DOI 10.15302/J-SSCAE-2018.06.014

Frontiers, Theory, and Practice of Quantum Communication

Wang Xiangbin[1,2]

1. Physics Department of Tsinghua University, Beijing 100084, China
2. Jinan Institute of Quantum Technology, Jinan 370102, China

Abstract: Quantum communication is an important branch of quantum information science. Its two most important applications are quantum key distribution (QKD) and quantum teleportation. QKD can provide unconditionally secure key distribution methods between two spatially separated parties, and its information-theoretical security is guaranteed by the laws of quantum mechanics. QKD has received considerable attention owing to its unconditional security. Reviewing the extensive research on QKD, this paper introduces the main content of QKD and the status of theoretical security proof and real-life security proof with a focus on the decoy-state method and measurement-device-independent QKD. This paper also investigates the problems faced by QKD in the case of severe channel attenuation and introduces the mainstream solution to the problem, i.e., quantum repeaters or satellite relay. The paper points out that the QKD has developed from a theoretical model to an actual system. It also provides useful guidance for subsequent research on QKD.

Keywords: quantum key distribution; unconditional security; practical security; entanglement distribution; quantum repeaters

1 Introduction

Quantum communication is a branch of quantum information science, and it uses qubits (quantum bits) as an information carrier to exchange information. It can overcome the limits of classical information technology in terms of ensuring information security and increasing information transmission capacity. As stated in the paper [1], there are two typical quantum communication applications: quantum key distribution (QKD) and quantum teleportation.

Quantum teleportation is the basic unit of distributed quantum information processing networks. Communication between quantum computers in the future will probably be based on quantum teleportation. In general, the teleported states may be entangled; therefore, quantum teleportation also includes quantum entanglement swapping, which is the basis of quantum repeaters. In addition to the two typical applications mentioned above, quantum communication also involves topics such as quantum dense coding and quantum communication complexity [2,3]. Limited by space, this article focuses on QKD which is also referred to as quantum cryptography.

2 Quantum key distribution

QKD allows spatially separated users to share unconditionally secure keys. This task cannot be accomplished using the classic communication technology. Therefore, QKD is an important research area in quantum communication. The international academic community commonly refers to QKD as quantum communication [4]. The subject classification system of the American Physical Society uses "quantum cryptography" as a sub-

Received date: October 25, 2018; **Revised date:** November 26, 2018

Corresponding author: Wang Xiangbin, Physics Department of Tsinghua University, Professor. Major research field is quantum information science. E-mail: xbwang @mail.tsinghua.edu.cn

Funding program: CAE Advisory Project "Strategic Research on Disruptive Technologies for Engineering Science and Technology" (2017-ZD-10)

Chinese version: Strategic Study of CAE 2018, 20 (6): 087–092

Cited item: Wang Xiangbin . Frontiers, Theory and Practice of Quantum Communication. *Strategic Study of CAE,* https://doi.org/10.15302/J-SSCAE-2018.06.014

entry under “quantum communication” entries. The latest release of the European Union’s (EU) flagship program of quantum technology, *Quantum Declaration*, regards QKD as the main development area of quantum communication. Because QKD is the first practical quantum information technology, when someone mentions quantum communication, they are often referring to QKD.

Existing practical quantum cryptography (QKD) systems mainly use the BB84 protocol, proposed by Bennett and Brassard in 1984 [5]. Different from the classical cryptography system, QKD security is based on the basic principles of quantum mechanics. Even if the eavesdropper controls a channel, QKD allows spatially separated users to share a secure key as long as the eavesdropper cannot break into the legitimate users’ laboratories. The academic community calls this “unconditional security” or “absolute security,” which refers to security with strict mathematical proof. However, this type of security has the following premises: (1) the eavesdropper cannot break into the users’ laboratories; and (2) the principles of quantum physics are the foundation of this security, which requires that the eavesdropper cannot possess techniques that violate the principles of quantum physics but can possess any technology that does not violate the principles of quantum physics, such as computers with arbitrary computing power, including quantum computers. This security of quantum cryptography is independent of computational complexity. Therefore, security is independent of the eavesdropper’s computing power.

The BB84 protocol requires four different single-photon states, such as the polarization states of horizontal, vertical, 45°, and 135°. When the protocol was proposed, there was no security proof, and only intuitive quantum mechanical analyses existed. For example, an unknown quantum state cannot be cloned, and the observation of quantum states inevitably brings disturbances. Briefly, an eavesdropper cannot measure the quantum states transmitted by legitimate users, without leaving any trace. However, there was no strict security proof based on quantitative analysis for a long time. Many studies suggested using the BB84 protocol to distribute a security key. If the noise was too large, the protocol would abort (as noise might be a trace of eavesdropping behavior.) If the noise was too small, the key would be retained or used; however, the protocol could not provide any standards for “big noise” and “small noise.”

3 Strict security proof

From the late 1990s to 2000, a breakthrough was achieved in terms of the security proof of QKD—the strict security proof of the BB84 protocol [6–8]. The authors’ proof can be generally expressed as follows: in the BB84 protocol, if the final key is distilled as the protocol request, the obtained final key is always safe. This security proof requires users to examine the error rate in the QKD process. The error rate is only the users’ own measurement result of the quantum state, and the channel need not be monitored. The authors presented an equation for the final key rate. According to this equation, when the error rate is higher than a certain value, there is, automatically, no final key. With this conclusion, generating a secure key only requires distilling the final key according to the prescribed procedures. If the key can be distilled, it is always safe, and it is not necessary to make a separate security decision on whether to abandon the experiment. The condition required by this security proof is the condition of the BB84 protocol itself: assuming that the users can generate the quantum states required by the BB84 protocol and that the eavesdropper cannot penetrate the users’ laboratories and can only possess the technologies allowed by the principles of quantum physics. Under these premises, the security proof by Mayers is strictly true. How reliable is the strict security proof? The authors’ conclusions can generally be expressed as follows: we have a high probability (e.g., $(1-2^{-50})\times 100\%$) of determining that the possible information leakage of the distilled final key according to the prescribed procedure is less than a small value (e.g., $2^{-50}\times 100\%$). The “very high probability” and “small value” here can be set by the users. The higher the set level, the lower the obtained final key rate.

Later, QKD gradually moved towards practical research, and some security-threatening attacks appeared [9,10]. This did not imply that the above security proof had problems. This threat appeared because the actual QKD system did not fully satisfy the conditions of the BB84 protocol. After 2000, several theories were presented to prove the security of practical systems [11–21]. The security of practical QKD systems has been proven for an increasingly wide range of conditions.

4 Security proof under realistic conditions

4.1 Security under realistic conditions, 1: Imperfect single-photon source and photon-number-splitting attack

A particularly serious problem faced by actual BB84 systems is the photon-number-splitting attack (PNS attack)

DOI 10.15302/J-SSCAE-2018.06.014

[9]. The ideal single-photon source is required to generate the BB84 state. However, a practical ideal single-photon source for QKD does not exist yet. In practical applications, an imperfect single-photon source, usually a weak coherent source, is used. Although a weak coherent source emits a single photon in most cases, there are still some cases where two or more photons in the same quantum state will be simultaneously emitted. The channel has losses, and the loss increases with the distance. The eavesdropper is assumed to have all the capabilities allowed by physics, such as having a lossless or low-loss channel. He can block all single-photon events. When the source simultaneously emits two photons, it can keep one of the photons and send the other to the receiver (through a lossless or low-loss channel) so that the users' keys can be fully known. This is the "photon-number-splitting attack." As long as the channel loss reaches a certain level, the eavesdropper will not expose himself, owing to the implementation of the PNS attack, because he can always cover his attack behavior with channel loss. It was estimated that with the best technology at the time, considering the PNS attack, the actual secure distance did not exceed 20 km. This distance is only the upper bound value, which implies that a key distilled at a distance exceeding 20 km is completely unsafe, and a key distilled at a distance less than 20 km is not necessarily safe. The PNS attack does not require an eavesdropper to attack the equipment inside the laboratory. The PNS attack can be performed anywhere in the channel outside the laboratory. Without a new theoretical approach, users would have to monitor the entire channel to prevent the PNS attack, which causes QKD to lose its dominant advantages. In fact, some well-known quantum communication experiment groups did not conduct QKD experiments until this problem had been solved. The problem was finally solved by the decoy-state method; the protocol using an imperfect single-photon source, such as a weak coherent source, can obtain a secure key that is equivalent to that of a protocol using an ideal single-photon source. The secure distance for QKD has been considerably improved to more than 100 km by developing theoretical methods [11–13]. In 2006, the experimental team from the University of Science and Technology of China and the joint experiment group of the Los-Alamos National Laboratory and National Institute of Standards and Technology (NIST) performed QKD experiments with secure distances exceeding 100 km for the first time using the decoy-state method which overcame the security loopholes caused by imperfect sources. At that time, three independent experimental articles on the same topic (QKD with decoy-state method) were published in the same issue of the *Physical Review Letters* [14–16]. Later, the research team from the University of Science and Technology of China extended the secure distance to more than 200 km.

4.2 Security under realistic conditions, 2: Detector attacks

In practical QKD systems, another possible security risk is concentrated at the terminal. Terminal attacks are essentially not a part of the security definition of the BB84 protocol. As in all classic cryptosystems, users must effectively manage and monitor terminal devices. A terminal attack in QKD mainly refers to an attack on the detectors, which assumes that the eavesdropper can control the efficiency of the detector in the user's laboratory. The representative specific attack method is to input a strong light to "blind" the detector [10], that is, to change the detector's working state. With this method, the detector responds only to what the eavesdropper wants to detect so that the key is fully known without being noticed. Monitoring the working state of the detectors can prevent this attack. Because the eavesdropper must change the property of the detector inside the laboratory, users need to only monitor that and not the entire channel.

Despite this, we are still concerned about deeper security issues due to detector defects, such as fully ensuring the success of monitoring and ensuring the security of imported detectors. In 2012, the "measurement-device-independent" (MDI) QKD scheme was proposed to completely solve the problem [17]. It has been rigorously proven that this method can resist all detector attacks including all known and unknown attacks against detectors. This method does not require the monitoring of detectors. Similar to quantum repeaters, even if the enemy controls the detectors, the security of the protocol will not be affected. Further, the protocol can be performed along with the decoy-state method, which enables QKD systems with imperfect sources and detectors to obtain the level of security equivalent to that of systems with ideal devices. In 2013, the team from the University of Science and Technology of China performed the first MDI-QKD experiment with the decoy-state method and later realized MDI-QKD at a distance of 200 km [22,23]. Since then, the main scientific problem faced by the MDI-QKD method has been obtaining a satisfied key rate. The team from Tsinghua University proposed a four-intensity protocol of MDI-QKD with the decoy-state method, which considerably improved its practical efficiency [20].Using this method, the joint team of Chinese scientists improved the secure distance of MDI-QKD to 404 km [21] and increased the key rate by two orders of magnitude, significantly promoting the practical application of MDI-QKD. The result also showed that the secure key could be obtained with a channel loss of up to 63 dB. This showed that this method with existing imperfect sources could obtain a secure key at a distance beyond what has been provided by the original BB84 protocol [21].The calculation showed that the original BB84 protocol cannot generate the key even if it were to adopt an ideal single-photon source with a channel loss of 63 dB.

Although the actual system has various defects, its security is approaching that of an ideal system with the efforts of theoretical and experimental scientists. As long as this approximation can reach a reasonable degree, the real QKD system can reflect its unique security value.

5 Ekert91 protocol and its security

The main methods of QKD are the BB84 protocol combined with the decoy-state method, or the BB84 protocol combined with the decoy-state and the MDI methods. Chinese scientists also use these methods in their QKD experiments. There are other methods, such as the Bell's inequality verification protocol (later known as the Ekert91 protocol), proposed in 1991 [22]. This method, which is based on entanglement distribution, can verify the security of QKD by verifying Bell's inequality. If the loss is less than a certain value, the security key can be obtained by proving whether Bell's inequality is broken or not. Considering detector attacks, such as the detector attacks method proposed in [10] or other various variant methods proposed in [23], if only the original Ekert91 protocol and no other methods are used, the total loss (including the channel loss and detector loss) needs to be less than 17%, e.g., 1 dB, to ensure the security of the key. However, this security condition is only for the original Ekert91 protocol, not other protocols, such as the BB84. The experiments conducted by the University of Science and Technology of China and other institutions mentioned above are based on the BB84 protocol combined with the decoy-state and the MDI methods, and the security of the obtained QKD results does not need to comply with the conditions of the Ekert91 protocol. In fact, the 404-km MDI-QKD experiment has proven that the protocol and the method it uses can still be secure when the total loss is greater than 60 dB. As mentioned earlier, the MDI method can resist all detector attacks. That is, the existing MDI-QKD experiments can resist all types of detector attacks, including the detector attack methods in [10] and other later variants, such as the attack in [23]. In fact, the attack method in [23] is only one of such detector attack methods; however, it is neither the first nor the most influential one. The earliest known and perhaps the most representative in the field of quantum communication is the detector attack method published as early as 2010 [10]. In this context, MDI-QKD can resist all detector attacks.

The security requirements of the BB84 protocol and the Ekert91 protocol are quite different. Our experiment uses the BB84 protocol with the decoy-state method and MDI methods. In addition, if the Ekert91 protocol is combined with other methods—e.g., implementing non-destructive testing for photon detection at reception to determine the specific time window for photon entrance and including the measurement data that corresponds to only these events—the security condition changes from a total loss of less than 1 dB to a detector loss of less than 1 dB, regardless of the loss of the external channel. Such a change in the security condition has virtually no limit on the secure distance. Compared with the BB84 protocol with MDI, the remote Ekert91 protocol requires extremely difficult experimental techniques (such as non-destructive photon detection.). This is because obtaining the secure key also means completing the loophole-free Bell's inequality experiment for the Ekert91 protocol, while obtaining the secure key cannot provide any results for Bell's inequality for the BB84 protocol with MDI.

Although the Ekert91 protocol and the "Device-Independent" (DI) QKD based on this [24,25] have their unique features in the field of quantum information, these methods require extremely strict experimental conditions. In fact, the existing methods, such as the BB84 protocol combined with the decoy-state and the MDI methods, effectively guarantee the security of quantum communication under practical conditions. This method can be used to generate a secure key; however, it cannot be used to prove whether Bell's inequality is broken or not, because it does not require entanglement.

6 Extension of unrestricted secure distance

Because the quantum communication signal cannot be amplified, the secure distance of various methods mentioned above is limited in practice [26–29]. To overcome this limitation, new technological breakthroughs such as satellite quantum communication are needed. In 2016, the team from the Chinese Academy of Sciences successfully realized the satellite-earth QKD by using the decoy-state method with the Quantum Science Satellite (QSS) [30–32]. They realized a QKD at a distance of thousands of kilometers [30]. Another approach is to use quantum repeaters that would allow quantum communication to operate over unlimited distances in principle. Quantum repeaters are only responsible for the establishment of long-distance quantum channels; however, they do not contain any information on the key. Therefore, the security of a quantum repeater does not need to be protected

DOI 10.15302/J-SSCAE-2018.06.014

by humans. If we view the intermediate measurement station in MDI-QKD from the perspective of quantum repeaters, it is easy to understand why this method can resist all detector attacks, even if a detector is controlled by the enemy, which does not affect the security of the key. In principle, even if a quantum repeater is controlled by the enemy, the secure QKD can be realized as long as the quantum entanglement or the appropriate associated data (virtual entanglement) can be established in the two remote users. As Gilles Brassard and Artur Ekert, the founders of quantum cryptography, have noted, “This will finally achieve the holy grail that all cryptographers have dreamed of for thousands of years.” Chinese scientists have achieved the best results globally in terms of comprehensive performance in the field of quantum memory, which is the core of quantum repeaters [26].

7 Conclusion

To summarize, Chinese scientists have made great achievements in quantum communication technology over the past ten years, as described by many international reviews. They have achieved breakthroughs in the field of practical quantum communication and created extensive records, which have helped close the gap between real and ideal systems and established the security of real systems. Thus, China is undoubtedly the global leader in quantum communication research.

References

[1] Su X Q, Guo G C. Two typical quantum communication technologies [J]. Journal of Guangxi University (Natural Science Edition), 2005, 30(1): 30–39. Chinese.

[2] Yao A C C. Quantum circuit complexity[C]. Palo Alto: IEEE 34th Annual Foundations of Computer Science, 1993.

[3] Yuan Z S, Bao X H, Lu C Y, et al. Entangled photons and quantum communication [J]. Physics Reports, 2010, 497(1): 1–40.

[4] Ursin R, Tiefenbacher F, Schmitt-Manderbach T, et al. Entanglement-based quantum communication over 144 km [J]. Nature Physics, 2007, 3(7): 481–486.

[5] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [C]. Bangalore: IEEE International Conference on Computers, Systems and Signal Processing, 1984.

[6] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances [J]. Science, 1999, 283(5410): 2050–2056.

[7] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. Physical Review Letters, 2000, 85(2): 441–444.

[8] Mayers D. Unconditional security in quantum cryptography [J]. Journal of the ACM (JACM), 2001, 48(3): 351–406.

[9] Brassard G, Lütkenhaus N, Mor T, et al. Limitations on practical quantum cryptography [J]. Physical Review Letters, 2000, 85(6): 1330–1333.

[10] Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination [J]. Nature Photonics, 2010, 4(10): 686–689.

[11] Hwang W Y. Quantum key distribution with high loss: Toward global secure communication [J]. Physical Review Letters, 2003, 91(5): 057901.

[12] Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography [J]. Physical Review Letters, 2005, 94(23): 230503.

[13] Lo H K, Ma X, Chen K. Decoy state quantum key distribution [J]. Physical Review Letters, 2005, 94(23): 230504.

[14] Peng C Z, Zhang J, Yang D, et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding [J]. Physical Review Letters, 2007, 98(1): 010505.

[15] Rosenberg D, Harrington J W, Rice P R, et al. Long-distance decoy-state quantum key distribution in optical fiber [J]. Physical Review Letters, 2007, 98(1): 010503.

[16] Schmitt-Manderbach T, Weier H, Fürst M, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km [J]. Physical Review Letters, 2007, 98(1): 010504.

[17] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution [J]. Physical Review Letters, 2012, 108(13): 130503.

[18] Liu Y, Chen T Y, Wang L J, et al. Experimental measurement device-independent quantum key distribution [J]. Physical Review Letters, 2013, 111(13): 130502.

[19] Tang Y L, Yin H L, Chen S J, et al. Measurement-device-independent quantum key distribution over 200 km [J]. Physical Review Letters, 2014, 113(19): 190501.

[20] Zhou Y H, Yu Z W, Wang X B. Making the decoy-state measurement-device-independent quantum key distribution practically useful [J]. Physical Review A, 2016, 93(4): 042324.

[21] Yin H L, Chen T Y, Yu Z W, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber

[J]. Physical Review Letters, 2016, 117(19): 190501.

[22] Ekert A K. Quantum cryptography based on Bell's theorem [J]. Physical Review Letters, 1991, 67(6): 661–663.

[23] Gerhardt I, Liu Q, Lamaslinares A, et al. Experimentally faking the violation of Bell's inequalities [J]. Physical Review Letters, 2011, 107(17): 170404.

[24] Mayers D, Yao A. Quantum cryptography with imperfect apparatus [C]. Palo Alto: IEEE Symposium on Foundations of Computer Science, 1998.

[25] Vazirani U, Vidick T. Fully device-independent quantum key distribution [J]. Physical Review Letters, 2014, 113(14): 140501.

[26] Yang S J, Wang X J, Bao X H, et al. An efficient quantum light–matter interface with sub-second lifetime [J]. Nature Photonics, 2016, 10(6): 381–384.

[27] Liao S K, Yong H L, Liu C, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication [J]. Nature Photonics, 2017, 11(8): 509–513.

[28] Chen T Y, Liang H, Liu Y, et al. Field test of a practical secure communication network with decoy-state quantum cryptography [J]. Optics Express, 2009, 17(8): 6540–6549.

[29] Chen T Y, Wang J, Liang H, et al. Metropolitan all-pass and intercity quantum communication network [J]. Optics Express, 2010, 18(26): 27217–27225.

[30] Liao S K, Cai W Q, Liu W Y, et al. Satellite-to-ground quantum key distribution [J]. Nature, 2017, 549(7670): 43–47.

[31] Yin J, Cao Y, Li Y H, et al. Satellite-based entanglement distribution over 1200 kilometers [J]. Science, 2017, 356(6343): 1140–1144.

[32] Ren J G, Xu P, Yong H L, et al. Ground-to-satellite quantum teleportation [J]. Nature, 2017, 549(7670): 70–73.