The recent progress and state-of-art applications in physics Quantum Communication

Xiaojing Su[1, *, †], Zixuan Zhu[2, †]

[1]Institute of physical science and technology Heilongjiang University, Heilongjiang, China

[2]Department of Optoelectronic Engineering, Lishui University, Zhejiang, China

[*]Corresponding author: 2211414@s.hlju.edu.cn

[†]These authors contributed equally

Abstract. Quantum communication is an emerging interdisciplinary discipline that combines classical telecommunication and quantum mechanics. This paper discusses the recent progress of quantum communication in terms of the basic theoretical framework of quantum communication technology, optical devices, state-of-the-art applications. Based on the analysis, quantum communication technology research hotspots mainly involve quantum key distribution, quantum confidential communication, quantum invisible transmission, quantum entanglement, quantum cryptography, etc., which exhibits an increasingly rich trend. In addition, the limitations of the quantum communication are demonstrated from the perspective of practical applications. Afterwards, the future prospects of quantum communication technology are proposed accordingly. These results reveal that quantum communication applications are promising and are moving toward practicality.

Keywords: Quantum communication, single-photon detection, Quantum Entanglement, quantum cryptography.

1. Introduction

With the advent of the information age, human beings are receiving and sending text messages, video messages and electronic messages all of the time. Information age offer a tool for millions of people to improve their lives, which also brings great changes in various fields, including industrial production, scientific research, and daily life. the transmission rate and security of communication methods have become a topical issue, and the traditional encrypted communication methods have insufficient security and risks. Consequently, the further development of information science will inevitably be based on new principles and methods.

Quantum communication is a new type of communication that uses quantum entanglement effect for information transfer, including quantum key distribution (QKD), quantum teleportation, quantum secret sharing (QSS) and quantum secure direct communication (QSDC) [1]. Thereinto, quantum key distribution is the core of quantum communication and has the widest application range, quantum key distribution takes quantum state as information carrier, uses the principle of quantum mechanics to transmit and protect information, transmits through quantum channel, and establishes shared key between communication parties to realize absolutely secure and confidential communication [2]. Due to the three principles of uncertainty, measurement collapse and no-cloning theorem in quantum mechanics, quantum communication cannot be eavesdropped, and has efficient and secure communication performance [3].

From quantum satellites to quantum computers, quantum entanglement and information security transmission in star and ground, quantum communication technology is not only widely used in the daily life, but also provides communication support for network infrastructure. In addition, it is also feasible to widely applied in finance and commerce, which will bring great changes to the industrial and scientific communities.

In 1984, Bennett and Brassard first introduced the concept of quantum key distribution and provided the first quantum key distribution scheme, namely the BB84 distribution scheme (a single-particle quantum state scheme) [4]. In 1991, Ekert proposed the Ekert91 scheme, which is a distribution scheme based on the maximum entangled state of two particles [5], and these results laid the foundation for the development of quantum cryptography.

The current frontier research directions in the field of quantum communication technology are mainly focused on quantum key distribution, quantum confidentiality communication, creating quantum communication networks, star-ground communication in communication mode and quantum relay technology [6]. Quantum communication technology is developing rapidly and is now relatively mature in both theoretical and laboratory aspects, but some challenges and difficulties have been encountered in the process of application.

This paper summarizes the basic principles, research progress, technical means and applications of quantum communication. The rest part of the paper is organized as follows. The Sec. 2 will briefly explain the principles of quantum communication. Subsequently, the Sec. 3 will introduce the optical devices used for quantum communication. The Sec.4 introduces some of the most advanced applications of quantum communication in recent years, including QUESS and the Beijing-Shanghai backbone. Then, based on related studies, The Sec.5 analyzes the limitations and future prospects of quantum communication technology. Eventually, a brief summary will be given in Sec. 6.

2. Principle of quantum communication

The basic principle of quantum communication is that the two communicating parties first share a code, and then this code is used to encrypt and decrypt the contents of the communication by means of One Time Password (OTP) encryption.

In 1948, Shannon had already demonstrated that the OTP mechanism, if the key is secure, provides unconditional security for confidential communications [7]. The basic process of quantum communication is as follows: the sender, usually called Alice, and the receiver called Bob, create pairs of entangled photons, send one of each pair to Alice and the other to Bob, and combine a particle with an unknown quantum state with Alice's particle. Bob can obtain the same quantum state as Alice by performing the Unitary transformation on the collapsed particle based on the received information (as shown in Fig. 1).

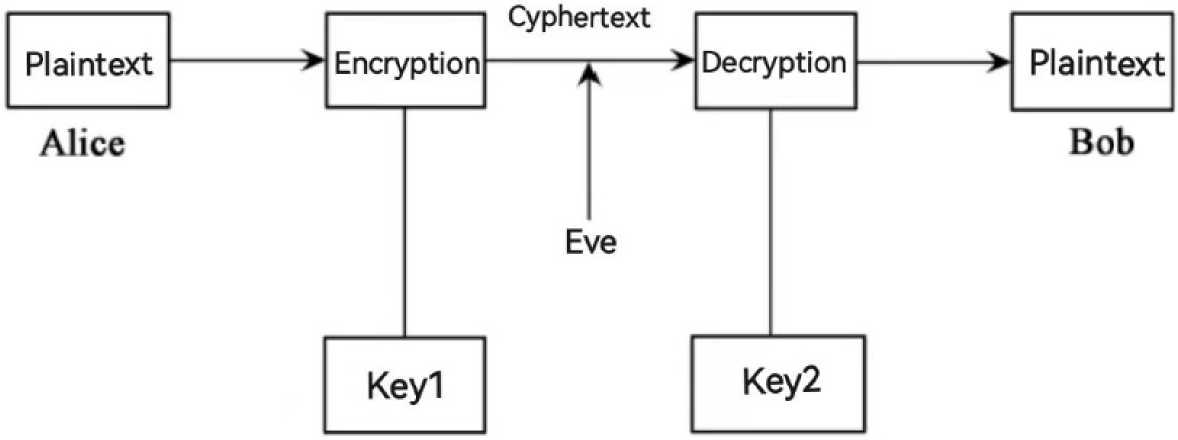

Figure 1. Principle of confidential communication.

Classical information uses bits as the basic information unit, and a bit is a two-state system that can be prepared as one of two identifiable states, in which the concept of quantum states is introduced as the information unit，called qubit. A quantum bit is a superposition of two logical states can be described as:

$$|\psi\rangle = C_0|0\rangle + C_1|1\rangle \tag{1}$$

where $|C_0|^2 + |C_1|^2=1$. Classical bits can be viewed as a subset of qubits [9]. Any two-state quantum system can be prepared into quantum bits, and after the quantization of information is realized, the processing of information is in accordance with quantum mechanical principles. In other words, information transmission has quantum mechanical properties, e.g., uncertainty, no cloning theorem. These properties can be used to accomplish the encryption of quantum state information.

Taking BB84 communication protocol as an example, we will briefly introduce the transmission process of quantum key distribution, because photons have two polarization directions and are perpendicular to each other. Therefore, when the photon source generates a single photon each time, it can be "horizontal and vertical" or "diagonal", in which the polarization direction "↑" is 0 and the "→" is 1. In the diagonal base, the direction of polarization "↗" is 0 and the "↘" is 1. When the measurement base and the photon polarization direction are polarized in the same direction, the result can be obtained. Contrarily, when the measurement base and the photon polarization direction are 45° off, the exact result cannot be obtained (50% probability of 1 or 0 each). After generating a set of binary keys, Alice randomly selects the measurement base for each bit, and sends the polarized photons to Bob subsequently. After receiving these photons, B randomly selects the measurement base for measurement, and finally A and B compare the measurement bases of both sides through the classical channel. The same measurement bases are kept and the different ones are discarded, and the bits that are kept are the final keys [10].

3. Optical devices for quantum communication

3.1 Preparation of single-photon sources

In 2022, a team of researchers from the University of Technology Sydney, University of New South Wales and Macquarie University in Australia developed a method for generating high-purity photons on demand [11]. It allows high-purity single-photon sources to operate at room temperature, helping to advance the application of quantum key distribution (QKD) systems that can be integrated into various types of quantum photonic applications. Examples include confidential communications based on QKD, which uses the quantum properties of light to generate secure random keys with which to encrypt and decrypt data, providing unbreakable encryption for data communications. QKD systems require a powerful and bright light source that emits light in the form of single photons. Previously, most single-photon sources needed to operate at temperatures of several hundred degrees below zero Celsius, which limited their practicality.

3.2 Single-photon detection in quantum key distribution systems

Single-photon detector is an ultra-sensitive photoelectric conversion device, which detects a single quantum of light. The quantum key generation rate is limited by the maximum technical frequency of single photon detector; hence the performance of single photon detector determines the performance of quantum key distribution system. Besides, quantum communication plays a very important role in promoting the development of single photon detection technology, which ensures the absolute security of key transmission through single photon, based on the principle of quantum mechanical inaccuracy, and single photon detector is an important factor limiting the performance of quantum confidential communication system. The single photon detector is an important factor limiting the performance of the quantum confidential communication system. Since light particles are discontinuous light, in practical measurement, a single photoelectron signal is firstly amplified, and the photoelectron signal is identified and extracted by techniques such as digital counting and pulse screening to reach the ultra-sensitive limit. At present, the commonly used single photon detector devices mainly include: avalanche photodiode (VAPD), superconducting single photon detector (SSPD), enhanced photodiode (IPD) and photomultiplier tube (PMT), etc. [12].

Contemporarily, some new single-photon detection methods have emerged, mainly quantum dot-based single-photon detectors, visible photon counters, single-photon detectors based on frequency up-conversion technology, superconducting single-photon detectors, etc. At present, researchers are focusing on two aspects: 1) improving and optimizing the peripheral control drive technology of the detectors in order to increase the detection rate; 2) developing and developing photodetectors with new structures of high sensitivity in order to increase the detection efficiency.

3.3 Applications of quantum entanglement

Quantum entanglement technology is an important development direction of the new generation of quantum technology, which has significant application prospects in information communication and encrypted transmission. Quantum invisible transmission needs to be built on the basis of classical physical channels in order to be realized, and quantum invisible transmission uses quantum entangled states as channel channels, using quanta as carriers, to transfer information from one place to another. Quantum secret sharing was proposed by Hillery and three other scientists in 1999 to share a key among two or more users [13]. Quantum dense coding was proposed by Bennett and Wiesner in 1992, using quantum entanglement to enable the dense coding of information from two particles by transmitting one particle [14].

4. State-of-art application

4.1 Quantum Experiments at Space Scale (QUESS)

In 2016, the “Micius” quantum science experiment satellite was successfully launched (as depicted in Fig. 2). This satellite is the world's first space-scale quantum science experiment satellite. Its main scientific objectives are diverse. To be specific, it will conduct high-speed quantum key distribution experiments with the help of satellite platform, as well as conduct wide area quantum key network experiments on this basis with a view to achieving a major breakthrough in the practicalization of space quantum communication. In addition, it is expected to conduct quantum entanglement distribution and quantum invisible transfer experiments at the space scale, and to carry out experimental research on the completeness test of quantum mechanics at the space scale [15].

The quantum satellite project is operated by the Chinese Academy of Sciences，this experiment will attempt to demonstrate the quantum key distribution between the Xinjiang Observatory and the Xinglong Observatory, and in addition, QUESS will test Bell's inequality at a distance of 750 miles and teleport photon states between Ali, TAR and the satellite.

Figure 2. QUESS was successfully launched [16].

4.2 Jing-Hu (Beijing-Shanghai) Trunk Line

In 2017, the world's first quantum communication backbone was opened between Beijing and Shanghai, marking the formation of a prototype wide-area quantum communication network. The "Jing-Hu Trunk Line" is a quantum communication network connecting Beijing and Shanghai, with a total length of more than 2,000 kilometers, and is connected to the "Micius" through Beijing, which is the basis for the realization of a quantum confidential communication network with global coverage. During the construction of the trunk line, the Jing-Hu trunk line team has broken through a series of key engineering technologies such as high-speed quantum key distribution, high-speed single photon detection, trusted relay transmission and large-scale quantum network control and monitoring [17]. After its completion, the Beijing-Shanghai backbone has been tested for more than two years for stability and security. The relevant research proved that the Beijing-Shanghai trunk line can resist all known quantum hacking schemes, the key rate of the whole line is greater than 20 kbps, and the key distribution volume of the network can support more than 12,000 users at the same time.

5. Problems and Prospects of Quantum Communication Technology Development

From the 1980s to the present, quantum communication has been developed rapidly, but there are still the following technical difficulties in optical preparation that need to be solved. First, the development of communication technology there is a weak coherent light source sexual security problem, the existing experimental systems mostly use coherent state laser weak pulse instead of the ideal single photon source, so there will be security risks, eavesdroppers can get all the password through the channel of photon separation technology. The second is the quantum entanglement problem. This problem is mainly manifested in the key distribution transmission, which largely affects the entanglement quality. As mentioned in previous research materials, in order to solve this problem can be considered to take quantum relay scheme, but need to pay attention to the implementation of the scheme using the entanglement purification technology, quantum storage technology is limited, there may be a mismatch quantum key distribution system situation. Third, the rate, anti-jamming performance has limitations. Quantum communication technology in the existing conditions, far from the classical communication system in the communication rate, anti-jamming and other aspects of performance. Fourth, the communication distance is limited by the problem, due to quantum communication technology of quantum channel loss is too high and quantum communication channel efficiency is reduced, these will lead to long-distance communication is limited.

Prospects for the application of quantum communication technology Quantum communication has shown its value in a wide range of areas, from defense and military, deep sea and space, to national economy, science, education and health. From theoretical to experimental, quantum communication is gradually becoming more and more practical. Quantum key distribution (QKD) technology has been developed and matured over a long period of time, and is slowly moving towards a trial period, which is an important manifestation of the development of quantum communication technology towards practicality. At present, Quantum Stealth Transmission (QT), Quantum Secure Direct Communication (QSDC) and Quantum Secret Sharing (QSS) are among the frontier theories of quantum communication and have been explored and experimented by scientists.

6. Conclusion

In summary, this paper discusses optical devices and the state-of-art applications for quantum communication. Specifically, this paper begins with a brief explanation of the theory of quantum communication technology, including the principles of quantum mechanics, quantum communication technology, secrecy technology and key. Moreover, this paper discusses optical devices from the perspective of quantum communication. It is worth noting that there are still some shortcomings in the application of this technology, which are problems that need to be solved in further research and practice, including single-photon source implementation bottlenecks, single-photon detectors, quantum entanglement etc. After the above issues are addressed, the development and application of quantum communication technology can be pushed to a higher level. In the future, though there are many problems in the development of quantum communication technology, it still has relatively large transmission capacity, high efficiency and security features, and has great application in military security communication, highly confidential important information transmission and life communication. Overall, these results offer a guideline for the development of quantum communication technology in the new era.

References

[1] Deng Fuguo. Research on quantum communication theory [D]. Beijing: Tsinghua University, 2005.

[2] Xu BJ, Liu WL, Mao Jun Q, Yang Y. Research on the current situation and problems faced by the development of quantum communication technology [J]. Communications Technology, 2014, 47(05): 463-468.

[3] Li Chuanfeng. Advances in Quantum Information Research [J]. Progress in Physics. 2000, (04): 407-431.

[4] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[J]. arXiv preprint arXiv:2003.06557, 2020.

[5] Ekert A K. Quantum Cryptography and Bell’s Theorem[J]. Quantum Measurements in Optics. Springer, Boston, MA, 1992: 413-418.

[6] Lin Youbin. Applications and Prospects of Quantum Communication Technology [J]. Electronic Technology. 2022, 51(02): 18-19

[7] Shannon C E. A mathematical theory of communication[J]. Bell Syst Techn J, 1948, 27: 379-423, 623–656.

[8] Xue P., Guo G C. Quantum communication [J]. Physics, 2002, (06): 385-391

[9] Guo G C. Introduction to Quantum Information [J]. Physics, 2001, (05): 286-293

[10] Imre S. Quantum communications: Explained for communication engineers[J]. IEEE Communications Magazine, 2013, 51(8): 28-35.

[11] Wen, P., Tiwari, P., Mauthe, S. et al. Waveguide coupled III-V photodiodes monolithically integrated on Si [J]. Nat Commun 13, 909 (2022).

[12] Ma Zicheng. Application of single photon detection in quantum communication[J]. Communication World, 2017(21): 20-21.

[13] Hillery M, Bužek V, Berthiaume A. Quantum secret sharing[J]. Physical Review A, 1999, 59(3): 1829.

[14] Bennett C H, Wiesner S J. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states[J]. Physical review letters, 1992, 69(20): 2881.

[15] Peng CZ. Pan JW. Quantum science experiment satellite-“Micius”[J]. Bulletin of Chinese Academy of Sciences. 2016, 31(09): 1096-1104

[16] Zhang Wenzhuo. The epoch-making quantum communication--Written to the world's first quantum science experiment satellite “Micius” [J]. Physics, 2016 ,45(09): 553-560

[17] Wu Changfeng. Quantum confidentiality communication “Beijing-Shanghai trunk line” has the opening conditions [J]. China Strategic Emerging Industry, 2017, (37):97