Proceedings of the 2nd International Conference on Computing Innovation and Applied Physics (CONF-CIAP 2023)
DOI: 10.54254/2753-8818/5/20230539

Comparison of the frontiers optical quantum communication technology with traditional classical communication technology

Yangyi Zheng[1]

[1]Yueqing Federation of Trade Unions vocational and technical School, Shanghai, China, 200135

18516170666@163.com

Abstract. Due to the advancement of technology, laser communication, fiber optic communication and optical quantum communication have been developed, not only in the field of life, but also in the field of aviation, military and information security. This paper, mainly compares the difference between optical quantum communication and other communication technologies in terms of security and effectiveness, presenting the current state of technology and applications and providing an outlook on future directions. Through the comparison, this paper argues that the application of technology in optical quantum communication can promote the rapid development of quantum communication technology and thus enhance the comprehensive strength of global communication technology.

Keywords: Optical quantum communication technology, Quantum key distribution, Asymmetric cryptographic algorithm/Symmetric-key algorithm, Quantum Cryptograph, Information Efficiency.

1. Introduction

In recent years, significant progress has been made in the field of quantum mechanics for cross-communication. Among them, optical quantum communication, which uses quantum invisible transmission for information transfer, is mainly based on quantum entangled states. In this paper, the research application of optical quantum communication is compared to modern conventional electronic communication technologies, and its advantages in terms of confidentiality and timeliness of information transmission are analyzed. The study of optical quantum communication and its practical applications in the international quantum physics information field are of international academic significance. It is of practical value for the study and understanding of the physical properties of quantum mechanics and for the research and development of new quantum communication technologies. This paper, analyses the obvious advantages of light in quantum communication based on the available theoretical data, which will provide better confidentiality and more stable information processing capability. Through a comparative analysis of optical quantum communication technology and traditional electronic communication technology, this paper argues that the application of technology in optical quantum communication can promote the rapid development of quantum communication technology and thus enhance the comprehensive strength of global communication technology.

2. Definition of Quantum Communication, Quantum key distribution, Asymmetric cryptographic algorithm/Symmetric-key algorithm and Cryptography

2.1. Quantum Communication

Quantum communication uses the laws of quantum physics to protect data. These laws allow particles - usually photons used to transmit data along fiber optic cables - to take on superposition, meaning that they can represent multiple combinations of 1s and 0s at the same time. In classical network information communication theory and network communication science, the "bit" is usually the most basic defining concept and the basic unit of measurement to define the amount of information [1]. The quantum bit unit is the unit of measurement for transmitting information in quantum science. And these particles are known as bits or qubits. From a network security point of view, the beauty of quantum bits is that their ultra-fragile quantum state "collapses" to 1 or 0 if an eavesdropper tries to observe their transmission. and it is this property that gave birth to the technology of Quantum Key Distribution (QKD). With this technique, in practical applications of transmission, companies or authorized users can transmit highly sensitive data under the scope of a network. It is theoretically very secure.

2.2. Quantum key distribution

Quantum encrypted communication is a two-step process in which a quantum key is distributed over a quantum channel. In this step, only the key is generated and distributed, and a completely random pair of quantum keys known only to the two communicating parties is obtained through quantum key distribution. The ciphertext is passed over the conventional channel. Using the obtained quantum key, the sender encrypts the message into a ciphertext, and the receiver decrypts the received ciphertext, thus achieving complete confidentiality of the communication. It follows that quantum encryption protects the "key" of traditional encrypted communication, also known as quantum key distribution (QKD).

2.3. Asymmetric cryptographic algorithm/Symmetric-key algorithm

The so-called symmetric encryption algorithm means that one party uses a specific algorithm and a specific key to encrypt a message; the other party uses the same algorithm and the same key to decrypt the message. Once both parties shake hands and negotiate the algorithm, and each holds a copy of the key, they are ready to communicate. However, since the communication often contains duplicate information and the randomness of the ciphertext is not sufficient, after multiple uses of a single cipher, even if eavesdropper does not know the encryption algorithm, the eavesdropper also can infer the original text by the correlation between different parts of the ciphertext, thus the transmission process will face the problem of key leakage. This system is both complex and variable due to the nature of the Internet's mesh structure. Traditional peer-to-peer communication is not only inefficient, but also costly. Therefore, asymmetric encryption algorithms (public key systems) provide a solution to this application scenario. The so-called asymmetric encryption algorithm uses the properties of some functions in mathematics (e.g., it is easy to calculate the value of a function based on its parameters, and it is difficult to deduce the value of a function based on its parameters) and uses a public key to encrypt and a private key to decrypt, so that only the public key is used for communication, thus ensuring the security of communication information. For example, the famous RSA algorithm (Figure 1). However, the security of asymmetric encryption algorithms depends entirely on an assumption that is not secure: the inverse function of the encryption function is difficult to obtain, such as the factorization of the product of two large prime numbers, on which RSA relies. However, there is no guarantee that any mathematician will create a faster factorization algorithm in the future. Or perhaps starting with hardware (such as a quantum computer) that can be quickly and violently cracked with faster computations. In the short term, this kind of encryption, which relies on the time complexity of mathematical calculations, can still be used, and does strike a good balance between security and usability. But in the long run, it is inevitable that it will be cracked and obsolete [2].

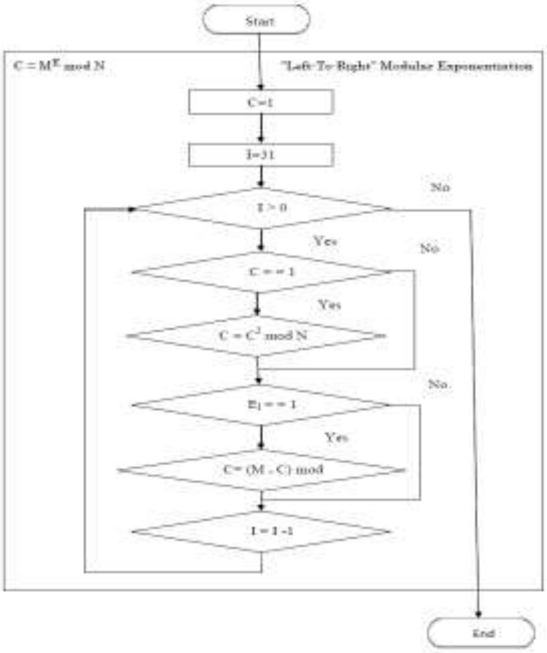

Figure 1. RSA Encryption and Decryption flowchart [3].

2.4. *Cryptography*

The three basic elements of cryptography are the algorithm, the cipher, and the key, The security algorithm itself can also be seen as a "coding rule", which alone cannot achieve total security because others can know the algorithm and derive it, so it is not realistic to rely on this rule alone. The goal of cryptography is to deny the eavesdropper access to the key so that the ciphertext cannot be deciphered. Currently it is possible to make the cipher itself secure, but the transmission of the key is not. Here we refer to Shannon's theorem: absolute security. This is also known as "One time pad", where the key is the same length as the plaintext and is a random string of characters, and the key is changed every time the ciphertext is transmitted [4]. Although this theorem is theoretically perfectly secure, if the authorised person must obtain the key once before each encrypted message, the entire communication cannot be secured if the key is leaked during the exchange. A detailed solution is also given in this paper.

3. Application of quantum key distribution in quantum communications and comparison with the traditional encrypted communications.

3.1. *Analysis on the Security from the Application of Quantum Key Distribution in Quantum Communications*

Research show that the Quantum key distribution is the only near practical and core technology development in the field of quantum communications at home and abroad. The applications of Quantum Key Distribution in recent years have been rising applications in quantum communications. And in quantum communication, Quantum Key Distribution is based on quantum's unclonable theorem mechanics [5], which says that it is inconceivable to duplicate an unknown quantum state without causing a disorder to it. Enabling secure key distribution and realizing unconditional security's possibility so that users can have accurate information from multiple ways and dimensions. Therefore, this technology reaches the maximal information processing capability in quantum communication and enhances the security and efficiency of quantum communication.

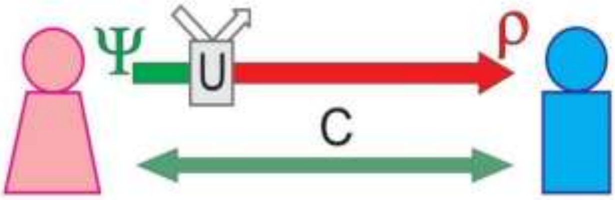

Figure 2. QKD’s setting: Alice and Bob are linked through a quantum channel [6].

The QKD general setup is illustrated in Figure 2. Partners were authorized by the two, those wanting to create the secret key at a distance, people call them Bob and Alice. They need to be associated via two channels: a quantum channel, which permits them to divide quantum signals, and a classical channel, on which they can forward classical information back and forth. As the classical channel demands authentication, this means that Bob and Alice need to identify themselves. The quantum channel, nevertheless, is exposed to any potential manipulation from a third individual. The third person can listen to the conversation but cannot participate. Specifically, Alice and Bob's job is to secure against an adversarial eavesdropper, the third individual, which commonly announced by Eve, who eavesdrops on the quantum channel and listens to the communication on the classical channel.

Here proposes an interesting idea is proposed, because there is no physical principle that would prevent Eve from cutting off the channel and thus Eve could block all information transmission between Alice and Bob [7]. Taking a step back, we can imagine the following eavesdropping strategy. Eve systematically cuts off all the QKD channels up to the one Alice and Bob are on - after all, they want to communicate, so they choose the less secure method which is to use the only channel, and Eve then eavesdrops on the message. This idea obviously has merit, but, considering that if QKD is used correctly, Eve has no hope. This is because Eve must interact with the quantum system before eavesdropping on the message, to learn about the key. If the encoding uses a randomly chosen non-orthogonal state, Eve's intervention will necessarily modify the state of the system [8]. Eve's modifications can be observed by both parties, and they can be quantified. That is, the perturbations observed in the quantum channel can be calculated as bounds on the information obtained by Eve. This is cannot be done with conventional encrypted communication, and of course, it will be argued that Any action by Eve to extract several information from a quantum state is a generalized shape of measurement. And a well-known principle of quantum physics tells that measurement qualifies the state of the system being gauged loosely. One might instead think that Eve's aim is to get a complete copy of the state that Alice sends to Bob. In any way this is banned by the no-cloning theorem, which says that one cannot duplicate an unknown quantum state when keeping the original state unchanged. These two arguments have appeared in several papers.

3.2. Quantum key distribution in quantum communication compared with the conventional cryptography in classical electronic communication

The importance of keys in cryptography, and their vulnerability to tampering, was mentioned earlier. When two authorized parties hold their own keys, they can only decrypt each other's messages after using their own keys, which are changed periodically. As the number of authorized persons increases, different keys are distributed. In this way, even if some people's keys are compromised, the entire private information is not compromised. This idea led to the development of a cryptographic algorithm, the Asymmetric Cryptographic Algorithm or Public Key Cryptographic Algorithm, or RSA for short. This algorithm has been mentioned in the previous section and will not be described in detail here. Its substitutability is also since the quantum factorization algorithm has overcome the problem of factorization. Due to the properties of quantum mechanics, it is also being passed during the generation of the quantum key. When a communication is established, both parties are given a random string with the exact same random number. This random string is the quantum key. So, without seeing the data between the two parties, the key is generated and distributed at the same time, thus avoiding all the risks of transmitting the key before. In addition, the quantum key is a random string of characters, the length of which can be set at will, and the key is reconstructed each time the message is prepared for transmission, so that all three requirements of Shannon's theorem are met, and the ideal state of perfect security in Shannon's theorem is achieved. Once both parties have the key, all that remains is to communicate. It is because the key after quantum key distribution is perfectly secure to match Shannon's theorem, that communication becomes indecipherable and secure.

So QKD preserves the authorized partner’s private information to the greatest extent possible compared to traditional classical communication techniques.

4. Information efficiency of optical quantum communication in quantum channel.

4.1. Comparison in information efficiency

The IM/DD (optical intensity modulation/direct detection) mode of fibre optic communication is used in almost all types of fibre optic communication systems in the world today [9]. However, due to the limitations of optical frequency carriers, new optimized fibre optic communication systems such as fibre optic coherent optical communication systems, optical wave multiplexed communication systems and optical soliton communication systems have been continuously proposed. These system solutions are able to increase the maximum information rate, i.e., the communication capacity, to a large extent and show great promise for the development of fibre optic communication technology. However, this increase is limited compared to the true potential of optical communications. This is because these communication modes are based on classical communication theories and concepts. Among other things, light is a wave in the electromagnetic wave range of 0.1 to 100 microns. The transmission of information as an optical carrier is therefore in essence no different from the already practical radio communication in the medium and short wave range up to the microwave band. In this context, such communications can be collectively referred to as classical communications, and the channel for such optical communications..., is also referred to as a classical channel. It is in this channel that the channel capacity is ultimately limited due to Gaussian noise limitations [10]. To go beyond this limitation, the concept of optical quantum communication and new communication models have been proposed, inspired by current optics. Due to some of the unique principles and phenomena of the quantum world, such as Heisenberg's Uncertainty Principle [11] and the No-Cloning Theorem, quantum communication can achieve faster communication rates than classical channels. It is possible to achieve faster communication rates than classical channels.

4.2. Proof

Here simply demonstrate the full advantage of information efficiency in the quantum channel over conventional communication based on Shannon's theorem. By the Shannon theorem, $C = B\ log2(1 + S/N)$, the information capacity of a classical channel is, $C = 1.44B \times ln(1 + SNR)\ bit/s$. The limiting signal-to-noise ratio for optical wave communication can be calculated from the quantum limit as: $SNRm = \eta PS/hvB$. Where η is the quantum efficiency, PS is the optical signal power, B is the bandwidth, v is the photon frequency and h is the Planck's constant. Then the photon emission power is, Np=PS/hv. And by Substitute in the Shannon's formula, the information efficiency limit of a photon in a classical channel can be calculated as $Pm = 1.44\ bits/photon$ when B→∞.

Then under the quantum channel, the signal-to-noise ratio of photons depends on the photon number rise and fall, and a theoretical analysis shows that the information efficiency of photons is, $Pm = 1.44hv/KT.\ K$ is the Boltzmann constant, T is the system temperature, and the information efficiency of the quantum channel at room temperature, i.e., $T = 300K$ and $v = 3 \times 10\char`^14\ ms\char`^ - 1$, is, $Pm = 69\ bits/photon$. This Calculation shows the overwhelming advantage of the optical quantum communication mode compared to the classical communication mode.

5. Conclusion

The security of classical secure communications has not yet been mathematically proven. With quantum properties, secure communication can be achieved with strict mathematical proof. In order to increase the sensitivity of the communication system, it is possible to use an optical quantum communication system, which uses the relevant monitoring of photon pairs at the receiver. In this way, the signal can be recognized by the receiver even if it is buried by noise. However, in the early stages of research into optical quantum communication, there are some unresolved shortcomings in its application, such as the susceptibility of light to scattering and hence loss, and the insecurity of existing systems with weakly coherent sources for the reported key distribution distances. This paper also analyses the technological frontiers of optical quantum communication and its development in terms of security and timeliness respectively. At present, it will take a long time to solve all these problems, a complete practical system solution for optical quantum communication is still a long way off. However, in today's era of rapid advances in information technology, it is always surprising to see how quickly technical problems can be solved.

References

[1] Shannon, Claude Elwood. A mathematical theory of communication. The Bell system technology journal 27.3, 1948: 379-423, pp. 1-2.

[2] Xiande Zhuo, F. Zhao, and Deming Zeng. Research on asymmetric encryption techniques [J]. Journal of Sichuan University of Science & Engineering (Natural Science Edition) Diss, 2010(563), pp.2.

[3] Mahajan P., Sachdeva A. A study of encryption algorithms AES, DES and RSA for security [J]. Global Journal of Computer Science and Technology, 2013, pp.19.

[4] Katz, Jonathan, and Yehuda Lindell. Introduction to modern cryptography, CRC press, 2020. pp. 34-40.

[5] Wootters, William K., and Wojciech H. Zurek. A single quantum cannot be cloned. Nature 299.5886, 1982: 802-803.

[6] Scarani V., Bechmann-Pasquinucci H., Cerf N. J., et al. The security of practical quantum key distribution [J]. Reviews of modern physics, 2009, 81(3): 1301, pp. 3-4.

[7] Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." Physical review letters 85.2, 2000: 441, pp.1.

[8] Scarani V., Bechmann-Pasquinucci H., Cerf N. J., et al. The security of practical quantum key distribution [J]. Reviews of modern physics, 2009, 81(3): 1301, pp. 8.

[9] Okoshi, Takanori, and Kazurō Kikuchi. Coherent optical fiber communications. Vol. 4. Springer Science & Business Media, 1988, pp. 2-3.

[10] Mitra, Partha P., and Jason B. Stark. "Nonlinear limits to the information capacity of optical fibre communications." Nature 411.6841, 2001, pp.1027-1030.

[11] Heisenberg, Werner. "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik." Original Scientific Papers Wissenschaftliche Originalarbeiten, Springer, Berlin, Heidelberg, 1985, pp. 478-504.