Research in the application of Quantum cryptography communication technology for Launch Vehicle Range

Fengzhu Ji[1], Yunting Zhou[1], Fan Qiang[1], Xiaobo Yang[1], Qijie Tang[1], Hongyang Liu[1]
[1]Xi Chang Satellite Launch Center
Si Chuan, China

***Abstract*—In view of the current network security situation, the basic principles and implementation method of quantum cryptography are studied. Considering the present situation of quantum cryptography communication technology and launch vehicle range, a network scheme is designed based on quantum cryptography communication network, and several miniature tests are carried out. From the results of the validation, network performance test results can meet communication support requirements of the rocket launch test in launch vehicle range, different types of information transmission is normal, and the quantum key technical indicators meet the requirements of the equipment. So the network scheme is a feasible solution.**

***Keywords*—quantum cryptography; QKD; principle; scheme; experiment**

I. INTRODUCTION

Quantum cryptography communication technology is an advanced technology in the field of current encryption communication technology[1,2]. Some experimental applications have been carried out, such as quantum communication experiment and demonstration of Hefei city network, Xinhua finance information validation quantum communication network, etc. From the test application, the results of the test meet the demand of users. And the application results also show that the communication based on quantum cryptography has been realized, and it improves the security of network.

The information transmitted on the network transmission of the launch vehicle range is very important. Higher requirements have also been placed, such as the real-time, stability and so on. The basic principles and implementation method of quantum cryptography is studied, a feasibility network scheme is presented based on quantum cryptography technology for communication security of the rocket launch test in launch vehicle range

II. PRINCIPLE OF QUANTUM CRYPTOGRA-PHY COMMUNICATION TECHNOLOGY

Quantum cryptography system includes quantum key distribution(QKD), storage and relay, quantum identity authentication, intrusion detection, quantum code, shared quantum cryptography, quantum security protocols, analysis of quantum cryptography, quantum information theory, combination of classical and quantum passwords and other research directions. The quantum key distribution is the core of the quantum cryptography system. With the deepening of research, the contents of quantum relay and intrusion detection are gradually contained in the research of quantum key distribution. So some researchers have narrow called quantum key distribution as quantum cryptography [3, 4].

A. Principle of quantum cryptography communication

Quantum key distribution is not used for transmitting cipher text, but is used to establish, transmit the cipher code. That is, key distribution in secret communication both sides, commonly known as quantum cryptography communication. As the main content of quantum information technology, quantum communication is one of the most promising applications. The purpose of Quantum cryptography communication is to achieve an absolutely secure communication between legitimate communicants. The main task of the quantum key distribution is generated a secure key between the communicating parties using the quantum channel. To carry out the secret information communication, the sender sends the cipher text which was generated from information encryption. Then the cipher text information will be sent to the receiver through classical communication. Receiver obtains the plain text using the cipher code to decrypt the cipher text. This is a four step communication process, that is, keys generated, information encrypted, and information transmitted and messages decrypted.

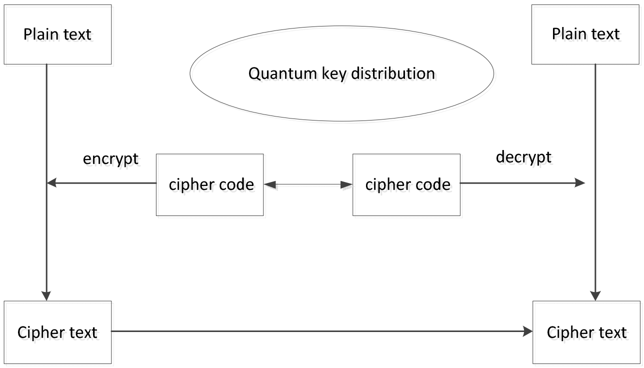

Fig 1. Principle of quantum cryptography communication

Copyright © 2017, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

B. Quantum Key Distribution Protocol

The practical application of quantum key distribution is mainly based on the BB84 protocol. BB84 key distribution process can be described as follows (the sender is named as Alice, the receiver is Bob) [5, 6]:

1) Information agreed: Alice and Bob agreed the loading way of information, which includes the orthogonal conjugation, and the corresponding relationship between each quantum state and binary information.

2) Photons preparation: Alice makes a single photon as the carrier of quantum information.

3) Information loading: At first, Alice produces a set of random sequence, and selects one from two groups of orthogonal conjugation. According to the random sequence, the information is loaded by the photon modulation in the corresponding quantum states. Such as: the horizontal and vertical base can be chosen using polarization beam splitter (PBS), and adding a 1/4 wave plate, 45 ° and 135 °base will be selected.

4) Measurement: When the photons arrive at Bob, Bob will select a group of base in a horizontal or diagonal randomly as a measuring method. Measuring process can also be accomplished by PBS and l/4 plate.

Because the photon will be attenuated in the path, it is not every photon that sent by Alice can be detected by Bob. Bob only records the photon position (active photon) which he detects. And others will be thought as lost in the quantum circuit. The fifth step operation that Alice does is only to aim at the active photon.

5) Base comparison: Bob publishes the measurement base that he uses. If the base of photon modulation that Alice modulates is the same as Bob, Alice notices Bob that the base comparison is successful. The both sides keep the polarization information that is used and measured for this transmission.

6) Key generation: the quantum key sequence is generated, according to the preserved polarization state, and the agreed relationship between the polarization states and the binary bits "0" and "1".

III. SCHEME OF QUANTUM CRYPTOGRAPHY COMMUNICATION

According to the structural characteristics of the network of launch vehicle range, using the existing mature quantum cryptography communication equipment in China, a typical three-node quantum cryptography communication network is presented, which is shown as Fig. 2.

Quantum key distribution system is composed of 3 switches, 4 sets of long distance quantum key generation equipment, 2 sets of short distance quantum key generation equipment, and 3 sets of equipment management, and which is to implement the quantum key distribution and management. The traditional data is encrypted by the application of quantum key encryption equipment. Controlling equipment monitors the state of the equipment management of quantum cryptography.

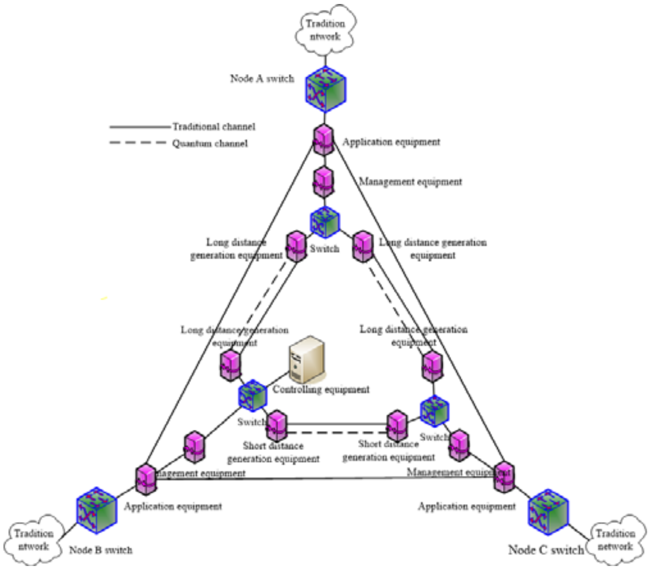

Fig 2. Three node quantum cryptography communication network topology

The scheme does not change the traditional network architecture. Only the quantum key application device is connected to the conventional network.

- The quantum key generation device integrates all the functions of the quantum key distribution, including the preparation of the light source, signal loading, measurement, and other related functions.
- The management device mainly implements the key management and the setting of the security policy, and realizes the network key synchronization.
- Application equipment is used to complete the data encryption and decryption.

IV. MINIATURE EXPERIMENT

A. Purposes of experimental verification

Set up the network operating environment, and check the correctness and feasibility of quantum cryptography communication network scheme through the experimental verification method.

And further optimize and improve the network architecture based on the experimental results. And it can provide experimental experience for the application of quantum cryptography communication technology in the launch vehicle range.

B. Test verification content

1) Communication performance indicators of quantum cryptography communication network

In both cases of the traditional encryption communication and quantum cryptography communication, the network performance is tested between each node. Check the throughput, network delay, delay jitter and packet loss rate and other communication indicators through the test. And confirm whether it meets the network communication security requirements of launch vehicle range

2) Information transfer capability test

Transmit voice, image and data between each node, and adopt multicast and unicast mode to transmit according to the information type. Check the quality and volume of the voice transmission, fluency and clarity of image transmission, and if there is the problem about loss packets, heavy frame, data disorder.

3) Quantum equipment indicators

The quantum code rate is the effective quantum key rate generated in the unit time under the attenuation of a certain optical fiber line. This indicator is used to evaluate the service capability of the QKD system. The code rate needs to be greater than 1kbps, which is basic condition of quantum cryptography communication.

Quantum error rate means the error rate of the transmitted signal state when the quantum key distribution is emitted. And the error rate needs to be controlled less than 5%.

Quantum error rate is an important parameter of the quantum key distribution system. It is an important indicator to ensure the quantum code rate and realize the quantum cryptography communication.

C. Environment of miniature test

Simple or complex quantum cryptography distribution network, which are all based on point-to-point distribution. On the basis of quantum cryptography distribution, quantum cryptography distribution network and quantum cryptography network distribution are realized by centralized control station / key relay. Point-to-point distribution is the basis of quantum key and application model of quantum key distribution network. So this test selects the basic model of the point-to-point quantum key distribution and application.

In this paper, the validity of quantum cryptography, the communication performance of quantum cryptography communication network, the transmission capability of quantum encryption system and the code rate of quantum device have already been tested.

D. Test results evaluation

According to the test verification contents, the test results are validated from three aspects: communication performance index, service transmission capacity, and quantum equipment indicators

TABLE I. COMMUNICATION PERFORMANCE INDICATORS

Test content	Standard	Typical	Quantum
Throughput	>300Mbps	387Mbps	342Mbps
Average delay	<100ms	1.241ms	1.132ms
Delay jittering	<25ms	0.049ms	0.052ms
Packet loss	<0.1%	0	0
Conclusion	results meet the requirements		

TABLE II. INFORMATION TRANSMISSION

Test content	Standar	Typical	Quantum
Sound transmission	fine	fine	fine
Video transmission	fine	fine	fine
Image transmission	fine	fine	fine
Data transmission	fine	fine	fine
Packet loss	<0.1%	0	0
Conclusion	results meet the requirements		

TABLE III. QUANTUM EQUIPMENT INDICATORS

Test content	Standard	Test result
Quantum code rate	>1kbps	1.2kbps
Quantum error rate	<5%	2.6%-4.1%
Conclusion	results meet the requirements	

V. CONCLUSIONS

In view of the current situation of network security, quantum cryptography communication principle and the realization method have been studied in this paper combining with the characteristics of the test range of IP space network. According to the existing conditions of quantum cryptography communication technology status and space range, the actual design scheme based on quantum cryptography communication network has been studied. And the experimental verification has been carried out. From the verification results, quantum key equipment can meet the technical requirements. The test results can guarantee the network performance during test task range of conventional aerospace. And it also has feasibility in aerospace site deployment.

However, there are still some distance between test environment and the actual environment. Such as the transmission distance, the transmission content and the complex electromagnetic environment, these may have an effect on the system. The next step, the research work can be continued to carry out. A verification demonstration system can be established, and we can get to provide more powerful technical support for quantum cryptography, which will be applied on IP network.

References

[1] Bennett C, Brassard G. Quantum cryptography: Public key distribution and coin tossing[C] Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. 1984:175.

[2] Takesue H, Diamanti E, Honjo T, et al. Differential phase shift quantum key distribution experiment over 105 km fibre[J]. New J. Phys., 2005, 7:232.

[3] Yin Z Q, Li H W, Chen W, et al. Security of counterfactual quantum cryptography [J]. Phys. Rev. A, 2010, 82:042335.

[4] Acín A, Gisin N, Masanes L. From Bell's Theorem to Secure Quantum Key Distribution [J]. Phys. Rev. Lett., 2006, 97:120405.

[5] Cai Q. Eavesdropping on the two- way quantum communication protocols with invisible photons [J]. Physics Letters A, 2006, 351(1-2):23--25.

[6] Liu W, Chen H, Li Z, et al. Efficient Many-to-One and One-to-Many Multi-party Quantum Secure Direct Communication with Authentication[C] International Conference on Intelligent Information Hiding and Multimedia Signal Processing.2008:1282--1285.