Academic Journal of Science and Technology
ISSN: 2771-3032 | Vol. 1, No. 1, 2022

The Progress of Quantum Communication

Yixuan Tang[1, a]

[1]Beijing 21st Century International School, Beijing, 100142, China
[a]tyx7250@foxmail.com

Abstract: In view of the pursuit of increasing the capacity of channels and confidential communication, quantum communication has been developed in recent years. No-Cloning Theorem signifies that bugging can be identified during quantum communication. BB84 protocol provides the changed emissive photon to the receiver and the difference of signals would appear if there has any eavesdropper, due to quantum cannot be copied but intercepted and random selection of measuring modes by the eavesdropper. Although quantum communication still has room for growth, significant advantages of this technique make it a great candidate for future communication methods.

Keywords: Quantum communication, No-Cloning Theorem, BB84 protocol.

1. Introduction

Communications have always played an indispensable role in human lives. Exchanging information enables the development of both societies and individuals. Phenomenal inventions such as telephones and televisions introduced a digital lifestyle to the world. Creative scientists and engineers have exerted themselves in providing more convenient and accessible methods to communicate. Traced back to the 1830s and 1840s, the invention of the telegraph by Samuel Morse led telecommunication into a new era. By constructing a telegraph circuit of forty kilometers, the first long-distance telegraph was sent and the receiver machine would interpret signals according to the time elapsed of the corresponding electric current. At the same time, Morse code was created to encode the messages. The emergence of the telegraph realized communication on a broader scale at a high cost spent in circuits. The deficit of the telegraph has been made up in the upcoming development of communications. Both wireless communication and wire communication began to appear in the market and, in the big picture, they possess different traits and limitations. For wire communication, fiber-optic communication was a widely used technology. Its large bandwidth, low attenuation, and low weight ensure the volume of messages transferred. With the invention of Erbium-doped Fiber Amplifier (EDFA) which can enlarge the bandwidth, it avoids building transfer stations between the optical transmitter and the receivers. Lasers used as a medium further accelerate the rate. However, in remote areas where fibers could be easily damaged, natural disasters occur frequently and it is difficult to install wires, wireless communication stands out for high mobility and resistance. Microwave communication has a relatively short transferring distance which requires relay stations to be built on the route to receive the signals. To have a higher coverage of signals, satellite communication utilizes satellites as "intermediate relay stations" to extend the distance that signals can be transferred. Noises would also occur in the channels to influences the signals to be correctly decrypted. The above traditional communications suffice the basic needs of people in delivering messages. However, there are many improvements to be made. The ideas of maximizing the distance that signals could be transmitted, preventing the private conversation from being bugged, and increasing the capacity of channels facilitate the adoption of new technologies into communication. As scientists delve deeper into the field of quantum physics, the arrival of quantum communication remarks a new era of encryption.

The origin of quantum communication should be dated back to 1900 when Max Planck discovers the first quantum during one of his studies of thermal radiation. In December, Planck announced his great discovery of the energy quantization hypothesis which states that the energy changes of the emitter and the absorber were discontinuous during the emission and absorption of the light wave. The Planck concept of energy for the first time reveals the non-continuous nature of the microscopic natural process or the quantum nature. In 1933, Einstein-Podolsky-Rosen paradox (EPR paradox) was initiated, challenging the completeness of quantum mechanics. John Bell, aiming to support Einstein, formulated Bell Inequality in mathematics which can directly test the completeness of quantum mechanics. Results later showed the violation of Bell Inequality and indicated the property of quantum entanglement - nonlocality. On June 15, 2020, the Chinese Academy of Sciences announced that the Micius Quantum Science Experiment Satellite has achieved the first entanglement-based quantum key distribution in the scale of thousands of kilometers in the world.

This paper aimed to describe vital principles used in quantum communication and introduce several protocols of quantum key distribution. At last, limitations and future focus of the field would be discussed.

2. Principle of Quantum Communication

No-Cloning Theorem enables the identification of bugging during the communication. [1] In 1983, W.H. Zurek and W.K. Wootters proposed the theorem that "A single quantum cannot be cloned." Apagogically, if quantum cloning machines exist, for constant unitary matrix U, for any quantum state |a>, the following equation is held.

$$U(|a\rangle \otimes |0\rangle) = |a\rangle \otimes |a\rangle \quad (1)$$

Change |a> to |b>.

$$U(|b\rangle \otimes |0\rangle) = |b\rangle \otimes |b\rangle \quad (2)$$

The dot product of the above two equations yields the following equation.

$$\langle a|b\rangle = (\langle a|b\rangle)^2 \quad (3)$$

So <a|b> =0 or 1, which is inconsistent with the statement any quantum state |a>. Therefore, quantum cloning machines do not exist. Since the third party cannot copy the original signal and the detecting the quantum would cause it to collapse. The difference in probability that the signal sending subject and the receiver has would enable them to notice the bugging of a third party. [3] Quantum communication and crytography promises secure communication over long distances. Figure 1 shows the basic quantum theory.

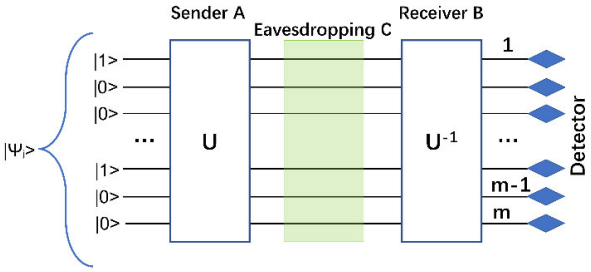

Figure 1. Basic quantum theory

3. Approaches for QC

BB84 protocol is commonly used in quantum communication.[4] After the changed photon of BB84 protocol is transmitted to receiver B, even if B chooses the same measurement mode "+" as sender A because the eavesdropping C has changed the polarization state of the intercepted photon, the measurement result of B cannot be 100% "↑", but will have A half-chance to detect "→".[5] The resulting passwords in the hands of A and B would not have been the same but would have been about 25% different.[6] To find out what information the photon is carrying, C must also measure it by randomly selecting a "+" or a "×".[7][8] At this point, the factor that determines whether C can successfully steal this one key is randomness. If C chooses the same measurement mode as A, it not only reads the bits correctly but also does not change the photon's polarization state. However, situations change when C chooses a different measurement mode than A. [9] For example, A uses the measurement mode "+" to send A photon with the direction of polarization "↑", but C chooses "×" to measure it, then C will completely change the photon's polarization state to "↑" or "→". The probability is 50% for each.[10] Therefore, if A and B compare A small part of the cipher book with each other through classical communication after the cipher book is generated, it will be clear whether there is an eavesdropper C. If 25% of the passwords are different from one another, it's a safe bet that the cipher communications are being tapped. Conversely, if the passwords are found to match 100 percent, the properties of quantum physics assure that the passwords were secure and the process was not intercepted.[11] The key exchange in the BB84 protocol has been shown in figure 2.

In 1984, Charles Bennett and Giller Brassard invented BB84 protocol.[12] Because the BB84 protocol can effectively detect eavesdropping and shut down communication, or redistribute the key until no one eavesdrops, the one-time cipher book assigned to A and B becomes an "unbreakable" encryption method that can encrypt classical communication and thus achieve completely secret encrypted communication. [2] [13] [14]

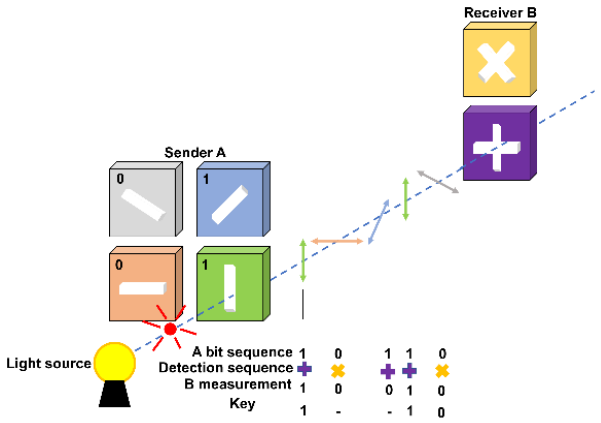

Figure 2. The key exchange in the BB84 protocol implemented with the polarization of photons.

4. Limitations & Future guidelines

Although quantum communication attains the ability to detect the bugging and stop the communication, the key still needs to be passed to each other in a classical communication way to ensure that the subjects do not communicate with someone else. [3] [15] [16]

5. Conclusion

In summary, since a single quantum cannot be cloned that the original signal would not be copied by a third party in quantum communication. The detailed approach is using the BB84 protocol to change emissive photon and transmit to receiver B, then measuring differences of the signal with sender A. If there exists eavesdropping C that the receiver B has a half chance to detect different polarization states of the photon. Further, when eavesdropping C tries to translate the information, a random selection of a "+" or a "×" mode increases the difference ratio of signal between A and B again. Therefore, quantum communication opens up a way of much safer and more confidential communication.

References

[1] Wootters, W. K., and W. H. Zurek. “A Single Quantum Cannot Be Cloned.” Nature, vol. 299, no. 5886, Oct. 1982, pp. 802–31

[2] Wilde, Mark. Quantum Information Theory. Cambridge, Uk ; New York, Cambridge University Press, 2017.

[3] Giuliano Benenti, et al. Principles of Quantum Computation and Information I: Volume I : Basic Concepts. Singapore, World Scientific, 2008.

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

[5] Bhaskar M K, Riedinger R, Machielse B, et al. Experiment al demonstration of memory-enhanced quantum communica tion[J]. Nature, 2020, 580(7801): 60-64.

[6] Hu X M, Huang C X, Sheng Y B, et al. Long-distance entanglement purification for quantum communication[J]. Physical Review Letters, 2021, 126(1): 010503.

[7] Joshi S K, Aktas D, Wengerowsky S, et al. A trusted node–free eight-user metropolitan quantum communication network[J]. Science advances, 2020, 6(36): eaba0959.

[8] Cozzolino D, Bacco D, Da Lio B, et al. Orbital angular momentum states enabling fiber-based high-dimensional quantum communication[J]. Physical Review Applied, 2019, 11(6): 064058.

[9] Ndagano B, Nape I, Cox M A, et al. Creation and detection of vector vortex modes for classical and quantum communication[J]. Journal of Lightwave Technology, 2018, 36(2): 292-301.

[10] Alarcon A, Argillander J, Lima G, et al. Few-mode-fiber technology fine-tunes losses in quantum communication systems[J]. Physical Review Applied, 2021, 16(3): 034018.

[11] Mastriani M, Iyengar S S, Kumar L. Satellite quantum communication protocol regardless of the weather[J]. Optical and Quantum Electronics, 2021, 53(4): 1-14.

[12] Richter S, Thornton M, Khan I, et al. Agile and versatile quantum communication: Signatures and secrets[J]. Physical Review X, 2021, 11(1): 011038.

[13] Saha D, Chaturvedi A. Preparation contextuality as an essential feature underlying quantum communication advantage[J]. Physical Review A, 2019, 100(2): 022108.

[14] Rudno-Rudziński W, Burakowski M, Reithmaier J P, et al. Magneto-optical characterization of trions in symmetric InP-based quantum dots for quantum communication applications[J]. Materials, 2021, 14(4): 942.

[15] Zhou R G, Zhang X. Controlled deterministic secure semi-quantum communication[J]. International Journal of Theoretical Physics, 2021, 60(5): 1767-1782.

[16] Kravtsov K S, Radchenko I V, Kulik S P, et al. Relativistic quantum key distribution system with one-way quantum communication[J]. Scientific reports, 2018, 8(1): 1-7.