Advances in Economics, Business and Management Research, volume 215
Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022)

Development and Application of Quantum Communication Technology from Economic Perspective

Rundian Zhang

High School affiliated to Xi 'an Jiaotong University
**Corresponding author. Email: 2103274631@qq.com*

ABSTRACT
From the earliest research and study of quantum communication to application and achievement. In recent years, with the continuous development of quantum communication, quantum secure direct communication became an important branch of quantum communication. Quantum secure direct communication uses distinct quantum states of photons as the information carrier in the transmission process to assure the safe and correct direct transmission of sensitive information between communication participants. This paper would introduce the application and development of quantum communication technology. It includes the theory and different protocol of quantum communication. From the earliest research and study of quantum communication to application and achievement. The paper discussed a QKD service interface between the QKD protocol and the security applications. This interface provides a set of common QKD services needed by existing security protocols. The application of quantum communication technology develops the economy to some extent as well. Therefore, governments of all countries will pay more attention to the development of quantum technology and invest more money and manpower costs.

Keywords: *quantum communication, quantum computing, BB84 protocol, quantum satellite, quantum key distribution.*

1. INTRODUCTION

Quantum communication involves many fields, including quantum key distribution network, quantum secure direct communication and quantum secret sharing network. As an important part of quantum information science, quantum communication uses the basic principles of quantum mechanics and completes the communication transmission process through a series of specific measurement methods for quantum states. Among them, quantum key distribution has the widest range of applications, which is the basis and support of other branches and the core content of quantum communication. From 1984, Bennett and Brassard proposed the first quantum cryptography protocol using orthogonal photon polarization state coding transmission. After BB84 protocol, people conducted a lot of research on quantum cryptography. Later, people proposed the B92 protocol network using non-orthogonal quantum state coding to realize quantum key distribution and the E91 equivalent key distribution protocol based on the maximum entangled state of two-particle pairs. Based on these classical protocols, researchers in various countries carried out extensive research and proposed a series of new schemes for quantum key distribution. In recent ten years, quantum key distribution made rapid progress in experiments in optical fiber and free space, and gradually moved towards the road of practicality. From 1995 to 2002, the transmission distance of quantum communication in optical fiber increased from 10km to 30km, and then to 67km. From 2000 to 2007, the transmission distance of quantum communication in free space increased from 1.6 km to 144 km.

2. REVIEW OF QUANTUM COMMUNICATION

2.1. The definition of QKD

Quantum key distribution (QKD) is a technique based on the laws of quantum physics, rather than the computational complexity of the assumed mathematical

problem. Secure cryptographic keys can be proven to be generated and distributed over insecure channels. The quantum error rate of single-photon technology and quantum channels is used to detect potential eavesdropping. A shared secret will be generated on a single photon transmitting a randomly encoded message, i.e. a random string, as the basis for security that measures the probabilistic nature of the photon state. The quantum channel and the classical channel make up the quantum key distribution system. The quantum channel must contain a transparent optical path used only for the transmission of quantum bit elements (individual photons). It is a probability channel. The classical channel can be the traditional IP channel, but according to the system design, it may need to be dedicated and closely linked with the quantum channel to meet the timing requirements.The main drawback of quantum key distribution is that it usually relies on a verified classical communication channel. In modern cryptography, having a verified classical channel means that a symmetric key with sufficient length or a public key with sufficient security level has been exchanged. Authentication and secure communication can be achieved without using QKD. Therefore, QKD completes the work of stream cipher at many times cost.

2.2. BB84 protocol

BB84 is a quantum key distribution scheme developed by Charles Bennett and Gilles Brassard in 1984. It is the first quantum cryptography protocol. The protocol is probably safe and is based on quantum qualities, which means that the information gain can only be at the expense of the interference signal. if the two states that being distinguished are not orthogonal and the channel is authenticated as a common classical channel. It is usually interpreted as a secure private key communication method from one direction to the other for one-time pad encryption. BB84 protocol and its variants are the only known provably secure QKD protocol. The differential phase shift keying of other QKD protocols is promising but has not been proven secure. As shown in figure 1, BB84 protocol consists of four stages. The first stage is that the random-coded single photon flows through the quantum channel and transmits from Alice (transmitter) to Bob (receiver) to establish the initial birth key. Alice maintains the temporary database of each photon sending state. The second stage is screening. Bob sends the detected photons and the list of their basis to Alice on the classical channel, but not their values. The basis is how to measure photons. Photons can be coded as one of two bases. Only one photon can be measured once, so only one fundamental can be applied. If the measurement is made on the proper cardinality, the measured value will be correct. If the measurement is made on the wrong basis, the value will be stochastic. Alice keeps only the correct entries that Bob obtains from her database and sends the modified list to Bob via the classic path. Bob keeps only those items from the modified list. Alice and Bob now have a list of filter keys. The lists have the same size and length, but there may be some errors between them. This is the quantum error rate, which is a sign of tapping. A third stage is used to correct these errors, which we collectively refer to as coordination. The cascade and its variants coordinate errors by exchanging check and error correction codes. It acts as the primary coordination algorithm, and the whole process requires multiple communications between Bob and Alice through the classical channel, ultimately helping to make its list smaller than the filtered list. The fourth stage is privacy amplification, which uses a hashing algorithm to compute the communication between Alice and Bob. Since the set of harmonic bits is random, the resulting privacy amplification set will also be random. The eavesdropper would need to know all or most of the original bits to eavesdrop, otherwise, the eavesdropper would not be able to compute the new set out of thin air. the advantage of QKD is that it can better detect potential eavesdropping that currently exists, as well as other security risks, while it ye can generate and distribute provably secure keys over non-secure channels. It is difficult for QKD to break through the complex key exchange methods or algorithms that are involved in current computing, even if it is not threatened by quantum computers. Secondly, it will not produce a mechanism to beat QKD, because QKD generates random strings for shared secrets, it will get a QKD system and reverse engineer it, but its theory of operation will not. The existing optical media infrastructure will be used by QKD for quantum communication.

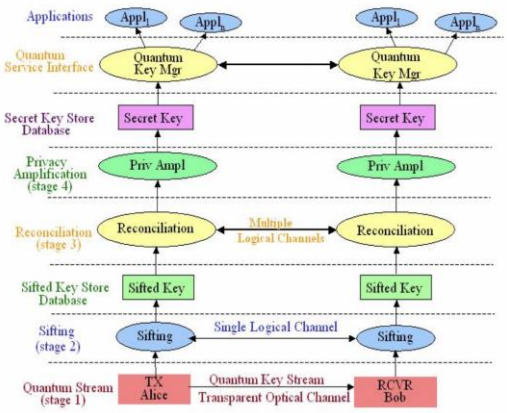

Figure 1. The steps of QKD

3. APPLICATION OF QUANTUM COMMUNICATION

China's quantum satellite enables first totally secure long-range messages. Mozi and Hebei Xinglong ground station established a free space optical link. The transmission efficiency of the satellite-ground quantum key is 20 orders of magnitude higher than that of the ground optical fiber channel at 1200 km communication distance. Recently, the research team optimized the ground station receiving optical system. At Nanshan

ground station, the quantum key generation rate of monorail satellite to ground station increased by about 40 times. In addition, the research team also extends the safe code distance between the satellite and the ground from 1200 km to 2000 km. Therefore, the channel loss is equivalent to the loss between the medium and high orbit satellite and the ground, which lays the foundation for the future application of quantum communication in medium and high orbit satellites. Also the realization of quantum secure communication network covering the world. From 2006 to 2016, great breakthroughs and achievements have been made in the fields of quantum storage, quantum entanglement distribution and quantum teleportation. China ' s quantum communication technology has been leading in the world. These studies and results also confirm the feasibility of exploring space-scale quantum entanglement based on global quantum communication network, and lay a solid foundation for launching quantum satellite Mozi.

According to the website of the University of Science and Technology of China, Pan Jianwei, a member of the Chinese Academy of Sciences and a professor of the University of Science and Technology of China, and his colleagues Zhang Qiang and Chen Tengyun collaborated with Wang Xiangbin and Liu Yang of Jinan Institute of Quantum Technology to break through the field long-distance high-performance single-photon interference technology. By virtue of time-frequency transmission technology and laser injection locking technology, a record 500 km-level field non-relay optical fiber quantum key distribution was realized. Relevant research results are published in the famous international academic journals Physical Review Express and Nature Photonology respectively. The above research results have successfully created a new world record for the longest distance of the on-site optical fiber relayless QKD. The coding rate of the fiber exceeding 500 km breaks the limit of the coding rate limited by the traditional relayless QKD, that is, it exceeds the coding limit of the relayless QKD under the ideal detection device. In the actual environment, it proves the feasibility of the dual-field quantum key distribution (TF-QKD) and paves the way for the realization of the long-distance optical fiber quantum network. Based on the on-site optical cable of Jiqing trunk line', the superconducting detector developed by Ulixing Group of Shanghai Microsystems Institute of Chinese Academy of Sciences has realized 428 km TF-QKD by laser injection locking, and 511 km TF-QKD by time-frequency transfer technology. The quantum non-cloning principle ensures the unconditional security of key distribution, and the non-cloning of the unknown quantum state also makes QKD unable to relay the transmission through optical amplification like the classical optical communication. Therefore, the transmission distance of QKD in practical applications is limited by the fiber loss. However，there might still be some drawbacks of the quantum satellite. For instance, small quantities of quantum satellite have limited abilities to support global communication since most of the countries does not have the quantum communication technology. It’s difficult to form quantum communication system since there are limited numbers of quantum satellite. Therefore the speed of signal propagation is still slow, and is difficult to achieve the desired speed. Also, the security of the system should be questioned. At present, the quantum satellite is still in the experimental stage. As a result, most of the quantum technology could not applied to it including quantum key distribution, quantum computing and quantum quantum secure direct communication. The market potential is huge, and most industries are not applied to quantum satellites. The complexity of technology makes it difficult to popularize to civil use. The threshold of quantum communication is too high, and the technology is still immature. Technical costs should be reduced to apply them to the Internet, cable television, telephone, etc. As more quantum satellite launch to air, the quantum communication would become more efficient and durable.

4. THE FUNCTION OF QUANTUM COMMUNICATION TO ECONOMIC

Quantum technology is far-reaching for economic development. In recent years, the United States, China, Japan, and the European Union have quantum technology that is far-reaching for economic development. In recent years, the United States, China, Japan, and the European Union have invested more and more in quantum technology, mainly reflected in the use of quantum computing, quantum communication, and other technologies. In the future, the application of quantum computing combined with the Internet and artificial intelligence is expected to generate more new industries. With the combination of quantum computing and big data, big data will have stronger statistical ability and complexity, so as to improve its fault tolerance rate. In this context, the stock market trend, financial technology, business decisions, and other aspects will also have a great breakthrough. The development of quantum communication will promote the development of communication industries such as 5G communication technology. Thanks to more secure and efficient quantum technology, online communication will be more frequent in the future, and social media, streaming media, and other industries will have more development possibilities. More people will choose to negotiate online rather than meet offline. Therefore, the Internet-based on quantum communication will become more perfect, requiring more people to participate in the network construction, and the positions on the network will become more. People will find the jobs they want more easily on the

Internet, and the scale of the Internet economy will become larger. In the future, the development of the network economy will depend more on the efficiency, security, quality, and cost of high-tech technology, and the advantage of technology is more likely to have a higher economic growth rate.

5. CONCLUSION

This paper provides a summary overview of the QKD protocol and the related applications of the Mercury satellite. In order to eventually work out a key exchange model and be able to implement it, the research question of how QKD can be integrated into these security applications is now presented based on current relevant theory. The paper also points out that authentication and integrity protection QKD protocol messages can be used in currently existing security protocols, but that they cannot be used until quantum keys exist. Finally, a QKD service interface between QKD protocols and security applications is discussed. The common set of QKD services required by this existing security protocol is provided by this interface. QKD may not evolve into a viable widely deployable technology, but with ongoing research and commercially available systems, it is too early to discard it. In the future, there will be more research and application possibilities for quantum communications.

ACKNOWLEDGMENTS

I am really appreciate to my professor from the university of Yale and my teacher guide because they have offered me substantial support.

REFERENCES

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys, 4 41.1-41.8

[2] Chou C W, Laurat J, Deng H, Choi K S, de Riedmatten H, Felinto D and Kimble H J 2007 Functional quantum nodes for entanglement distribution over scalable quantum networks Science 316 1316-20

[3] R. Perlner and D. Cooper, “Quantum Resistant Public Key Cryptography: A Survey”, Proc of IDtrust 2009, Gaithersburg, MD, Apr. 14-19, 2009.

[4] SECQO, “QKD Network Demonstration and Conference”, Vienna, Austria, Oct 8-10, 2008.

[5] Proc. Updating Quantum Cryptography 2008 Conf., Tokyo, Japan, Dec 1-2, 2008

<http://www.rcis.aist.go.jp/events/uqc2008/>

[6] European Telecommunications Standards Institute (ETSI), Standards work started in Dec 2008 < http://etsi.org/WebSite/homepage.aspx> (select “Committees & Portals”, then select “ISG” and then select “QKD”)

[7] C. H. Bennet and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proc IEEE Intern’l Conf on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179.

[8] K. Inoue, E. Woks and Y. Yamamoto, “Differential phase shift quantum key distribution” Phys. Rev. Lett. 89, 037902, (2002).