more than OPP. The security analysis of TPP is also given, an eavesdropper's eavesdropping will caused at least a bit error rate of 50%. In order to achieve the same detection effect, the TPP needs 30 quantum key bits as the detection sequence, while the MEQKD needs 33 qubits and the BB84 protocol needs 72 qubits [10]. Compared with OPP, TPP can transmit the secret message and detect the eavesdropper at the same time, and TPP also doesn't need to store the quantum states.

We also give a simulation which is based on the law of large numbers and Monte Carlo method, In our simulation, the simulation data (the probability proportion of measurement result) $\hat{p}$ is approach to the theoretical probability proportion p, and mean square error is used to measure the similarity between $\hat{p}$ and p, and its value is 1.8115×10^{-5}. In another word, our theoretical security analysis is correct, TPP can detect eavesdropping effectively.

2 The TPP Protocol

2.1 The Relationship Between the Classical Bits and Quantum Bits

At the beginning of the paper, let's introduce the relationship between the classical bits and quantum bits.

The TPP only uses the *Z-basis*: $B_Z = \{|0\rangle, |1\rangle\}$ and a single-particle $|0\rangle$ and $|1\rangle$. $|+\rangle$ and $|-\rangle$ are unnecessary. Beside, the TPP protocol also uses one of the four Bell states as follows:

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \tag{1}$$

Alice and Bob agree on that there is two unitary operations as follows, just as OPP, when Bob takes a I operation, Alice knows that Bob wants to send the classical bit 0, and when Bob takes a σ_x operation, that means Bob wants to send the classical bit 1.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2}$$

As we know, Eve usually takes an intercept-resend attack between Alice and Bob, according to the Heisenberg's uncertainty principe and no-clone theory [3], Eve needs to re-prepare the qubit particles with her measurement result and resend them to Bob. But the position of the Bell state is only known to Alice, that means Eve can only choose the position randomly, which will cause a bit error rate ϵ. If there is no eavesdropping, ϵ should be 0 [18,26], In the next section, we will analysis the bit error rate ϵ caused by Eve's eavesdropping and we will also proved that the Eve's eavesdropping will always be detected as long as the quantum sequence is long enough.

2.2 A Brief Introduction of TPP

Now, let's introduce the process of TPP and how TPP detects an eavesdropping. A complete process of the TPP protocol can be described as the following 9 steps.

1. Alice wants to send a message to Bob, this message can be the key or the secret message, she firstly encode the message with classical binary and get the classical bit sequence N in order.
2. Bob prepares an EPR pairs and a single-particle to form a three-particle groups and remembers their position as $(1, 2, 3)$, if all the classical bits of N have taken out, then goto the step 9, or goto the step 3.
3. For every three-particle quantum group, the single-particle can be put in the 1st, 2nd or 3rd position. For example, Bob prepares a group $\{|\Phi_{12}^{+}\rangle|\Phi_{12}^{+}\rangle||1\rangle\}$ and sends them to Alice, $|\Phi_{ij}^{+}\rangle$ means the i^{th} and the j^{th} qubits in a group make up a Bell state $|\Phi^{+}\rangle$. Bob records the location information and sends the qubits sequence S to Alice.
4. After Alice received the group, if she wants to send a classical bit 0 to Bob, she takes a I unitary operation on these three qubits. If Alice wants to sends a classical bit 1 to Bob, she can take a σ_x unitary operation.
5. After taking an unitary operation, Alice resends the three qubits group back to Bob.
6. Bob receives the qubits from Alice, he know the position of the EPR pairs. And he takes B_Z measurement on the single-particle, and a Bell measurement on the EPR pairs. If there is no bit error, the bell state's measurement should be always the same when sends $|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\Phi^{-}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, the bell state's measurement should be always different when Bob sends $|\Psi^{+}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and $|\Psi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. If the single particle has been changed, Bob know that Alice sends a classical bit 1; If the single particle has not been changed, means Alice sends a classical bit 0.
7. Only Bob knows which Bell state he sends, so the Bell state can be used to detect the eavesdropping while the single-particle is used to transmit the classical bit.
8. If there is a wrong Bell state measurement result, Bob know there's an eavesdropping, Alice and Bob will intercept this communication and restart a new one.
9. Alice and Bob have confirmed that the channel is safety, they will transmit the remaining keys to obtain the finally key.

Table 1 gives an example that Alice sends a classical bit 0 to Bob without eavesdropper.

If there is no eavesdropping, the measurement result of the EPR pairs should always be the same when Bob sends $|\Phi^{+}\rangle$ or $|\Phi^{-}\rangle$, and the result should always be different when Bob sends $|\Psi^{+}\rangle$ or $|\Psi^{-}\rangle$.

If there is no eavesdropping, the bit error rate ϵ should be 0. In another words, if there is a bit error rate in ideal environment, means there is an eavesdropper, Alice and Bob should intercept the communication and restart a new one.

Table 1. Alice successfully transmits a classical bit 0

Number of the position	1	2	3
EPR pairs that Bob prepares	$\|\Phi_{12}^{+}\rangle$	$\|\Phi_{12}^{+}\rangle$	$\|1\rangle$
Unitary operation that Alice chooses	I		
The state after unitary operation	$\|\Phi_{12}^{+}\rangle$	$\|\Phi_{12}^{+}\rangle$	$\|1\rangle$
The particle that Alice resends	$\|\Phi_{12}^{+}\rangle$	$\|\Phi_{12}^{+}\rangle$	$\|1\rangle$
The measurement result (2 situations)	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$
Detecting eavesdropping	**not exist**		
The classical bits Alice sends	**0**		

3 The Security Analysis and Simulation of TPP with an Eavesdropper

3.1 The Probability of Detecting Eavesdropper

Now let's analysis the probability of detecting the Eve's eavesdropping, Table 2 shows that Eve gets the right and wrong position.

Table 2. Eve gets the right or wrong position of EPR pairs

Number of the position	Right			Wrong		
	1	2	3	1	2	3
EPR pairs that Bob prepares	$\|\Phi_{12}^{+}\rangle$	$\|\Phi_{12}^{+}\rangle$	$\|1\rangle$	$\|\Phi_{12}^{+}\rangle$	$\|\Phi_{12}^{+}\rangle$	$\|1\rangle$
The position Eve chooses	$\surd$	$\surd$		$\surd$		$\surd$
The qubits group Eve resends	$\|\Phi_{12}^{-}\rangle$	$\|\Phi_{12}^{-}\rangle$	$\|1\rangle$	$\|\Psi_{13}^{-}\rangle$	$\|0\rangle$	$\|\Psi_{13}^{-}\rangle$
Unitary operation that Alice chooses	σ_x			σ_x		
The state after unitary operation	$\|\Phi_{12}^{+}\rangle$	$\|\Phi_{12}^{+}\rangle$	$\|0\rangle$	$\|\Psi_{13}^{+}\rangle$	$\|1\rangle$	$\|\Psi_{13}^{+}\rangle$
The particle that Alice resends	$\|\Phi_{12}^{+}\rangle$	$\|\Phi_{12}^{+}\rangle$	$\|0\rangle$	$\|\Psi_{13}^{+}\rangle$	$\|1\rangle$	$\|\Psi_{13}^{+}\rangle$
The measurement result (2 situations)	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
Detecting eavesdropping	**not exist**			**exist**		
The classical bits Alice sends	**1**			**not sure**		

Eve randomly chooses the position of the EPR pairs, that means she has the probability of $p_1 = 2/3$ to choose a wrong position.

When Eve chooses the wrong position to take the Bell measurement, she will randomly gets one of the four Bell state: $|\Phi^{+}\rangle$, $|\Phi^{-}\rangle$, $|\Psi^{+}\rangle$ and $|\Psi^{-}\rangle$. She has the probability of 1/2 to correct the bit error rate caused by wrongly choice of the position. So the probability that Bob gets a wrong EPR pairs is: $p_2 = 1 - 1/2 = 1/2 = 0.5$.

When Bob gets a wrong EPR pairs, the Bell measurement will change, and Eve's eavesdropping will be detected. The probability will be easy calculated [8]: $p_d = p_1 \times p_2 = 1/3 = 0.333$.

3.2 The Bit Error Rate Caused by Eavesdropping

When Eve chooses a wrong position of EPR pairs, the single particle will changed or unchanged with a probability of 50%. That's means when Eve's eavesdropping has been detected, Alice will also has the probability of 1/2 to receive the right particle. So the bit error rate is: $\epsilon = p_d \times (1/2) = 1/6 \approx 0.167$

If Eve's eavesdropping has been detected when the EPR pair isn't entangled or the bit error was found when the single particle is different from the expected result, Alice and Bob know that the quantum channel has been unsafe, the probability of this situation can be easily calculated because the detections in single particle and EPR pair are separated.

$$P = p_d + \epsilon = \frac{1}{2} = 50\% \tag{3}$$

If Alice wants to send the length of n classical bits to Bob, the probability of detecting the eavesdropper is:

$$P_d = 1 - (1 - P)^n = 1 - (\frac{1}{2})^n \tag{4}$$

To detect an eavesdropper with the probability of $P_d = 0.999999999$, Alice and Bob need to compare n = 30 qubits in TPP while 33 key bits in MEQKD and 72 key bits in BB84 protocol [10].

TPP costs more qubits in detecting eavesdropping, but it can detect the eavesdropper in every transmission [12]. In another words, TPP can not only used as a QKD protocol, but also as a QSDC protocol. To get the information, Eve will at the risk of the probability 0.5 to be detected.

3.3 The Information that Eve Obtains

When there is an eavesdropper, the probability of detecting eavesdropping is 1/2. That's to say, Bob has the probability of $P_r = 1 - 1/2 = 1/2$ to get a classical message and the probability of $P_w = 1 - P_r = 1/2$ to get a another classical message. So is Eve.

According to the theory of Shannon information entropy, we can calculate the mutual information that Eve gets [6,15]:

$$I(A, E) = 2 - \left(-\sum_{i=0}^{1} P_i \log_2 P_i \right) = 1 \tag{5}$$

Eve can still gets $(1/2) = 0.5$ of the mutual information which doesn't meet the mutual information relations of privacy amplification. If TPP is used as a QKD protocol, Eve can only gets part of the key, and she cannot read the secret message.

3.4 Simulation Based on Monte Carlo Method

Based on Chebyshev's law of large numbers and Monte Carlo method, we can simulate the proportion of Bob's receive measurement result.

Supposed Bob sends $|0\rangle|\Phi_{23}^{+}\rangle|\Phi_{23}^{+}\rangle$ to Alice, Alice takes an I operation and resends the quantum pairs to Bob, Bob knows the single particle is the first place and he takes an B_Z measurement on the first place, he also takes a Bell measurement on the second and third place. If there is no eavesdropping, the measurement will be 000 or 011 equiprobability. If there is an eavesdropping, the measurement should be one of the measurement result set:

$$\mathcal{S} = \{000, 001, 010, 011, 100, 101, 110, 111\} \tag{6}$$

In our prior security analysis, all the measurement result should be equip probability. So, we can get the theoretical value of the result proportion.

$$\begin{aligned} p_{000} = p_{011} &= \frac{1-P}{n_r} = \frac{0.5}{2} = 0.25 \\ p_{001} = p_{010} = p_{100} = p_{101} = p_{110} = p_{111} &= \frac{P}{n_w} = \frac{0.5}{6} = 0.0833 \end{aligned} \tag{7}$$

In our simulation, the right results' probability distribution should approach to 0.25 when the wrong results' probability distribution should approach to 0.0833.

We used Python to simulate this protocol. The Table 3 shows the simulation result of TPP, in this table, the sum of each column is approached to 1.0, the value of each line is approached to the theoretical value $p_s, s \in \mathcal{S}$. The Fig. 1 shows the proportion of the simulate results.

Table 3. Simulation Result, times means the simulate times, result means the simulate result

Result/times	100	250	500	1000	2000	3000	4000	5000
000	0.1782	0.2470	0.2555	0.2476	0.2574	0.2463	0.2467	0.2476
001	0.0792	0.0797	0.0858	0.0879	0.0920	0.0890	0.0897	0.0882
010	0.1485	0.1076	0.0938	0.0859	0.0790	0.0793	0.0792	0.0788
011	0.2178	0.2191	0.2176	0.2398	0.2429	0.2456	0.2499	0.2539
100	0.0891	0.0797	0.0938	0.0879	0.0900	0.0903	0.0910	0.0870
101	0.0891	0.0966	0.0898	0.0849	0.0825	0.0833	0.0825	0.0802
110	0.0990	0.0916	0.0758	0.0789	0.0715	0.0776	0.0752	0.0766
111	0.0990	0.0757	0.0878	0.0869	0.0850	0.0886	0.0857	0.0880

From Table 3 and Fig. 1 after 5000 times of simulation, The probability distribution of all the results $\hat{p}_s, s \in \mathcal{S}$ is close to stability. The probability that Alice

receives the right result $\hat{P}_r$ and the probability that Bob find eavesdropping $\hat{P}_w$ can be concluded:

$$\begin{aligned} \hat{P}_r &= \hat{p}_{000} + \hat{p}_{011} \to 0.5000 \\ \hat{P}_w &= \sum_{s \in \mathcal{S}} p_s - \hat{P}_r \to 0.5000 \end{aligned} \tag{8}$$

In a word, the theoretical value $p_s, s \in \mathcal{S}$ is approach to the simulate value $\hat{p}_s, s \in \mathcal{S}$. The probability of detecting eavesdropping $\hat{P}_r$ is also approach to $P = 0.5$. We use mean square error MSE to determine the degree of similarity between the simulate value and theoretical value, and set a threshold $\theta = 10^{-3}$. If $MSE \leq \theta$, means the simulation results are very close to the actual results.

$$MSE(\hat{p}) = \frac{1}{n} \sum_{s \in \mathcal{S}} (\hat{p}_s - p_s)^2 = 1.8115 \times 10^{-5} \ll \theta \tag{9}$$

From formula 9, $MSE \ll \theta$, we can conclude that our simulation is close to the actual. In other word, our security analysis is right and TPP is a safe protocol.

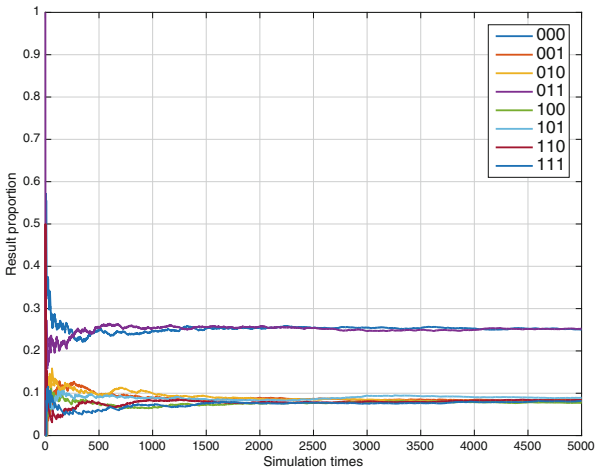

Fig. 1. Two lines above are $\hat{p}_{000}$ and $\hat{p}_{011}$, which is approaching to 0.25; six lines below are the rest of the measurement results, all of them approaching to 0.0833

4 Conclusion

In this paper, we presented an improved "Ping-pong" protocol based on single-particle and EPR pairs which is called TPP. During the transmission, TPP sends one single particle and a pair of EPR. The TPP protocol not only can use as a

QKD protocol, but also a QSDC protocol. Compared with the BB84 protocol, TPP only needs to prepare two kinds of single-particles $|0\rangle$ and $|1\rangle$, but TPP has to prepare another EPR pair.

Compared with the original "Ping-pong" protocol (OPP), TPP doesn't need the control mode, which makes TPP is easier to conduct. What's more, the TPP protocol doesn't need to store the quantum state, making it easy to application.

The security of the TPP protocol is also analyzed. If there is no eavesdropper, the bit error rate ϵ_0 should be 0. The bit error rate will be $\epsilon_1 = 0.167$ if Eve intercepts and resends the quantum bits, and Eve's eavesdropping will also be detected through the EPR pairs with the probability of $p_d = 0.333$. That's to say, there is two ways to detect the eavesdropping, the total probability of detecting eavesdropper is $P = 1/2 = 0.5$.

The information that Eve can get is also analyzed, Eve can at most get $1/2 = 50\%$ information without being detected but she doesn't know which parts she has gotten.

We also give a simulation based on Monte Carlo method and use mean square error (MSE) to estimate the similarity between $\hat{p}$ and p. In our simulation, the simulate value $\hat{p}$ is approach to the theoretical value p and $MSE = 1.8115 \times 10^{-5}$, so we can concluded that we have proved the security of TPP both in theory and simulation.

The TPP protocol is only discussed in ideal environment theory, When come to application, we must face to a difficult problem: how to maintain the entanglement state of quantum. And we should also take the environmental noise into account in the future.

References

1. Bennett, C.H., Brassard, G.: An update on quantum cryptography. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 475–480. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_39
2. BostroM, K., Felbinger, T.: Secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
3. Busch, P., Heinonen, T., Lahti, P.: Heisenberg's uncertainty principle. Phys. Rep. **452**(6), 155–176 (2006)
4. Chang, Y., Zhang, S.B., Zhu, J.M.: Comment on "flexible protocol for quantum private query based on B92 protocol". Quantum Inf. Process. **16**(3), 86 (2017)
5. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**(6), 1192–1195 (2010)
6. Deng, F.G., Gui, L.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**(4), 113–114 (2003)
7. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: Three-party quantum secure direct communication based on GHZ states. Phys. Lett. A **372**(18), 3333–3336 (2008)
8. Howard, R.A.: Dynamic programming and Markov process. Math. Gaz. **3**(358), 120 (1960)
9. Hwang, T., Luo, Y.P., Yang, C.W., Lin, T.H.: Quantum authencryption: one-step authenticated quantum secure direct communications for off-line communicants. Quantum Inf. Process. **13**(4), 925–933 (2014)

10. Jian, L., Na, L., Li, L.L., Tao, W.: One step quantum key distribution based on EPR entanglement. Sci. Rep. **6**, 28767 (2016)
11. Jian, L., Yang, Y.G., Chen, X.B., Zhou, Y.H., Shi, W.M.: Practical quantum private database queries based on passive round-robin differential phase-shift quantum key distribution. Sci. Rep. **6**, 31738 (2016)
12. Li, J., Pan, Z., Zheng, J., Sun, F., Xinxin, Y.E., Yuan, K.: The security analysis of quantum SAGR04 protocol in collective-rotation noise channel. Chin. J. Electron. **24**(4), 689–693 (2015)
13. Liao, S.K., et al.: Satellite-to-ground quantum key distribution. Nature **549**(7670), 43–47 (2017)
14. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050–2056 (1999)
15. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**(3) (2002)
16. Padmavathi, V., Vardhan, B.V., Krishna, A.: Provably secure quantum key distribution by applying quantum gate. Int. J. Netw. Secur. **20**(1), 88–94 (2018)
17. Shannon, C.E.: Communication theory of secrecy systems. M.D. Comput. Comput. Med. Pract. **15**(1), 57 (1998)
18. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
19. Vernam, G.S.: Cipher printing telegraph systems for secret wire and radio telegraphic communications. Trans. Am. Inst. Electr. Eng. **XLV**(2), 295–301 (2009)
20. Wan, L., Huang, Y., Huang, C.: Quantum noise theory for phonon transport through nanostructures. Phys. B **510**, 22–28 (2017)
21. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A **71**(4), 44305 (2005)
22. Wang, C., Deng, F.G., Long, G.L.: Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt. Commun. **253**(1), 15–20 (2006)
23. Wiener, M.J.: Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1989)
24. 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)
25. Yang, Y.G., Teng, Y.W., Chai, H.P., Wen, Q.Y.: Revisiting the security of secure direct communication based on ping-pong protocol [quantum inf. process. 8, 347 (2009)]. Quantum Inf. Process. **10**(3), 317–323 (2011)
26. Zhao, N.P.: Quantum key distribution secure threshold based on BB84 protocol. Acta Phys. Sin. **60**(9), 1358–1364 (2011)
27. Zhou, X.Y., Zhang, C.H., Zhang, C.M., Wang, Q.: Obtaining better performance in the measurement-device-independent quantum key distribution with heralded single-photon sources. Phys. Rev. A **96**(5), 052337 (2017)