Front. Phys. China (2006) 3: 251—255
DOI 10.1007/s11467-006-0023-y

REVIEW ARTICLE

WANG Xiang-bin, YING Hao, MA Huai-xing, PENG Cheng-zhi, YANG Tao, PAN Jian-wei

The security and recent technology of quantum key distribution

Abstract In principle, quantum key distribution (QKD) can be used to make unconditionally secure private communication. However, the security of the existing real system for QKD needs to be carefully examined. Actually, the existing experiments based on weak coherent states are not secure under photon-number-splitting attack. Fortunately, the decoy-state method and the entanglement-distribution method can be used to realize the unconditionally secure QKD based on real-life systems with existing technology.

Keywords QKD, security, BB84 method, decoy-state method, photon-number-splitting attack

PACS numbers 03.67.Hk, 03.67.Dd, 42.50.Dv

1 The background

The most direct way for private communication is to let two remote parties first share a secret random binary string (the private key). They can then do private communication by encryption and decryption with the pre-shared string.

However, they should make sure that the pre-shared string is indeed secure, which seems to be a difficult task by any traditional way. For example, one can suppose that the two parties may use a certain secret classical channel to set up the random string. But in classical information, it is impossible to prove the security of any assumed secure channel because an eavesdropper (Eve) may always obtain the information without being detected by the legitimate users. In other words, when the two parties try to do the private key distribution with any assumed secure classical channel, they have no way of knowing whether the distributed key has been attacked, i.e., no classical key distribution can be proven to be secure.

In the 1970 s, mathematicians proposed the so called public key system for private communication. With such a system, the two parties (i.e., Alice and Bob) don't have to pre-share any secret key. With such a system, Bob announces the public key X but keeps the secret key K. If anybody, say Alice wants to send Bob a private message, she can first encrypt P with X, say $E_X(P)$ as a result. Then, Alice sends Bob the encrypted message, which is based on the public key X and the encryption method E. Encrypting a message is a simple task given the public key X. However, to convert $E_X(P)$ to the original message P, i.e., $D_K[E_X(P)] = P$ is assumed to be exponentially complex unless one owns the private key K. Bob is the only person in the world who owns the private key K. However, so far there has been no proof about the complexity of the decryption function of any known public key system. For example, the most well-known public key system, the so called RSA system, is based on the assumed complexity factorizing the product of two huge prime numbers:

$$f(p,q) = p \cdot q$$

The security risk here is that the complexity is an assumption rather than a proven conclusion. Such a factorization can be done easily with quantum computation [1]. This is to say, the security of RSA system is unknown with classical computation while it has been proven to be insecure if Eve has a quantum computer. Moreover, some other classical systems have been proven to be insecure by Wang *et al*. in Shandong University [2—4] even if Eve only has a classical computer. Undoubtedly, this fact raises our concern on the security of the existing classical private communication systems, even if Eve only uses a classical computer.

WANG Xiang-bin (✉), PENG Cheng-zhi
Department of Physics, Tsinghua University, Beijing 100084,China
E-mail: wang_xiangbin@hotmail.com

YING Hao, MA Huai-xing
China Electronic System Engineering Company, Beijing 100039,China

YANG Tao, PAN Jian-wei
Hefei National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Hefei 230026, China

Received April 14, 2006

For the purpose of developing private communication with proven security, Benett *et al*. proposed the concept of quantum key distribution (QKD) in 1984 [5] with a specific protocol that uses 4 different quantum states of a two-level quantum system (qubit). Their protocol was eventually called the BB84 protocol. The security of QKD is guaranteed by principles of quantum mechanics. Starting with the BB84 protocol, we shall review the protocols and security proofs [6—8] of QKD and the technology status [10—15, 28, 29] and security of QKD with real systems [18—21].

2 The BB84 protocol and its security

2.1 The BB84 protocol

In the BB84 protocol [2], a binary bit value is encoded by a 2-level quantum state (such as the photon polarization). For simplicity, we consider the state of photon polarization (see Fig. 1). Both the horizontal and the $\pi/4$ polarizations are for bit value 0; both the vertical and the $3\pi/4$ polarizations are for bit value 1. In the protocol, Alice sends Bob a number of single-photon polarization states that are randomly chosen from the polarization angles of $\{0, \pi/4, \pi/2\ 3\pi/4\}$. This is to say, Alice has randomly chosen two bases: $\{0, \pi/2\}$ basis and $\{\pi/4, 3\pi/4\}$ basis. To each incident photons, Bob measures it in a basis randomly chosen from $\{0, \pi/2\}$ or $\{\pi/4, 3\pi/4\}$. Therefore, Bob has half a probability to do his measurement in the wrong basis, to each of the incident photon. After Bob's measurement, Alice announces the preparation basis of each photon and they discard those results where Bob uses a measurement basis different from Alice's. Bob announces some of the remaining bit values to test the error rate of bit values in each basis. They then discard those bits for test. If they find that the error rate is too high, they abort the protocol otherwise they do error correction and privacy to the remaining bits (the raw key) until they believe that the shortened final key is sufficiently secure. Since the final key is shorter than the raw key, we also call the procedure of error correction and privacy amplification as distillation. The security of the final key from the BB84 protocol can be proven mathematically. The existing security proofs require either subtle physics concepts or complex mathematics or both. For clarity, we first look through the issue intuitively using the principles of quantum mechanics.

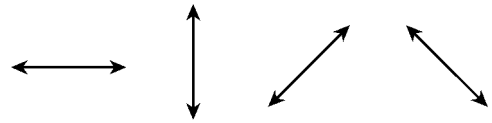

Fig. 1 The 4 different polarization states for the BB84 protocol of quantum key distribution.

2.2 Security of BB84 protocol with a noiseless channel

Suppose there is no channel noise. In such a case, they shall discard the protocol whenever they detect any error of the raw bits in the error test. Eve must observe some of the qubits transmitted from Alice to Bob if she wants to have any information about them. However, since she does not know the preparation bases of each qubits, she is not able to always choose the right basis for the observation. This will, inevitably, cause errors to the raw bits due to the uncertainty principle of quantum mechanics. For example, suppose Eve has chosen the basis $\{0, \pi/2\}$ to observe a certain photon. If that photon has happened to be prepared in the same basis, Eve's observation will cause no disturbance to the state therefore bring no noise. However, if the photon polarization happened to be prepared in basis $\{\pi/4, 3\pi/4\}$, Eve's observation can disturb the state and bring noise. Mathematically, suppose Alice has prepared a polarization state of angle $\pi/4$

$$|\pi/4\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right)$$

and H and V represent for the horizontal and vertical polarizations respectively. If Eve has measured in H, V basis, the polarization state must be collapsed to either the horizontal or the vertical. Eve then sends the qubit to Bob after her measurement. In the suture, if Bob measures it in the right basis, i.e., $\{\pi/4, 3\pi/4\}$ basis, Bob has half a probability to obtain the outcome of $3\pi/4$, i.e., with half a probability Bob obtains a wrong bit. Similarly, if Alice has prepared a polarization of $3\pi/4$,

$$|3\pi/4\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right)$$

If it is measured in H, V basis by Eve, it will also have half a probability to cause a wrong bit if Bob measures it in the right basis. If Eve measures $4n$ of the transmitted photons, on average, she uses $2n$ wrong basis. The probability that she will not cause any error to Bob's result is 2^{-n}. The probability that Eve can pass the error test of BB84 protocol is almost 0.

In practice, the existing technology does not produce a noiseless channel. Therefore the most important problem is the security proof with a noisy channel if n is not too small.

2.3 Security proof of QKD with a noisy channel

Due to the length limit here, we only recall the main ideas of the proof. Let's start with the definition of the unconditional security.

Definition: The probability that Eve has non-negligible amount information about the final key is exponentially close to 0, e.g., 1 in a billion.

In the early literatures, it is often studied intuitively by connecting Eve's information about the raw key and the bit error rate of the raw key. However, such type of study so far has not provided any conclusion on Eve's information about the final key. In particular, since Eve may directly attack the final key, conclusions about privacy amplification method in classical information are not necessarily correct here, unless

there is a proof first.

The first strict mathematical proof of the unconditional security is given by Mayers *et al*. [6] in 1996. The original proof seems to be rather complicated. Here we introduce its main idea using the simplified interpretation given by Koashi [7]: One can use a classical CSS code [8] to distill the final key. The distillation includes error correction, which makes Bob's key and Alice's key be identical; and privacy amplification, which removes any third party's information about the final key. Consider two possible protocols in Mayers proof: the virtual protocol and the real protocol. In the virtual protocol, Bob can obtain k final photons and each of them is in a pure state in basis $\{\pi/4, 3\pi/4\}$. Therefore, nobody can tell the outcome if Bob measures each of them in basis $\{H, V\}$. Consequently, Eve has no information about Bob's final string if he obtains his final string by measuring each photon in $\{H, V\}$ basis. However, in such a virtual protocol, Bib's final string cannot be used as the final key because Alice does not share it. But in the real protocol, Bob can obtain k photons, which are pure states in $\{H, V\}$basis and if Bob measures each of them in $\{H, V\}$ basis, his final string will be identical to Alice's and it is regarded as the final key. Since the density operator of each photons sent from Alice in both protocols are identical, Eve actually cannot distinguish which protocol is actually used. Therefore, even if Alice uses the real protocol, Eve's information about the final key is also almost 0, similar to the case when Alice uses the virtual protocol. This makes the security full proof.

Shor *et al*. [8] greatly simplified Mayers' proof from the viewpoint of entanglement distillation. Suppose Alice and Bob can share k maximally entangled pairs of the state

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|HH\right\rangle + \left|VV\right\rangle\right)$$

They can obtain the final key by measuring the photons in each side in $\{H,V\}$ basis. The outcome must be totally random to any third party. However, given a noisy channel, they cannot share pure entangled states. But they can obtain a fewer number of almost pure entangled pairs with a CSS code, if the channel is not too noisy. Also, it is known that, if the state of those shared pairs is exponentially close to that of pure entangled pairs, Eve's information about the measurement outcome is exponentially close to 0. Moreover, our real purpose here is to obtain a secure final key rather than obtain some high quality entangled pairs, they don't have to really complete the entanglement distillation with a CSS code. In fact, since the phase flips do not change the final key obtained from the measurement outcome in $\{H, V\}$ bases, they don't have to really correct them. They only need certain operations with which they *can* correct those phase flips. These operations are actually the privacy amplification. With this argument, Alice can measure her photons initially and the final key distillation only needs a classical CSS code: Bob first measures every photon and they then distill the classical data as if they were doing the entanglement distillation.

Since Eve's information to the final key is exponentially close to 0, the private communication is secure if they use the key as the one-time-pad to encrypt and decrypt the message.

The final key rate is dependent on the channel noise. For the BB84 protocol, CSS code gives a key rate of:

$$r = 1 - 2h(t)$$

$$h(t) = -t\log_2 t - (1-t)\log_2(1-t)$$

and t is the bit-flip rate of both bases. This key-rate formula requires a noise threshold of 11 % where the key rate hits 0.

2.4 The difference between a real system and an ideal system

We must emphasize that the security proof of BB84 protocol does not necessarily guarantee the security of any real QKD system. Since the intended protocol realized in a real set-up does not necessarily meet all conditions as requested in the security proof of the ideal BB84 protocol. For example, the security proof has assumed the perfect single-photon source for Alice. Since the single-photon source is a very difficult technology, the existing experiments normally uses the weak coherent states or the weak entangled states from parametric down conversion. Now we introduce these two methods.

3 The security of QKD with weak coherent states

3.1 The status of existing experimental results

Since it is difficult to control the photon polarization exactly in an optical fiber, normally we use the phase-coding rather than the polarization. But there are still 4 states as requested by the BB84 protocols. This requires Bob to observe the interference of two beams remotely. The earliest proposal for robust control uses the plug-and-play (PP) method where Bob sends light to Alice first and Alice prepares a BB84 state and sends the attenuated light back to Bob [9]. This method can correct the path difference of two beams automatically. In the PP method, the source and measurement are on the same side (Bob). The intensity of the attenuated light sent from Alice is about 0.1, i.e., each pulse may contain 0.1 photon on average. But the initial light sent to Alice from Bob can be rather strong. The earliest experiment did the QKD over a distance of 67 km [9] with this PP method, with a key rate (raw key) of 160/s and bit-flip rate of 5 %. Later, the PP method is further developed for a distance of more than 100 km. However, the noise caused by the backscattering of bright light has restricted its development for a longer distance. Since the higher bit-flip rate caused by the backscattering will prevent them to distill the final key with a meaningful key rate.

Later, more experiments appeared, which replace the PP method by single-way transmission of weak coherent light,

as requested in the original BB84 protocol. As we have mentioned, the main difficulty for QKD with one-way transmission is in the robust observation of interference of two beams. So far, at least three groups have reported experimental results with one-way light transmission. The experiments done in Cambridge [10, 11] takes active and continuous corrections of the transmission errors for an exact and robust observation of remote interference. They have reached a distance of 122 km with a bit-error rate of 8.9 %. The NEC group uses an integrated-optic interferometer and an improved single-photon detector. They have reached a distance of 150 km for the remote quantum interference experiment [12—14]. The USTC group uses self-correction method to reduce the polarization so that the stability of MZ interferometer is enhanced. They have reached a distance of 125 km with a bit-flip rate of 6 % and the generation rate of 10^3/s for raw key.

However, all these experiments simply replace the single-photon source as requested by the BB84 protocol with weak coherent light without further proof of the security. Actually, because of channel loss, all these results can be insecure if Eve uses the photon-number-splitting (PNS) attack [16, 17].

3.2 The photon-number-splitting attack

In practice, the channel loss for long distance QKD is rather large. For example, given a distance longer than 100 km and an imperfect detector with detection efficiency around 10 %, the overall transmittance is less than 0.1 %. If Alice uses a perfect single-photon source, the BB84 protocol is still secure even with large channel loss. However, the situation is quite different if Alice uses a weak coherent source because Eve can actually obtain full information about the raw key with the PNS attack as it is shown in Fig. 2. For the ease of presentation, we now demonstrate this with the BB84 protocol in polarization space. In the photon number space, the state of a coherent light beam with intensity μ is:

$$|\mu\rangle\langle\mu| = \mathrm{e}^{-\mu}\sum\frac{\mu^n}{n!}|n\rangle\langle n|$$

Here, n is the photon number. The physical meaning of this state is that sometimes the pulse is a vacuum, sometimes it contains only one photon and sometimes it contains 2 or more than 2 photons. The existing experiments set the intensity around

$$\mu = 0.1$$

This shows that the probability that a non-vacuum pulse contains 2 or more than 2 photons is larger than 5 %. After Eve intercepts each photon, she first observes the photon number of that pulse. (This does not cause any disturbance to the polarization.) She blocks it if it contains only 1 photon. But if the pulse contains 2 or more than 2 photons, she splits the pulse, keeps one and sends the other photons of the pulses to Bob through a channel that is more transparent than the one used by Alice and Bob. After Alice announces the bases of each pulse in the protocol, Eve measures her photons in polarization space accordingly. In such a way, Eve has full information of Bob's raw key. On the other hand, since Eve has only observed the photon number and split the multi-photon pulses, these in principle do not have to disturb the polarization. Therefore, Eve's actions here do not bring any disturbance to Bob's bits. Since Eve may have a channel that is more transparent than that for Alice and Bob, Eve's attack here does not decrease the average transmittance as expected by Alice and Bob. In short, to the existing realizations of QKD with weak coherent states [10—15], Eve can have all the information without being detected if she uses the PNS attack [16, 17]. Therefore, "the existing schemes do not offer the unconditional security for the reported distance and signal strength." [17] Although the existing schemes [10—15] can transmit the weak pulse for quite a long distance, they have lost the most important selling point of QKD unless we can solve the problem of PNS attack, or use other schemes.

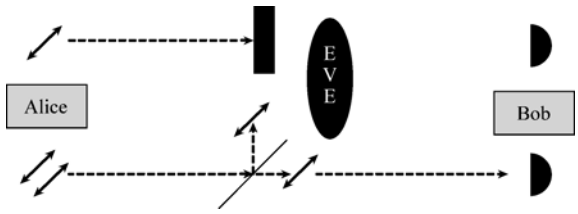

Fig. 2 The photon-number-splitting attack.

Actually, one can obtain the unconditional security with existing technology, by, e.g., either using the decoy-state method with a few different intensities of weak coherent states or directly using weak entangled states in polarization space. The entangled-pair based QKD have been demonstrated in both optical fiber [24—27] and free space [28, 29].

3.3 The decoy state method

This method is to verify the counting rate of those single-photon pulses by randomly changing the intensity of each pulse among 3 different values [18—20]. And then one can use the verified fraction of those raw bits generated by single-photon pulses from Alice to distill the secure final key. The security of the final key here is equivalent to that from a protocol based on a perfect single-photon source. Of course, the decoy-state method is not the only way for secure QKD with existing technology. The so called SARG04 protocol seems to be also quite practically useful [21].

4 QKD with entangled pairs

The security of QKD schemes based on the distribution of entangled pairs is guaranteed by the theory of entanglement distillation. From the theoretical result of entanglement distillation we know that one can always obtain some al-

most-perfect final pairs after distillation provided that the initially shared raw pairs are not too noisy. Measuring in each side of the final pairs will produce the identical final key for Alice and Bob to which Eve's information is exponentially close to 0.

Theoretically, if our purpose is to obtain the secure final key rather than the entangled pairs, we don't have to really do the entanglement distillation. Instead, we can measure the shared raw pairs initially and obtain the final key by distilling the raw bits as the measurement result to raw pairs. In the entanglement-distribution based QKD experiment, the entanglement source is noisy. However, since we only care about the noise of the shared raw pairs, we don't have to worry about the source noise. In particular, the multi-pair events in the source do not change the security. Actually, as has been shown [7, 23], if they use a bipartite state in the protocol and they measure each side in a 2-level space, the entanglement distillation result always applies for the security of the final key.

There are mainly two types of experiments that are based on entanglement distribution. One is to use energy-time entanglement. Gisin's group has completed such an experiment for a distance of 8.5 kilometers [24]. Another one is based on the entanglement in polarization space. Recently, the experimental study of such type of QKD has been very active. In particular, it has been demonstrated in free space. Viena's group demonstrated the polarization entanglement distribution in free space over a distance of 600 m in 2003 [28]. Pan's group at USTC demonstrated the distribution over 13 km [29]. Their entanglement source is produced by the type II parametric down-conversion with BBO crystals. They have successfully produced about 10 000 pairs per second of wavelength 72.2 nm after filtration. They used a large telescope for the detection. This experiment for the first time demonstrated that one can distribute the entangled pairs with existing technology over a distance equivalent to the thickness of the atmosphere. This is an inspiring result for the study of global QKD with satellite-based quantum network [30].

One can refer to Ref. [31] for a complete review of the development of QKD.

5 Summary and concluding remarks

The classical RSA system has been proven insecure if Eve has a quantum computer. Even if Eve is restricted to only use a classical computer, so far none of the classical systems has been proven to be secure. Moreover, Wang's group has shown that some systems have been proven to be insecure under attack with only classical computers. This has further raised our concern for the security of classical systems.

Quantum key distribution can offer unconditional security with strict mathematical proofs, given whatever computer Eve has, including quantum computers. The realization of a QKD protocol does not require any quantum computer or quantum memory. It only requires the preparation, transmission and measurement of a 2-level quantum state.

Although the existing experiments based on weak coherent states [10—15] do not offer unconditional security for the reported distance and signal intensity, we can convert them to the unconditionally secure ones with the decoy-state method [18—20] or other method such as SARG04 [21]. We can also obtain unconditionally secure QKD with entanglement distribution [24—29], which has been demonstrated in free space over a distance of 13 km.

The initial version of this work was published in Chinese [32].

References

1. Shor P., Proc. 35th Ann. Symp. on Found. Of Computer Science. (IEEE Comp. Soc. Press, Los Alomitos, CA, 1994: 124—134
2. Wang X. Y., et al., Efficient collision attacks on SHA-0, Crypto'05
3. Wang X. Y., et al., Finding collisions in the full SHA-1 Collision search attacks on SHA1, Crypto'05
4. Wang X. Y., et al., Collision for some hash functions MD4, MD5, HAVAL-128, Crypto'04
5. Bennett C. H., et al., in: Proc. IEEE Int. Conf. on Computers, systems, and signal processing, Bangalore, IEEE, New York, 1984:175
6. Mayers D., et al., Comput. Mach., 2001, 48:351. Its preliminary version appeared in "Advances in Cryptology-Proc. Crypto" 96, Vol. 1109 of Lecture Notes in Computer Science, New York: Springer-Verlag, 1996:343
7. Koashi M., quant-ph/0507154
8. Shor P. W., et al., Phys. Rev. Lett., 2000, 85: 441, and references therein
9. Stucki D., et al., New J. Phys., 2002, 4: 41
10. Gobby C., et al., Applied Phys. Lett., 2004, 84: 3762
11. Yuan Z. L., et al., Optics Express , 2005, 13: 660
12. Nambu Y., et al., Jpn. J. Appl. Phys., 2004, 43: L1109
13. Kimura T., et al., Jpn. J. Appl. Phys., 2004, 43: L1217
14. Hasegawa T., et al., Proceedings of the 2005 Symposium on Cryptography and Information Security, 2F-3 (in Japanese) Maiko Kobe, Japan, Jan., 2005: 25—28
15. Mo X.- F., et al., Optics Letters, 2005, 30: 2632
16. Huttner B., et al., Phys. Rev. A, 1993, 51: 1863
17. Brassard G., et al., Phys. Rev. Lett., 2000, 85: 1330
18. Hwang W. -Y., Phys. Rev. Lett., 2003, 91: 057901
19. Wang X. -B., Phys. Rev. Lett., 2005, 94: 230503
20. Lo H-K., et al., Phys. Rev. Lett., 2005, 94: 230503
21. Scarani V., et al., Phys. Rev. Lett., 2004, 92: 057901
22. A cin A., et al., Phys. Rev. A, 2004, 69: 012309
23. Gottesman D. et al., Phys. Rev. A, 2001, 63: 022309
24. Ribordy G. et al., Phys. Rev. A, 2001, 63: 012309
25. Tittle W. et al., Phys. Rev. Lett., 2000, 84: 4737
26. Jennewein T., et al., Phys. Rev. Lett., 2000, 84: 4729
27. Naik D. S., et al., Phys. Rev. Lett., 2000, 84: 4733
28. Aspelmeyer M. et al., Science, 2003, 301: 621
29. Peng C. Z. et al., Phys. Rev. Lett., 2005, 94: 150501
30. Zhang J., Physics, 2005 (in Chinese)
31. Gisin N., et al., Rev Mod. Phys., 2002, 74: 145; quant-ph/0101098
32. Wang X. -B., H. Yi, Ma H.-X., Peng C.-Z., Yang T., and Pan J.-W., Physics, 2006, 35: 125 (in Chinese)