# The Development and Implementation for Encryption of Quantum Communication

Tianhong Wu*

Shanghai Foreign Language School affiliated to SISU, Shanghai, China

* Corresponding Author Email: caishuqi@shisu.edu.cn

**Abstract.** Contemporarily, the quantum world is a new area in physics which has been widely explored. With the contributions of the scholars, the whole structure of the quantum world might cause great revolution on all the knowledge in various fields including teleportation, computing etc. Among various applications, quantum teleportation has attracted plenty of researchers, where remarkable results have been achieved based on the advanced facilities and proposed concepts. For quantum teleportation. The encryption is the key of the process. On this basis, the main topic of the whole paper will demonstrate the possible encryption concluded from two main communication methods. To be specific, the history and basic notes of quantum physics will be recalled primarily. In addition, the principle of encryption and applications of quantum communication will be discussed. Moreover, the state-of-art applications and implementations for encryption of quantum communication will be clarified. These results shed light on guiding further exploration of the encryption process of quantum communication.

**Keywords:** Quantum Communication; Encryption; Quantum Physics.

## 1. Introduction

For thousands of years, human has changed the way of communication again and again. It started with letters sent by mail men, and then went on with underground wires connecting telephones or teleport machines far from each other. The information age has brought us internet, smartphones and PC which allow human to enjoy convenient, wireless communications with the help of the router. The basic theory is electromagnetic waves containing codes representing the information [1-3]. The speed is getting much faster from days to seconds. However, the problem is still the speed of electromagnetic wave. Even though concept like 5G has improved the network efficiency as much as possible, there is still time can't be squeezed, and if the distance between two terminals gets far enough, the delay will bring about more inconvenience with the time added from milliseconds to minutes [4, 5]. Contempoaraily, Quantum communication is a feasible path.

Along with the researches published in 20th and 21st century. The existence of Quantum Physics has been proved to be true and is finding its way getting into our sight [6, 8]. Max Planck first mentioned the existence of quantum theory in 1900. He guessed that the energy existed in the universe is not continuous. He thought that it is possible to divide energy flow into single particles, and all energy in the universe is presented as a multiple of the basic unit. The Planck constant is placed in the function Ek=hv-Φ, and he proved it with the spectrum measuring the black body. Then, in the 1920s, Werner Karl Heisenberg posted his Uncertainty principle proving that the uncertainty of particle's position multiplied by the uncertainty of particle's energy must be greater than or equals to the Planck constant. Marked as $\Delta x \Delta p \geq h/4\pi$. While at the same decade, Erwin Schrodinger published his discovery inspired by Louis Victor Duc de Broglie's essay. He found the equation which can calculate the potential function, since the quantum is considered a type of wave particles, so it must have the same characteristics that other wave particles have. He has a famous explanation of quantum's existence called Schrodinger's cat. Elbert Einstein is opposed to quantum theories, and in order to prove it wrong, he published his Hidden variable theory, coping with his famous words that 'God does not play dice with the universe.' He thinks that there must be a code hidden inside the particles which decides the states of the particle itself. In 1964, John Stewart Bell published his new theory, Bell' theorem, proving that some particles in the universe can travel faster than the light. Also

he listed the Bell inequality, which marked as $Pxz - Pzy \mid \leq 1 + Pxy$. If this equation is correct after calculations, then it will also prove that Einstein's hidden variable theory is correct. As for the recent progress in quantume physcis, Alain Aspect, John Clauser and Anton Zeilinger managed to prove that the Bell inequality is incorrect, with the help of their modern equipment used in the photon experiment [8].

In recent years, quantum communication is one of the advanced topics, which will be detailly discussed in this paper. The rest part of the paper is organized as follows. The Sec. 2 will introduce the principle of quantum communication as well as the encryption protocol. The Sec. 3 will demonstrate the applications, state-of-art facilities as well as prospects. Eventually, a brief summary will be given in Sec. 4.

## 2. Principle & Encryption Protocols

Quantum communication technology aims to encode, transmit, process and decode information by means of quantum states, especially the distribution of quantum keys by means of quantum states (single photon states and entangled states). Among the many ways to communicate, quantum communication technology has been called the "most difficult to break" encryption technology. The greatest advantage of quantum communication lies in its secrecy. Many economic, scientific and military information are highly confidential, so quantum communication has no shortage of potential users. The security of quantum communication is based on the fundamental principles of quantum physics. As the smallest particle of light, each quantum of light has two characteristics: indivisibility and imprecision reproduction when transmitting information. If eavesdropping exists, it will be detected and avoided by the information sender. Therefore, quantum communication ensures the security of information [9-11]. A sketch of the principle is shown in Fig. 1.

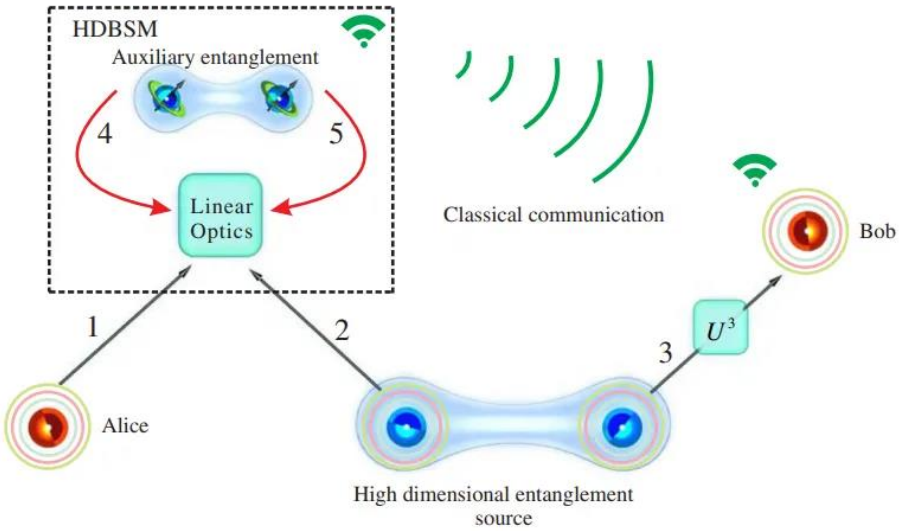


**Fig. 1** A sketch of quantum communication.

While before the Bell's equation is proved, ideas of testing the capability of Quantum Communication had started. Two main type of quantum communication is quantum key distribution and quantum teleportation. The first type of quantum communication was put forward by Charles H Bennett. He raised two main protocols, BB84 and B92 (seen from Fig. 2). In BB84, the communication process is separated into two channels. A use the photon channel to send a code composed of 4 different types of photons representing 0 and 1, and B observe it with 2 measurement bases, and each of the base can measure 2 out of 4 types of photons. Then there is a possible rate at about 50% that B would use the wrong base. Then B would send the result back to A through the normal channel, and A would seek out the correct ones. After sending it back to B, B would pick

randomly from the correct ones and send it back to A again [12]. However, this time A would delete the picked ones sent by B from the correct samples which A had picked out, and the rest ones would compose a new key code. B92, however, need only 2 out of 4 photons, and B is the one to decide what should be reserved. It needs only one channel to communicate, and the only problem is the diversity of photons.

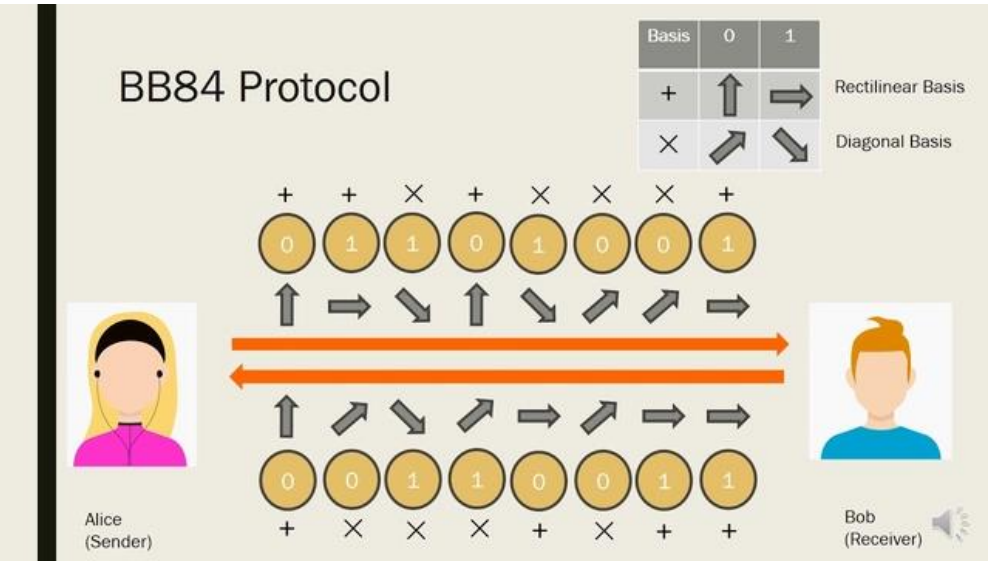


**Fig. 2** A sketch of BB84 Protocol of quantum communication.

The second method, known as the quantum teleportation, is a new type of quantum communication discoveredby Pan Jianwei, who has recently succeeded in Multi-degree-of-quantum teleportation. It shares a pair of particles which is in Bell status, and the information is transported to the receiver by quantum channel, the difference between this method and the key distribution method is that the teleportation doesn't need any normal communication channel, since the particle on the other side would represent an upside downed message (seen from Fig. 3). However, such techniques can be used in computer chips. The possible way of a secured message sending using quantum key distribution combined with quantum teleportation. It is assumed that the quantum teleportation channel is functioning well, and it has been spied on. It is possible to place more than one teleportation channel in the device, which means the receiver can receive quantum information from muti channels at the same time. However, before the message is transported, an extra quantum channel and a normal channel is needed for key making. One can make a key using BB84 protocol, and the result turned out to be a code composed with '0' and '1'. This time, the code is not going to be an encryption of normal channel message. One can have same amount of quantum channels as the amount of the numbers in the code do. '0' represents a closed channel, and '1' means that the channel on the position is opened for exact message transportations.

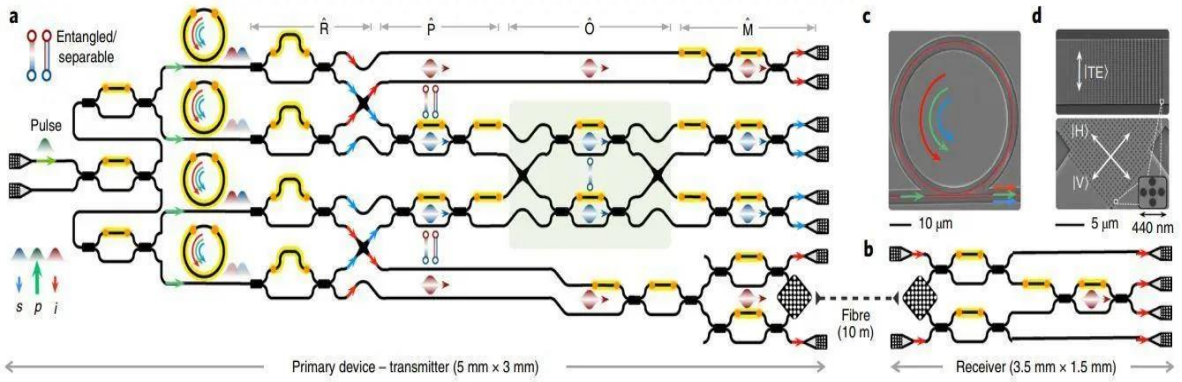


**Fig. 3** A design of entanglement.

## 3. Applications, State-of-art Facilities, Limitations & Prospects

All walks of life, including the financial industry, are expected to rebuild a new application platform based on quantum key technology to protect information security. Taking the financial industry as an example, the core process of communication encryption and decryption processing using quantum key technology in the future is envisaged as follows.

- The information sender and receiver apply for registration with the quantum key distribution agency in advance.
- Before sending the information, the information sender requests the quantum key distribution institution to obtain the one-time quantum key in real time.
- The quantum key distribution mechanism calls the service provided by the communication satellite in real time to realize one-time random key exchange between the information sender and receiver.
- The sender uses the key to encrypt the message text using the traditional symmetric encryption algorithm.
- The ciphertext is transmitted to the receiver through the traditional channel.
- The receiver uses the same key for decryption.

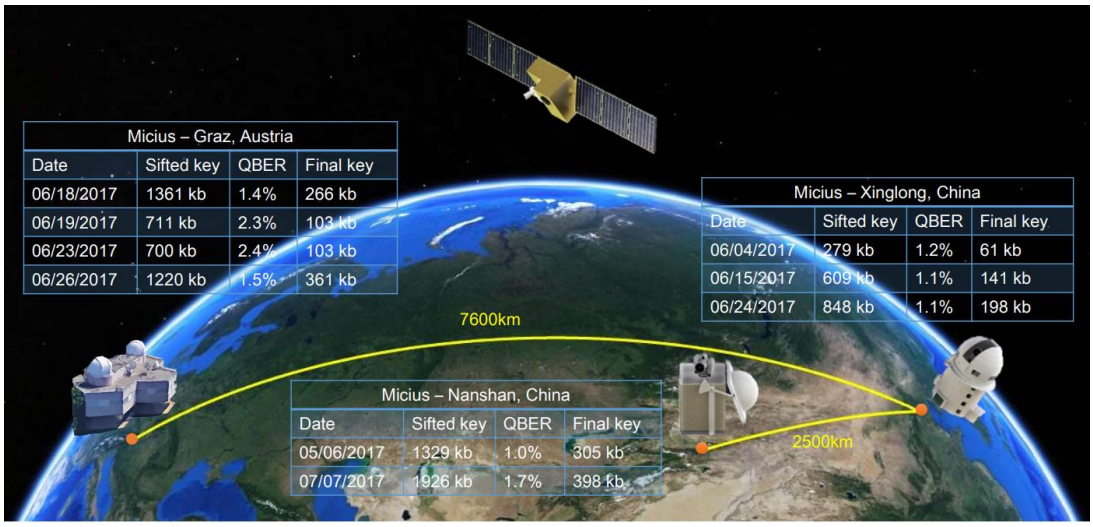


**Fig. 4** A sketch and parameters of Micius.

The Micius satellite project (seen from Fig. 4) is under the general charge of the National Space Science Center of the Chinese Academy of Sciences (Space Center for short). The satellite is one of the first batch of scientific experiment satellites of the strategic Pilot science and technology Project of Space Science of the Chinese Academy of Sciences [13]. Its main scientific objective is to carry out satellite-earth high-speed quantum key distribution experiment with the help of the satellite platform. On this basis, the experiment of wide-area quantum key network is carried out in order to make a breakthrough in the practical application of space quantum communication. Experiments on quantum entanglement distribution and quantum teleportation are carried out at space scale, and experimental studies on the completeness of quantum mechanics at space scale are carried out [14]. The typical encryption results are shown in Fig. 5.

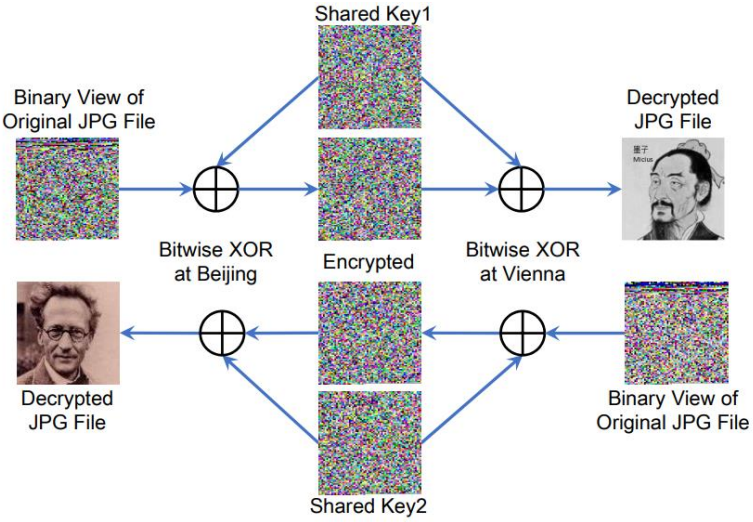


**Fig. 5** Examples of encryption.

Both the sender and receiver of the information mentioned above may be interbank banks or banks and customers. The future society is likely to reshape the traditional cryptographic technology system and ecology. In the scenario of high security demand, the above core processing process can be deduced. Since the key itself can be exchanged securely, the asymmetric key system may withdraw from the historical stage.

Quantum communication is another epoch-making revolution in communication technology and has wide application prospect. First, quantum communication can meet the requirements of long-distance space, large capacity, easy networking and other aspects. Quantum communication can be used to build high-speed and large-capacity communication networks, and realize the transmission of large-capacity ultra-high-speed data such as high-definition images, laying a solid foundation for the establishment of quantum Internet. The transmission rate of quantum communication can theoretically be equal to the vibration frequency of particles, which means the transmission rate can reach trillion Gbit/s, which is of great significance for solving the current communication bandwidth bottleneck. In classical information theory, the transmission rate and bandwidth need to meet the Shannon formula, and the signal-to-noise ratio cannot reach infinite, so the transmission rate must be restricted by the bandwidth. Quantum communication breaks through the restriction of Shannon's formula and increases the bandwidth and transmission rate to infinity.

Secondly, quantum communication can realize completely confidential communication, which makes quantum communication play an important role in military, national defense, national economic construction and other fields. In the current communication mode, even the most confidential optical fiber communication, there is a possibility of eavesdropping. Due to the strict application conditions of quantum entanglement effect, any eavesdropping attempt will lead to the change of information, and the information obtained by the eavesdropper must be different from the original transmitted information, which ensures that the transmitted information cannot be illegally obtained by a third party. Now some people have proposed to use quantum communication theory to distribute the key, which can completely eliminate the possibility of detection.

Finally, since the time delay of quantum communication is zero, it is possible to realize the superluminal communication. The development of quantum communication will definitely accelerate the process of human exploration of the universe. In earth communication, the speed of light can basically meet the real-time transmission. However, in interstellar exploration, such as lunar exploration, a round-trip delay of information reaches 2 seconds, which increases the difficulty of attitude control and other commands, and brings certain uncertainties. If quantum communication can be applied to the field of space exploration, due to the insensitivity of quantum communication to distance, the data collected by the aircraft can be transmitted to the ground segment in real time and at high speed, and the information sent by the ground segment can also be instantaneously transmitted

to the deep space aircraft, and the aircraft can even be manipulated to explore many light years away just like the remote-control aircraft.

## 4. Conclusion

In summary, this paper discusses the principle and encryption of quantum teleportation. To be specific, the basic history of quantum physics has been reviewed. Subsequently, the principle, encryption schemes as well as the state-of-art facilities and application of quantum teleportation is given. Nevertheless, the applications of quantum teleportation still face lots of limitations (e.g., costs, information capacity). In the future, more advanced scheme ought to be proposed and new encryption approach should be given. Overall, these results offer a guideline for encryption and applications of quantum teleportation.

## References

[1] Li X, Deng F. Controlled teleportation. Frontiers of Computer Science in China, 2008, 2(2): 147-160.

[2] Ma X S. On-chip teleportation. Nature Photonics, 2014, 8(10): 749-751.

[3] Bashar M A, Chowdhury M A, Islam R, et al. A review and prospects of quantum teleportation. 2009 International Conference on Computer and Automation Engineering. IEEE, 2009: 213-217.

[4] Qian P, Huynh V S H, Wang N, et al. Remote Production for Live Holographic Teleportation Applications in 5G Networks. IEEE transactions on broadcasting, 2022, 68(2): 451-463.

[5] Benzaïd C, Taleb T, Farooqi M Z. Trust in 5G and beyond networks. IEEE Network, 2021, 35(3): 212-222.

[6] Le Bellac M. Quantum physics. Cambridge University Press, 2011.

[7] French A P, Taylor E F. An introduction to quantum physics. Routledge, 2018.

[8] Zeitler C K, Chapman J C, Chitambar E, et al. Entanglement Verification of Hyperentangled Photon Pairs. Physical Review Applied, 2022, 18(5): 054025.

[9] Cozzolino D, Da Lio B, Bacco D, et al. High‐dimensional quantum communication: benefits, progress, and future challenges. Advanced Quantum Technologies, 2019, 2(12): 1900038.

[10] Chen Y A, Zhang Q, Chen T Y, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature, 2021, 589(7841): 214-219.

[11] Bhaskar M K, Riedinger R, Machielse B, et al. Experimental demonstration of memory-enhanced quantum communication. Nature, 2020, 580(7801): 60-64.

[12] Jeong Y C, Ji S W, Hong C, et al. Deterministic secure quantum communication on the bb84 system. Entropy, 2020, 22(11): 1268.

[13] Yin J, Ren J G, Liao S K, et al. Quantum Science Experiments with Micius Satellite. CLEO: QELS_Fundamental Science. Optica Publishing Group, 2019: JTu3G. 4.

[14] Liao S K, Cai W Q, Handsteiner J, et al. Satellite-relayed intercontinental quantum network. Physical review letters, 2018, 120(3): 030501.