Application of quantum secure communication technology in the power grid services

Mengmeng Xing¹⁴, Guojun Liu² and Xu Lu³

¹School of Electrical & Electronic Engineering, North China Electric Power University, Beijing 102206, China;
²Laboratory of Electric Power Communication Network Technology, Institute of Information and Communication, Global Energy Interconnection Research Institute Co., Ltd., Beijing 102209, China;
³State Grid Eastern Inner Mongolia Electric Power Co., Ltd., Hohhot 010020, China.

E-mail: 526941349@qq.com

Abstract. With the development of power communication networks, the demand of information security involved in power network services also increases. Traditional secure communication technology have not been able to guarantee the security of the information transmitted in absolute security. This paper focuses on the problem of secure transmission of power communication networks, and proposes a suitable quantum secure communication technology scheme to ensure the key rate of the long-distance quantum secure communication and the security of the power communication network.

1. Introduction

With the increase of security attacks on power grid business in recent years, the security of power information transmission has also attracted people's attention. Because of the large-scale parallel computing characteristics of quantum computers, their computing speed can be several orders of magnitude faster than that of classical computers, which makes the traditional public key cryptosystem based on mathematical difficulties no longer secure [1]. Quantum cryptography is a kind of physical cryptography, which uses the intrinsic physical quantities of information carrier and its quantum mechanical properties to protect the loaded key information, and has provable security [2-3].

The combination of grid services and quantum secure communication technology can effectively improve the security of grid service delivery. However, due to the long transmission distance of power information and the overhead lines, quantum signals are very vulnerable to external environmental factors. In the literature [4], the MDI-QKD protocol based on quantum storage is studied. The research results show that after adding quantum memory cells, the safe transmission distance of MDI-QKD is greatly increased, and the key generation rate is less affected. In the literature [5], the quantum trusted repeater is used to improve transmission distance, which requires the deployment of stations, and has high environmental requirements and large investment. For example, UHV transmission lines in power systems, whose single-span transmission distance is usually 200-400 km, can’t achieve signal relay in the middle. Therefore, this paper firstly introduces the principle of quantum secure communication and analyzes the requirements of the security of the power communication network, and proposes and tests the quantum secure communication technology and scheme applicable to the power communication network.
2. Quantum secure communication

Quantum secure communication mainly uses Quantum Key Distribution (QKD) technology as the core. The BB84 protocol was first proposed by Charles H. Bennett and Gilles Brassard to use two sets of orthogonal states for key distribution. The agreement has been proven to be unconditionally secure [6-8]. However, due to current technical limitations, the preparation of a single photon source is difficult. In general, the attenuated weak coherent light source is used to replace the single photon source. This method makes the communication system have multi-photon, which causes the attack of photon number splitting (PNS) and changes the counting rate of Bob terminal [9-11]. In order to use weakly coherent light as a source for efficient key distribution, Hwang proposed the basic decoy state method in 2003, which was developed by Wang and Lo, Ma and Chen et al. Decoy state can overcome PNS attack. The QKD system based on the decoy state randomly changes the intensity of the weak coherent light source pulse, and the decoy pulse is randomly added to the signal pulse, making Eve unable to distinguish them. Both sides of communication estimate the loss and bit error rate of signal pulses by detecting decoy state error, judge whether there is an eavesdropper (Eve), and finally Alice and Bob produce quantum keys together.

3. Application of quantum secret communication in power grid service

3.1. Security requirements analysis of power grid services

In recent years, there have been a series of major security incidents, such as the attacks on the power grids of Ukraine and Israel, indicating that information technology facilities involving national security such as finance, power, and communications are facing major risks and security threats [12]. In the power system, there is a communication network that operates independently, that is, a power communication network that is an important part of the secondary system of the power grid. It carries important services such as power production, dispatching, marketing, management and etc. It is an important part of the information age transformation and reshaping the combination of power grid production factors.

The dispatching service can realize the remote monitoring of the operation status of power grid, including the sensitive information closely related to the safety of power grid operation. At present, the vertical secure encryption authentication mechanism between schedulers mainly depends on the point-to-point key agreement process in classical cryptography, which still has the risk of being intercepted and cracked. There is a need to introduce quantum secure communication technology to enhance the security of key distribution. For the management of information services, only VPN tunnel technology is used to protect the information transmission. The communication process may be received and monitored. Quantum encryption can be applied to the transmission process of video and voice information to improve the security of videoconference and video consultation. Therefore, from the aspects of communication requirements, confidentiality requirements and the impact of leakage, we can conclude that quantum secure communication technology, as the most secure communication encryption system at present, has broad application prospects in power communication network [13].

Since the transmission between power communication networks is based on overhead lines, quantum signals are very vulnerable to external environmental factors. It is necessary to solve the problem of quantum key generation rate under overhead lines.

3.2. Research on long distance quantum secure communication technology

3.2.1. Long-distance quantum secure communication technology. For the selection of long-distance quantum secure communication technology for power grid services, there are four technologies, polarization coding, phase coding (based on F-M interference ring), continuous variable and differential phase shift [11]. Comparisons are made in terms of ease of implementation, security, stability and performance. [14-16]. For the F-M system is not affected by channel interference, the
phase coding technology is adopted. The response speed of the phase modulator is fast, which can realize fast coding and better solve the birefringence problem, thus increasing the transmission distance [17].

The specific quantum secure communication technology used in this paper is the F-M (Faraday-Michelson) GHz phase modulated quantum secure communication system which has been proved to be suitable for long-distance optical fiber transmission [18].

3.2.2. Long-distance quantum key distribution technology solution. Higher signal transmission rates and longer transmission distances are required during power communication. However, there will be a nonlinear effect when transmitting over long distances. We can add a dispersion compensation module (Dispersion Compensator Module, DCM for short) to the fiber link, which is very simple to operate. Since there are optical connectors on both the input and output, fiber amplifiers can be used to compensate for insertion loss. For example, a doped fiber amplifier is used in a 1500 nm communication system. The DCM is usually placed between two amplifiers. Therefore, in the long-distance quantum secure communication technology of electric power, DCM is added to both transmitter and receiver to meet the needs of dispersion compensation and solve the problem of nonlinear effects. The solution uses a long fiber, a dispersion-shifted fiber, to be wound on a bobbin, which optimizes the fiber used to compensate for dispersion in a 100-km long transmission fiber.

3.2.3. Test. In the test of the grid-specific quantum security communication equipment, the phase modulation coding is implemented by adopting the structure of the F-M ring. It has the characteristics of high key generation rate, long communication distance and good stability, and can achieve stable and efficient quantum key distribution in long-distance optical fiber transmission. In the application of power grid, the main optical fiber is out of the overhead state. Dispersion compensation module is used to reduce the GHz quantum pulse broadening effect caused by dispersion of long-distance optical fibers, so as to improve the final key generation rate. At present, there are two common methods of dispersion compensation for optical fibers, one based on dispersion compensation fiber (DCF) and the other based on chirped fiber grating. This solution mainly uses optical fiber and DCF for testing. The following steps are used to test the length of the overhead fiber line, line loss and end-to-end loss:

1. Take out the QKD device connection of the optical fiber circuit under test;
2. Test fiber line length and line loss with OTDR;
3. Measure end-to-end loss using a portable light source and an optical power meter.

The main test overhead optical fiber is the Shengli Substation to the Datang Power Plant section. The specific connection diagram is shown in Figure 1 and Figure 2.

![Figure 1. Quantum optical channel wiring diagram.](image-url)
Using OTDR test length of optical fiber, source and optical power meter to test end-to-end loss. The test results are as follows.

Test for the length and loss of overhead optical fiber is shown in Table 1.

|                        | Overhead fiber length (km) | Overhead fiber loss (dB) |
|------------------------|---------------------------|--------------------------|
| **Quantum Optical Channel** | 64.93                     | 13.66                    |
| **Synchronous optical channel** | 66.82                     | 15.01                    |

The OTDR test results of the quantum optical channel are shown in Figure 3:

![Figure 3. Quantum Optical Channel OTDR Test Results.](image)

The OTDR test result of the synchronous optical channel is shown in Figure 4:
The total length and loss test of overhead fiber and fiber is shown in Table 2.

### Table 2. The total length and loss test of overhead fiber and fiber.

|                     | Total length of overhead fiber and fiber (km) | Total loss of overhead fiber and fiber (dB) |
|---------------------|---------------------------------------------|---------------------------------------------|
| Quantum Optical Channel | 101.84                                      | 22.79                                       |
| Synchronous optical channel | 101.79                                      | 22.54                                       |

The OTDR test results of the quantum optical channel are shown in Figure 5:

![Figure 5. Quantum Optical Channel OTDR Test Results.](image)

The OTDR test result of the synchronous optical channel is shown in Figure 6:

![Figure 6. Synchronous optical channel OTDR test results.](image)
The total length and loss of end-to-end optical fiber are shown in Table 3:

| Table 3. The total length and loss of end-to-end optical fiber. |
|---------------------------------------------------------------|
| Total length of end-to-end fiber (overhead fiber + End-to-end fiber length and coil fiber + dispersion compensating fiber) (km) | loss (dB) |
| Quantum Optical Channel                                       | 113.93    | 27.98    |
| Synchronous optical channel                                  | 113.87    | 29.14    |

The OTDR test results of the quantum optical channel are shown in Figure 7:

![Figure 7. Quantum Optical Channel OTDR Test Results.](image)

The OTDR test result of the synchronous optical channel is shown in Figure 8:

![Figure 8. Synchronous optical channel OTDR test results.](image)

The results of three groups of tests show that the scheme can compensate the dispersion in 100 km long transmission optical fibers, increase the coding rate of QKD system from 1 kbps@22 dB to 1.96 kbps@27.98 dB, and the insertion loss is only a few decibels, whether in quantum channel or synchronous channel, and add appropriate dispersion compensation module in transmission line.

4. Conclusions
The proposal of quantum secure communication can unconditionally guarantee the security of communication. The integration of quantum key distribution and power network can guarantee the absolute security of power communication services. In the face of an increase in the transmission distance required for the power communication service, the use of a scheme such as adding a repeater cannot be fully realized due to problems such as the decoherence time of the memory [19-20]. In this paper, a dispersion compensation module is added to the system, so as to provide an all-round technical guarantee for the long-distance quantum secure communication technology of power. "Beijing-Shanghai Trunk Line" and "Ningsu Quantum Trunk Line Project" ensure the safe
transmission of information for power communication network. Faced with the needs of all kinds of business in the industry, quantum secure communication needs constant innovation, which is suitable for information security protection in all kinds of industries [21].

References
[1] Shor P W 1994 A Algorithms for quantum computation: discrete logarithms and factoring J. Foundations of Computer Science 2002:12-134
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. 2009 The security of practical quantum key distribution J. Review of Modern Physics 81(3): 1301-1350
[3] Gisin N, Ribordy G, Tittel W, et al. 2008 Quantum cryptography J. Physics 74(1): 145-195
[4] Sunying, Zhaoshanghong 2015 Research on Device-independent Quantum Key Distribution for Long Distance Measurement Based on Quantum Storage J. Acta Phys. Sin 64:14
[5] Quantum repeater accelerates long-distance quantum communication 2017 J. Optoelectronic Engineering, 44(10): 944+1035
[6] Lo H K,Chau H F 1999 Unconditional security of quantum key distribution over arbitrarily long distances J. Science 283(5410): 250-2056
[7] Shor P w, Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol J. Physical review letters 85(2):441
[8] Renner R, Gisin N, Kraus B 2005 Information-theoretic security proof for quantum-key-distribution protocols J. Physical Review A 72(1):012332
[9] Sharma, Vishal, and Subhashish Banerjee 2019 Analysis of atmospheric effects on satellite-based quantum communication: a comparative study J. Quantum Information Processing 18 3 (2019): 67
[10] Sharma V, Banerjee S 2018 Analysis of Quantum Key Distribution based Satellite Communication J. In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2018 Jul 10 (pp. 1-5). IEEE.
[11] Arockia Bazil Raj, Vishal Sharma, Subhashish Banerjee 2019 Chapter 15: "Principles and Applications of Free Space Optical Communication" J. ISBN: 978-1-78561-415-6, IET, UK
[12] Chenhui, Zhuxihixiong and Zhuyichen 2008 Security analysis of quantum communication J. Information Security &Communication Security 30(12):120-121
[13] CASTELVECCHI D 2017 IBM’s quantum cloud computer goes commercia J. Nature 543(7644):159
[14] Ralph T.C 1999 Continuous variable quantum cryptography J. Physical Review A 61 010303
[15] Wanghuaisgeng, Yangjie 2018 Continuous Variable Quantum Secure Communication Technology J. Information Security & Communication Confidentiality (07):86-91
[16] Sharma, Vishal, U. Shrikant, R. Srikanth and Subhashish Banerjee 2018 Decoherence can help quantum cryptographic security J. Quantum Information Processing 207: 1-17
[17] Grosshans F, Van Assehe G and Wenger J, et al. 2003 Qunrum key distribution using Gaussian-modulated coherent states J. Nature 421(6920):238-241
[18] Fanwei, Weishiha and Yangjie 2018 Review of Quantum Secure Communication Technology J. Journal of China Academy of Electronics and Information Technology 13(03): 356-362
[19] Liu, Quyansheng and Liming 2018 Progress in Research and Application of Power Quantum Secure Communication J. Shandong Electric Power Technology 45(08): 29-32+40
[20] China opened the world's longest distance optical fiber quantum communication trunk 2014 J. ZTE Technology 20 (03): 43
[21] Rujia, Wangfeng 2012 Experimental Research on Long-distance Quantum Communication—Taking the First Step of the Development of Practical Quantum Communication Network in China J. Chinese Journal of Academy of Sciences 27(02): 242-243