Quantum Information Processing (2021) 20:69
https://doi.org/10.1007/s11128-021-03000-8

An improved QKD protocol without public announcement basis using periodically derived basis

Qidong Jia[1] · Kaiping Xue[1,2] · Zhonghui Li[1] · Mengce Zheng[2] · David S. L. Wei[3] · Nenghai Yu[1,2]

Received: 10 April 2020 / Accepted: 14 January 2021 / Published online: 15 February 2021

Abstract
The quantum key distribution (QKD) protocol provides an absolutely secure way to distribute secret keys, where security can be guaranteed by quantum mechanics. To raise the key generation rate of classical BB84 QKD protocol, Hwang et al. (Phys Lett A 244(6):489–494, 1998) proposed a subtle variation (Hwang protocol), in which a pre-shared secret string is used to generate the consistent basis. Although the security of Hwang protocol has been verified in ideal condition, its practicality is still being studied in more depth. In this work, we propose a simple attack strategy to obtain all preparation basis by stealing partial information in each round. To eliminate this security threat, we further propose an improved QKD protocol using the idea of iteratively updating the basis. Furthermore, we apply our improved method to decoy-state QKD protocol and double its key generation rate.

Keywords Quantum key distribution · Derived basis · PNS attack

1 Introduction

Quantum key distribution allows two parties (typically called Alice and Bob) to generate a secret string called secret key in the presence of an eavesdropper, which was first studied by Bennett and Brassard [2] in 1984 (BB84). In principle, QKD offers unconditional security guaranteed by quantum mechanics [16,20,22]. However, non-ideal single photon sources such as weak lasers or parametric down converting sources are used in practical QKD experiments due to the lack of an ideal single photon source.

✉ Kaiping Xue
kpxue@ustc.edu.cn

1 School of Cyber Security, University of Science and Technology of China, Hefei 230027, China

2 Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230027, China

3 Department of Computer and Information Science, Fordham University, Bronx, NY 10458, USA

As a result, such non-ideal sources have to transmit multiphoton signals, and hence, the practical application of the QKD protocol is unable to achieve theoretical security [7]. The famous photon-number-splitting (PNS) attack [5] able to effectively attack in the multiphoton scenario was proposed. In order to resist PNS attack, Lo et al. [18] and Wang [24], respectively, proposed a decoy-state QKD protocol based on the deception strategy introduced by Hwang [10]. However, the key generation rates of these two schemes are still low due to the imperfect single photon source, the low detection efficiency, and lossy/noisy communication channel.

In 1998, Hwang et al. [12] proposed a variation of BB84 protocol, in which public announcement basis (PAB) is not needed. Hwang protocol has a higher key generation rate compared with BB84 protocol due to the adoption of avoiding sifting procedure, and this method has been applied to many researches [14,19,23,26–28]. The security of Hwang protocol has been discussed in ideal condition [11–13], which show that it is robust against individual attacks [12] and coherent attacks [11]. References [13,16] prove Hwang protocol is unconditionally secure in theory. The security of Hwang protocol in practical circumstance has also been studied. The basis is encrypted by the Advanced Encrypting Standard (AES) cipher and transmitted to the receiver through classical channel in Ref. [19]. By avoiding the sifting, the scheme makes BB84 exactly 100% efficient and the scheme is secure as long as AES cannot be broken. Reference [15] discusses the security against PNS attack and proposes a modified protocol based on cipher block chaining. In the improved protocol, the raw secret key is directly used as the input of block cipher mode without eliminating the bit error caused by lossy/noisy channel. Therefore, the secret string used as preparation basis and measurement basis in the next round is different between the sender and the receiver. In other words, the modified protocol proposed in Ref. [15] is indeed not practical. Reference [8] generates basis from a short pre-shared secret key by biasing the basis distribution. This method is interesting and could avoid the sifting phase. Using pseudorandom numbers to generate basis has been proposed to improve the key generation rate in [23]. But this method is also impractical as a single photon source is required.

In this work, we first analyze the security flaw of Hwang protocol in realistic scenario. We point out that an attacker can perform two types of attack strategies. One is similar to the attack strategy on BB84 protocol which aims to get the secret key directly, and the other takes some methods to obtain the initial key which is used to create basis. The first attack has many kinds of implementation, and some famous methods have been proposed to resist it [10,18,24]. We focus on the second attack strategy and propose a simple attack strategy on Hwang protocol. We utilize PNS technology and quantum state measurement technology to steal partial information of the basis in each round in our attack strategy. After about 50 rounds, we can obtain all the information of the basis without being found. To resist this attack, we propose a new protocol which has the same secret key generation rate as Hwang protocol. In our design, by updating preparation basis in each round, the preparation basis stolen by the eavesdropper in the previous round is useless for stealing the preparation basis and secret key in the next round. Therefore, the eavesdropper cannot get the whole information of basis and the security is guaranteed. Besides, we apply the improved method to decoy-state QKD protocol [18,24] to resist the PNS attack that is aimed to steal secret key directly. Furthermore, compared to Hwang protocol, we change the

way to generate basis and our protocol can be implemented as part of a software patch on preexisting QKD devices so that no hardware modification is required. The secret key generation rate of our protocol is twice as much as the rate of the traditional BB84 protocol. The secret key generation rate of our protocol is twice as much as the rate of the traditional BB84 protocol. Besides our protocol is more practical than the protocol proposed in Ref. [15] and more secure than the protocol using pseudorandom basis proposed in Ref. [23].

Furthermore, our method can be applied to the QKD protocols that are based on preparation and measurement [4,6,17]. In these QKD protocols, single photon containing the information of secret key is prepared and sent to the receiver through quantum channel. As the basis used to prepare and measure single photon is chosen randomly, half of the raw key will be discarded in sifting phase. In addition, part of the raw key is used to calculate the bit error rate which helps us find out whether the channel is eavesdropped. In our design, our protocol avoids the sifting phase without affecting the detection of the bit error rate. However, our method cannot be applied to those QKD protocols which are based on entanglement. Because those QKD protocols determine whether there are eavesdroppers by bell inequality [1] which requires that the measurement basis of both sides of the communication must be chosen randomly.

2 Procedure of Hwang protocol and our attack strategy

We give a brief description of Hwang protocol below. We use Z for the rectilinear basis and X for the diagonal basis, in which $\{|0\rangle, |-\rangle\}$ represents 0 and $\{|1\rangle, |+\rangle\}$ represents 1. The complete protocol procedure is as follows:

(1) Alice and Bob pre-share some secure binary random sequence C with length n that is known to nobody by any possible means (by courier or by the BB84 scheme). This random sequence is used in each round to determine the preparation basis and measurement basis.
(2) Alice generates a random secret string

$$S = (s_1^1, s_2^1, \cdots, s_n^1, s_1^2, s_2^2, \cdots, s_n^2, \cdots, s_1^r, s_2^r, \cdots, s_n^r),$$

whose bit length is $N = n \times r$ (r is the number of round) and prepares a qubit string $\bigotimes_{i=1:r, j=1:n} |\Phi_{c_j^i, s_j^i}\rangle$. Each qubit $|\phi_{c,s}\rangle$ is defined as

$$|\phi_{0,0}\rangle = |0\rangle,\ |\phi_{1,0}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$|\phi_{0,1}\rangle = |1\rangle,\ |\phi_{1,1}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

according to C and S. Then, Alice sends the qubit string to Bob.
(3) Upon receiving the qubit string, Bob measures it in the basis of Z or X according to binary string C. The measurement results are the raw key shared between Alice and

Bob. Then, Alice and Bob implement privacy amplification (PA) [3] to generate a secure key that is used to encode classical information by one-time pad [21].

In Hwang protocol, Alice and Bob pre-share a secret string C which is used to determine preparation basis and measurement basis. So, Bob can choose correct basis to measure qubits according to C with no need of public announcement of basis. The confidentiality of the pre-shared string is important as all the qubits are prepared in basis generated by the pre-shared string repeatedly. Once an attacker gets the pre-shared string, he/she can compute the correct basis to measure the single photon signal without introducing additional bit errors between Alice and Bob. Even though we can guarantee that the pre-shared string is absolutely secure, the reuse of the pre-shared string may leak partial information due to the imperfect devices and lossy/noisy channel. Reference [15] has shown that an eavesdropper can get some information about the secret key by performing joint Bell-state measurement and PNS attack. However, in its attack strategy, the eavesdropper does not steal the information about C, but steals the information about secret key generated in the end directly. As shown in this paper, an eavesdropper can only steal partial information about the secret key and the upper bound of the information about the secret key that the eavesdropper can get is about 0.25 in this attack strategy. Thus, we propose a new attack strategy in which the eavesdropper can firstly steal the information about C; then, he/she can steal all the information about secret key without being detected. Furthermore, we use single-photon-state measurement technology in our attack strategy that is easier to implement than joint Bell-state measurement.

The attack aims at recovering pre-shared secret string by eavesdropping and measuring the qubits in channel. As we know, practical light sources may emit more than one photon in a pulse, in which two or more photons have the same state. If we measure these photons in the same measurement base, we will get some information about the base. Here we give an example. Assume that there is a pulse created by practical photon source containing two photons in $|-\rangle$. If we measure them in rectilinear basis and the measurement results are different, we can ensure that these two photons are prepared in diagonal basis. In this case, we get the right preparation basis with probability of $\frac{1}{4}$ as the probability that measurement results are different is $\frac{1}{4}$. If measurement results are the same, the probability that the preparation basis is rectilinear basis is $\frac{2}{3}$ and the probability that the preparation basis is a diagonal one is $\frac{1}{3}$. Therefore, if the measurement results are the same , we can affirm that the preparation basis is a rectilinear one and we get the correct preparation basis with probability of $\frac{2}{3}$. In general, we can get the correct preparation basis with probability of $\frac{1}{4} + \frac{3}{4} \times \frac{2}{3} = \frac{3}{4}$ as shown in Table 1.

If one pulse contains more than two photons, we will have a higher probability to get right preparation basis. Assume that the number of photons in one pulse is m, the probability of getting correct preparation basis is $1 - \frac{1}{2^m}$. If Poisson light source is used and the mean photon number is μ, the average information entropy I that we can get about the preparation basis is:

$$I = -\left(\mathrm{e}^{-\mu}\frac{\mu^m}{m!}\right)\left(1-\frac{1}{2^m}\right)\log_2\left(\left(\mathrm{e}^{-\mu}\frac{\mu^m}{m!}\right)\left(1-\frac{1}{2^m}\right)\right). \tag{1}$$

Table 1 The relationship between the distinct measurement result and its probability

Qubits	Measurement results	Probability
$\|0\rangle, \|0\rangle$	$\|0\rangle, \|0\rangle$	$\frac{1}{4}$
$\|-\rangle, \|-\rangle$	$\|0\rangle, \|0\rangle$ or $\|1\rangle, \|1\rangle$	$\frac{1}{8}$
	$\|0\rangle, \|1\rangle$	$\frac{1}{8}$
$\|1\rangle, \|1\rangle$	$\|1\rangle, \|1\rangle$	$\frac{1}{4}$
$\|+\rangle, \|+\rangle$	$\|0\rangle, \|0\rangle$ or $\|1\rangle, \|1\rangle$	$\frac{1}{8}$
	$\|0\rangle, \|1\rangle$	$\frac{1}{8}$

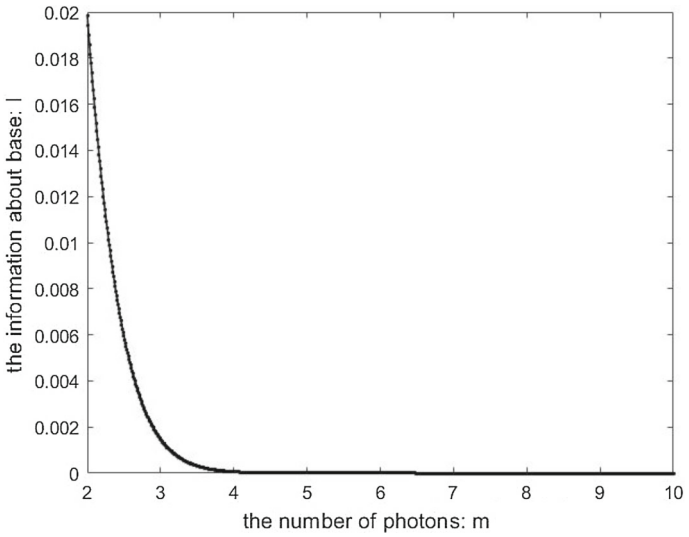

Fig. 1 The relationship between information about preparation basis (I) and the number of photons (m). The photon source is Poisson light source and the mean photon number $\mu = 0.1$

Let μ be 0.1, we conduct a simulation and the result is shown in Fig. 1. We can see that there is at least 2% information about preparation leaked to an eavesdropper in each round. So, after about 50 rounds, the eavesdropper may obtain all the preparation basis that are generated from the pre-shared string directly. So, the eavesdropper is able to obtain the whole pre-shared string by performing this attack repeatedly. Then, the eavesdropper is able to obtain the new secret key generated in posterior rounds without introducing additional bit errors.

Now we present our attack strategy. The detailed steps are as follows:

(1) At the beginning of Hwang protocol, an eavesdropper, called Eve, replaces the lossy channel with an ideal lossless one.
(2) Eve performs a quantum nondemolition measurement and obtains the number of photons in one pulse without disturbing the qubits. If the pulse contains more than one photon, Eve stores them and prepares the same amount of photons using random basis. Then, Eve sends these photons to the receiver.

(3) Eve measures these photons in the same basis and obtains partial preparation basis according to measurement results. If the measurement results are different, Eve can affirm that the preparation basis is a rectilinear or a diagonal one. Then, Eve can measure qubit at the same position in correct basis without introducing additional bit errors.

3 A new protocol and security analysis

To eliminate this security threat, we propose a new method. By updating preparation basis in each round, the preparation basis stolen by the eavesdropper in the previous round is useless for stealing the preparation basis and secret key in the next round. The complete procedure is shown in Fig. 2, and the details are given in what follows:

(1) Alice and Bob pre-share a shifting register filled with security bits, which are generated by implementing classical QKD protocol for several times. We assume that there are N bits in the shifting register.
(2) Both Alice and Bob take the whole contents in the shifting register as the input of KDF to generate the secure bit string, respectively, as

$$C = (c_1, c_2, \ldots, c_i, \ldots, c_n), \tag{2}$$

of length n. Alice and Bob further determine the preparation basis and the measurement basis according to C (0 for the Z basis and 1 for the X basis), respectively. Note that the string C is the output of the KDF, which takes the whole contents of the shifting register as the input rather than directly extracted some bits from it. Thus, the length of the shifting register is not reduced after Step 2.
(3) Alice randomly creates a random bit string

$$S = (s_1, s_2, \ldots, s_i, \ldots, s_n), \tag{3}$$

of length n as secret key and prepares a corresponding qubit string $\bigotimes_{i=1:n} |\Phi_{c_i,s_i}\rangle$ based on C and S and then sends them to Bob via quantum channel.
(4) Upon receiving these qubits, Bob measures them in the basis of Z or X according to the binary string C and get the raw key bits.
(5) Alice and Bob implement sampling, error correction and privacy amplification to obtain the m-bit secret key. If $m = 0$, which means that there could be attackers, Alice and Bob terminate the protocol and throw out these N bits in the shifting register for security reasons. Otherwise, they shift the content in the shifting register to the left by m bits, and the newly obtained security key is placed in the rightmost m bits in the shifting register, respectively. The m bit string shifted from the leftmost of the shifting register is used to derive a part of the session key flow, via a secure derivation algorithm, e.g., KDF-based algorithm, to encrypt the classic information. After implementing this step, the shifting register is updated and its length still remains unchanged.

What follows is the essential part of our protocol:

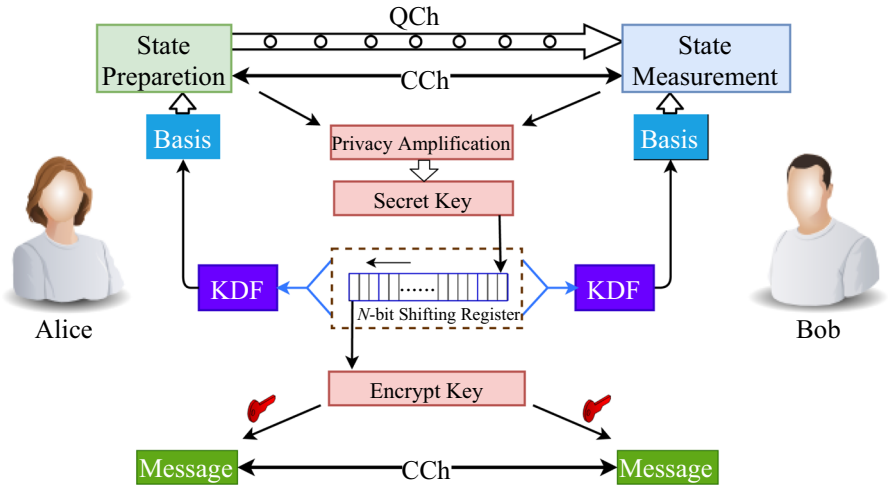

Fig. 2 Procedure of our protocol. QCh represents quantum channel which is used to transmit qubits, and CCh represents classical channel which is used to transmit classical information

(A) *Shifting register*: A bit shifting register structure for storing a large number of secret bits in order. In our protocol, classical QKD protocol is first implemented for several times to fill up the shifting register. Thereby, when a new bit string C with a certain length, e.g., m-bits, is generated, the contents of the shifting register are shifted left by m bits, and the bit string C is placed in the rightmost m bits of the shifting register. Meanwhile, we know there is a bit string of the same length will be shifted from the leftmost of the shifting register, which is used as a part of the secret string. To sum up, the shift register has two main functions, one of which serves as the input of key derive function to create a binary string which is regarded as preparation basis, while the other one is to output a secret string for encrypting classical information.

(B) *KDF*: Key derive function, a cryptographic function used to derive new binary string, though which an arbitrarily long input yields an random output with a specific length. In this protocol, we use a universal hash function which has a good performance in resisting the quantum attacks introduced by quantum computing [9]. To ensure the security of the protocol, the hash function must have the property of preimage resistance which means that the attacker cannot get the input of the hash function based on its output. Besides, as part of the input of hash function updating in each round, we need the hash function to have the property of avalanche effect which ensure that even a tiny little change of input will cause the tremendous change of output [25].

(C) *Secret key*: Random bit string created by QKD protocol. Secret key will be inserted into the shifting register before encrypting classical information. It is regard as new random information to enhance the security of preparation basis.

(D) *Encrypt key*: Encrypting classical information. Encryption key is created by QKD protocol, so it is absolutely secure. When a new secret key is added in shifting register, encryption key will be shifted out from the shifting register to encrypt classical information by one-time pad which guarantees that information is absolutely secure.

Now let us analyze how our new protocol resist the attack strategy mentioned above. Our protocol is able to prevent an eavesdropper from obtaining more information about preparation basis used in the next round and secret key except that the eavesdropper could obtain the information by performing attack strategy mentioned above. The purpose of our new protocol is that the information that the eavesdropper obtains in the previous round cannot help him/her obtain more information about the preparation basis used in the next round. In the first round, preparation basis will be generated as the output of the KDF that takes the whole contents of the shifting register as the input. Then, the standard BB84 protocol is performed without public announcement of basis and m-bit secret key is generated after PA. We insert the m-bit secret key into the shifting register and extract another m bits from shifting register so as to update it. As the shifting register has been updated, preparation basis used in the next round is different from that in the previous round because of the different input of KDF and its features of the design [9]. It is assumed that the eavesdropper may steal 2% information of preparation basis in the first round of our protocol. However, he/she can do nothing with the 2% information, because hash function guarantees that the preparation basis in the next round are not relevant to this information [9]. Then, it is not hard to see that the information that the eavesdropper obtains could not help the eavesdropper get some information about the secret key generated in the current round, because the security of secret key is guaranteed by PA [3]. So, our protocol is more secure and more practical than Hwang protocol and has the same secret key generation rate which is twice as much as traditional BB84 protocol.

Then, we apply the improved method to decoy-state QKD protocol to double its key generation rate and analyze the security. Decoy-state QKD protocol is firstly proposed to resist PNS attack, which uses the decoy state to detect the presence of PNS attacks [18,24]. In the decoy-state QKD protocol, Alice sends two laser pulses with different average photons to Bob with fixed probability, representing the signal state source and the decoy source, respectively. The signal state light source is used to generate the security key, and the decoy-state light source is used to monitor the PNS attack. The light pulses generated by the two different light sources are identical such that eavesdropper is unable to determine whether it belongs to the single state or the decoy state according to the photon number information in the light pulse. Although decoy-state protocol could resist PNS attacks effectively, there is still a security threat to combine decoy-state QKD protocol and Hwang protocol directly. Because the decoy-state QKD protocol is only able to guarantee the security of the secret key, but is not able to protect the pre-shared string from eavesdropping, an eavesdropper can still obtain information about pre-shared string in the complex protocol by performing attack strategy mentioned above. Now, we analyze the security of the well-designed protocol that combines our new proposed protocol and decoy-state QKD protocol.

The decoy-state QKD protocol assumes that the detection efficiency for the signal state, the decoy state, and the bit error rate of the receiver at the receiving end are equal. Under this hypothesis, the lower bound of the single photon signal response rate Δ_1 is given as [24]:

$$\triangle_1 \geq \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(\frac{Q_\nu e^\nu}{Q_\mu} - \frac{\nu^2}{\mu^2}e^\mu - \frac{\mu^2-\nu^2}{\mu^2}\frac{E_\mu e^\mu}{e_0}\right), \tag{4}$$

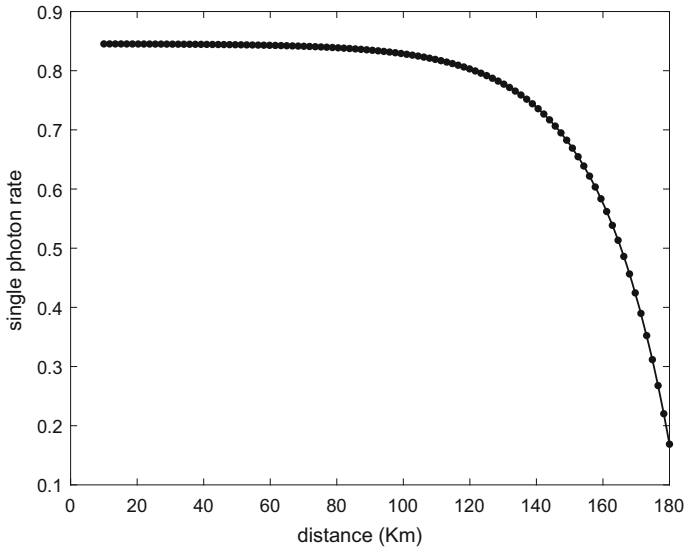

Fig. 3 The relationship between single photon rate and distance. To facilitate analysis, we use Poisson light source in which the average photon number of the signal state $\mu = 0.1$ and the average photon number of decoy state $\upsilon = 0.05$. Besides, we also consider the following experimental parameters: the loss coefficient of the channel is 0.2 dB/km, the detection efficiency of receiver (i.e., the transmittance of its optical components together with the efficiency of its detectors) is 15.0%, and the background count rate is 8.5×10^{-7} and $e_0 = 0.5$

where μ and υ represent the average photon number of the signal state and the decoy state, respectively, E_μ and E_υ represent the bit error rates of the signal state and the decoy state, respectively, and Q_μ and Q_μ represent the detector response rates of the signal state and the decoy state, respectively. We make a simple simulation of decoy-state protocol, and the relationship between the lower bound of the single photon rate generated by the photon source and the communication distance is shown in Fig. 3.

It can be seen from Fig. 3 that when the communication distance is 50 km, the single photon rate is 84.15%, and the corresponding multiphoton rate is 15.85%. According to the worst case, even if all the multiphoton signals are attacked by the eavesdropper, he/she can only obtain 15.85% of the basis information. Because the hash function has a good performance in resisting the quantum attack introduced by quantum computing, we do not have to worry if the eavesdropper can obtain the whole contents of the shifting register through the 15.85% of the basis information. Also, because the newly generated secret key is inserted into the shifting register, preparation basis created in the next round is different from that of the previous round. Furthermore, the hash function guarantees that the eavesdropper is unable to obtain information about preparation basis used in the next round from the information obtained in the previous round. Although, as the communication distance increases, the single photon rate is reduced and more information will be obtained by the eavesdropper, the update of the shifting register that is the input of hash function makes the eavesdropper unable to get the

information about preparation basis in the next round. Thus, our improved method is still secure when applied to decoy-state QKD protocol.

4 Conclusion

We analyzed the actual security feature of Hwang protocol and proposed an efficient attack strategy which is easy to implement. To solve this problem, we modify Hwang protocol and proved that our new design is able to resist the attack strategy mentioned above. In our design, a structure named shifting register and a key derive function able to resist the quantum attack introduced by quantum computing is used in an effective way. Then, to make our improved method more practical, we applied our improved method to decoy-state QKD protocol and discuss the security features. Finally, we come to a conclusion that by combining decoy-state QKD protocol with our improved method, the design is secure and its secret key generation rate is twice as mush as the traditional decoy-state QKD protocol.

Acknowledgements This work is supported in part by Anhui Initiative in Quantum Information Technologies under grant No. AHY150300 and Youth Innovation Promotion Association Chinese Academy of Sciences (CAS) under grant No. 2016394.

References

1. Bell, J.S.: On the Einstein Podolsky Rosen paradox. Phys. Phys. Fizika **1**, 195–200 (1964)
2. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**, 7–11 (2014)
3. Bennett, C.H., Brassard, G., Crepeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inf. Theory **41**(6), 1915–1923 (1995)
4. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**, 557–559 (1992)
5. Brassard, G., Lütkenhaus, N., Mor, T., Sanders, B.C.: Limitations on practical quantum cryptography. Phys. Rev. Lett. **85**, 1330–1333 (2000)
6. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
7. Gottesman, D., Lo, H., Lutkenhaus, N., Preskill, J.: Security of quantum key distribution with imperfect devices. In: Quantum Information Computation, pp. 136 (2004)
8. Grasselli, F., Kampermann, H., Bruß, D.: Finite-key effects in multipartite quantum key distribution protocols. New J. Phys. **20**(11), 113014 (2018)
9. Hamlin, B., Song, F.: Quantum security of hash functions and property-preservation of iterated hashing. Post-quantum cryptography, pp. 329–349. Springer, New York (2019)
10. Hwang, W.Y.: Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. **91**, 057901 (2003)
11. Hwang, W.Y., Ahn, D.D., Hwang, S.W.: Eavesdropper's optimal information in variations of Bennett–Brassard 1984 quantum key distribution in the coherent attacks. Phys. Lett. A **279**(3–4), 133–138 (2001)
12. Hwang, W.Y., Koh, I.G., Han, Y.D.: Quantum cryptography without public announcement of bases. Phys. Lett. A **244**(6), 489–494 (1998)
13. Hwang, W.Y., Wang, X.B., Matsumoto, K., et al.: Shor-preskill-type security proof for quantum key distribution without public announcement of bases. Phys. Rev. A **67**(1), 012302 (2003)
14. Ji, S.W., Lee, S.B., Long, G.: Secure quantum key expansion between two parties sharing a key. J. Korean Phys. Soc. **51**(4), 1245 (2007)

15. Lin, S., Liu, X.F.: A modified quantum key distribution without public announcement bases against photon-number-splitting attack. Int. J. Theor. Phys. **51**(8), 2514–2523 (2012)
16. Lo, H.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050–2056 (1999)
17. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)
18. Lo, H.K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**, 230504 (2005)
19. Price, A.B., Rarity, J.G., Erven, C.: Quantum key distribution without sifting. arXiv:1707.03331 (2017)
20. Renner, R., Gisin, N., et al.: Information-theoretic security proof for quantum-key-distribution protocols. Phys. Rev. A **72**, 012332 (2005)
21. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
22. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
23. Trushechkin, A.S., Tregubov, P.A., Kiktenko, E.O., Kurochkin, Y.V., Fedorov, A.K.: Quantum-key-distribution protocol with pseudorandom bases. Phys. Rev. A **97**, 012311 (2018)
24. Wang, X.B.: Beating the photon-number-splitting attack in practical quantum cryptography. Phys. Rev. Lett. **94**, 230503 (2005)
25. Yang, Y., chen, F., Zhang, X., Yu, J., Zhang, P.: Research on the hash function structures and its application. Wirel. Person. Commun. **94**(4), 2969–2985 (2017)
26. Yang, Yy, Luo, Lz, Yin, Gs: A new secure quantum key expansion scheme. Int. J. Theor. Phys. **52**(6), 2008–2016 (2013)
27. Yuen, H.P.: Direct use of secret key in quantum cryptography. arXiv:quant-ph/0603264 (2006)
28. Yuen, H.P.: Key generation: foundations and a new quantum approach. IEEE J. Sel. Top. Quant. Electron. **15**(6), 1630–1645 (2009)