ATLANTIS PRESS

Advances in Computer Science Research (ACSR), volume 73

7th International Conference on Education, Management, Information and Computer Science (ICEMC 2017)

Analysis of Quantum Security Direct Communication Protocol

Jinxin Gong

School of North China Electric Power University, Beijing, China

792948048@qq.com

Keywords: Quantum secure direct communication; Two-step scheme; Ping-pong protocol; Quantum secure direct communication network model

Abstract. Quantum security direct communication is based on quantum physics, combined with the classic communication theory. It becomes a new communication model, its transmission of information on the high efficiency, security has been more and more extensive attention. That is, since the beginning of this century, has been rapid developed. In this paper, we will describe several common quantum secure direct communication protocols and economic quantum secure direct communication network models theoretically. At the end of this paper, we will discuss and analyze the development and the future of quantum safety direct communication.

Introduction

With the development of the information period, the classical information theory is limited to a large extent. The quantum effect and its corresponding theoretical system play an increasingly important role in the information system. Quantum informatics is born, Quantum Key Distribution (QKD) is a mature theoretical system in quantum information science, which makes the key generation in the classic password, and the distribution problem solved. However, the non-direct transmission key feature of the standard QKD causes a large loss of quantum bits, resulting in a problem that its information transmission efficiency is low. In order to improve the transmission efficiency of the problem, based on QKD , we proposed quantum safety direct communication.

Quantum Secure Direct Communication (QSDC) is a kind of information carrier with quantum state in communication. It uses quantum mechanics principle and various quantum properties to transmit confidential information directly through quantum channel. It is a new type of quantum communication mode. It does not need to distribute the key in advance during the communication to encrypt the information, but in the legitimate communication between the two sides directly transmit information, it is more demanding on the security.

In 2000, Longgui Lu and others first proposed the concept of QSDC, and proposed the first quantum secure direct communication scheme - efficient two-step quantum secure direct communication scheme, but the program was later proved to be not safe by its author. 2001 Beigeetal. proposed a communication scheme that achieves an approximate safety using quantum entangled states. In the same year, Bostrom and Felbinger proposed a quasi-secure quantum secure direct communication protocol, the ping-pong protocol, based on the dense coding principle. Although there are some security problems, the protocol clarifies the concept of direct communication for the first time. In 2003, Dengfu Guo and others proposed a two-step quantum secure direct communication scheme based on dense coding, and discussed the standard of quantum secure direct communication scheme. In the last ten years, quantum safety direct communication has been greatly developed. In this paper, we will analyze several representative quantum safety direct communication protocols and make a prospect of the quantum safety direct communication network scheme future quantum safety direct communication.

Quantum Direct Communication Protocol

Two-Step QSDC Protocol. The two-Step QSDC protocol uses the protocol of the entangled particle pair and the single-photon sequence. The following is a schematic diagram of the Two-Step

QSDC protocol (Fig 1). We set the sender for Alice, the receiver for the Bob, the specific process is as follows:

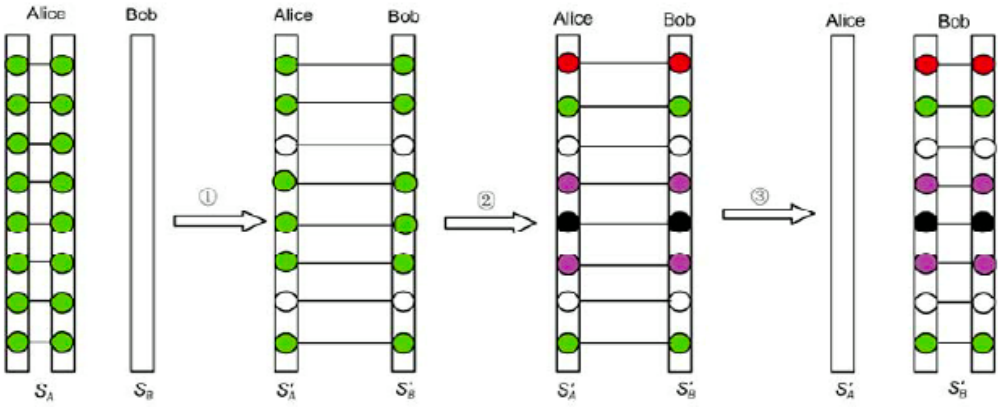

Figure 1 Schematic diagram of Two-Step QSDC protocol

Alice first sends Bob a set of quantum signals consisting of N entangled photon pairs, which are in the same quantum state$|\varphi^- >= \frac{1}{\sqrt{2}}(|0>_A|1>_B - |1>_A|0>_B)$. Bob receives the N entangled photons into two columns: first Is listed as S_A (information sequence), which is composed of a pair of pairs of photons to select a photon; the second column is recorded as S_B (detection sequence), composed of residual photons.

Alice controls the information sequence, sends the detection sequence to Bob, Bob randomly measures the amount of photons from the detection sequence to measure it, and then tells Alice on the classical channel the position and measurement of the single photon and the measurement base in the detection sequence result. Alice, based on information obtained from Bob, finds photons that are paired with Bob's sampled photons in the information sequence and performs these single photon measurements with a measurement base that is consistent with Bob and writes down the results, and then Alice's measurements An error rate analysis is performed with the result of Bob's transmission, which is much lower than the pre-set security threshold, indicating that the transmission of the sequence S_B is secure and the communication process is safe,we can continue transmitting the massage; otherwise, the communication ends.

After all the photons of S_A for safety detection are deducted, we get the sequence S'_A Alice, after determining the transmission channel security, will do the corresponding unitary operations for each photon in the sequence S'_A, and encode the sequenceS'_Acompletion information. This unitary operation is one of the $\{U_0 = \mathrm{I}, U_1 = \sigma_z, U_2 = \sigma_x, U_3 = \sigma_{iy}\}$. The above four unitary operations may represent 00,10,01,11 at the time of encoding. Subsequently, Alice sends the encoded sequence S'_A to Bob, Bob combine the sequence S'_A with the sequence S'_B (that is, deducting all the photons in the sequence for security detection) to do the Borgki joint measurement, resulting in the transmission of information .

In fact, the above process to achieve two security analysis, the first security analysis, because the photon pair sequence is divided into two columns S_A、S_B, so the eavesdropper Eve has been unable to listen to all the information at the same time. And the second security analysis is to detect the accuracy of information transmission. The two security analyzes improve the security and validity of the information transmission from the aspects of preventing the monitoring and improving the accuracy rate.

Ping-pong Protocol. In order to further improve the transmission efficiency of information, people put forward the ping-pong communication protocol based on the pulse of the relevant organs. After that, many scholars have proposed a variety of Ping-pong communication protocol, these agreements are mostly based on entangled EPR or non-orthogonal state. The following is a brief description of the original Ping-pong communication protocol of the basic process.

First, the sender Alice prepares a set of quantum bit strings in an entangled or nonorthogonal state and passes it over the channel to the receiver Bob. Bob receives this string of bits after it is

divided into two parts, part of which is used as a control mode, the quantum bits of which are randomly selected at probability C, and the remaining quantum bits are used as messages Mode, and Bob then encodes the two sets of qubits, passing the encoded result to Alice. Alice, when it gets the encoded information, checks it with Bob's QKD control mode to determine whether the transmitted information has been attacked. If the transmission is safe, then continue to transmit, if attacked, which stop communication.

The above is the basic process of the original Ping-pong communication protocol. It is known that this communication protocol greatly improves the communication efficiency.

Quantum Security Direct Communication Network Solution

In order to efficiently transmit a large amount of information, we need to establish a quantum secure direct communication network, which is a very important topic in the field of quantum communication. An efficient and secure quantum secure direct communication network consists of three parts: the sender, the receiver, and the server, where the server is used for quantum fabrication and quantum signal measurements.

Based on the above, we propose an economical quantum secure direct communication network scheme, as shown in Fig 2.

Alice is the server; Bob is the sender, C_B is the Bob's encoding operation; Charlie is the receiver, C_C is the Charlie's encoding operation; M_A、M_B、M_C is the three measurements; E_1、E_2、E_3 is the attack operation. In this scenario, a single photon is prepared using the server Alice, which has a characteristic of horizontal polarization, and then sends these single photons over the channel to Charlie, which may encounter Trojan attacks or disruptions in this process ,such as E_1.So the receiver Charlie received a single photon to measure it, that is M_C, to determine the transmission process when attacked. After determining that no attack has been made, Charlie encodes the received information and adds a partially oblique polarized photon to the code and sends it to Bob, which also sends a measure of the process and prevents the information from being subjected to the above two kinds of attacks. Bob receives the information from Charlie and then measures it, that is M_B, if there is no attack on the problem, then encode it again, and the encoded results back to the server Alice. In the process of Bob's transmission to Alice, the information may be subject to disruption attacks, so when the server receives the information, it will first measure it, that is M_A.If the information is not attacked, then the receiver and the sender to publish the measurement results .The receiver and the sender according to the published results and their own encoded information to send the message, complete the transmission of information.

Although the above-mentioned network model is cost-effective, it is only suitable for smaller local area network communication. When the communication distance becomes longer, it is easy to lose the signal. For quantum safety direct communication, the loss of signal represents the reliability of

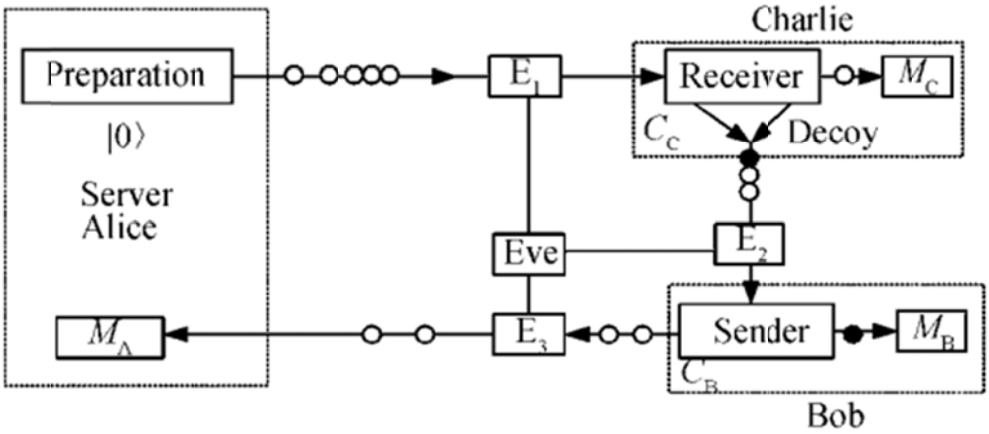

Figure 2 Economical Quantum Security Direct Communication Network Model

information transmission is reduced, so in the design of quantum security direct communication program, we must reduce the signal loss principle, improve the reliability of the program, for which we Can be added to all aspects of security testing this link.

In addition to the above-mentioned economic quantum safety direct communication network model, scientists have proposed a variety of network models in recent years, such as quantum safety direct communication network model based on two-step quantum secure direct communication scheme, wide-area quantum secure direct communication based on decoy Network model and so on. In short, with the development of quantum communication, quantum security direct communication network program is more and more perfect, security and effectiveness are getting higher and higher, can be applied to wide area network, local area network and other forms of network communication.

Looking to the Future

Since the end of the last century, quantum safety direct communication because of its higher security, higher transmission efficiency has been a high degree of concern, more and more scientists into the field of quantum safety direct communications, put forward a variety of Communication protocols and communication network solutions, this article describes the common few.

In the field of quantum safety direct communication protocol, how to resist noise becomes a quantum security direct communication field needs to overcome the problem. In 2011, Xiaofen Liu proposed a two-way QSDC protocol, which is based on the idea of collective noise, can resist rotation noise and is safe and efficient. How to make the QSDC protocol safer and more economical while resisting noise is also a problem that scientists have been solving. In 2012, Kai Li proposed an effective solution: to allow legitimate communicators to carry a transmission of particles can be transmitted secret messages, use it instead of detecting the particles to complete the detection process of eavesdropping, so there will not be any information leak , At the same time in theory, both sides of the quantum signal theoretical efficiency reached 100%, to ensure the unconditional security.

In the case of quantum safety direct communication network model, how to improve the transmission distance of information without affecting the security of information transmission is also an urgent problem to be solved. In 2009, Dongxiao Quan proposed a wide-area quantum secure direct communication network model based on the decoying state. The model placed a server in each local area network to generate and measure the quantum, so that when the need for different local area network Communication, can greatly reduce the communication distance, as a basis for the establishment of a wide area network quantum secure direct communication network, but this network model on the other hand also increased the cost of establishing the network.

With the development of quantum communication, the limitations of classical communication technology have been exposed, and more secure and efficient QSDC technology has been widely

concerned. At present, the QSDC popular researches are: long-distance quantum safety direct communication, anti-noise QSDC protocol, Dimensional photon for information transmission. With the increasing problem of communication and more serious, high security QSDC technology in the future will eventually become more and more widely used.

References

[1] Dongxiao Quan, Changxing Pei, Dan Liu, Nan Zhan. A Wide Area Quantum Secure Direct Communication Network Scheme Based on Excluded State [J]. Journal of Photonics, 2009, (12): 3283-3287.

[2] Dazu Huang, Chen Zhigang, Guo Ying. Insecurity "Ping-pong" Quantum Communication Protocol [J] COMPUTER SYSTEMS, 2008 (12): 2202-2206.

[3] Haipeng Ren. Overview and Prospect of Quantum Security Direct Communication Protocol [J]. Communication Technology, 2013, (04): 31-33.

[4] Guilu Long,Chuan Wang, Yansong Li,Fuguo Deng. Quantum Security Direct Communication [J]. Chinese Science: Physics Mechanics Astronomy, 2011, (04): 332-342.

[5] Fuguo Deng, Ping Zhou, Xihan Li,Chunyan Li, Hongyu Zhou. Quantum safety direct communication research progress [J]. Nuclear Physics Review, 2005, (04): 382-