Research on Point to Point Quantum Secure Optical Fiber Transmission System of Distribution Network Control Signal

Xin MIAO
State Grid Economic and Technological Research Institute Co. Ltd., Beijing 102209, China

***Abstract*—In order to solve the problem of how to protect the confidentiality and integrity of the distribution network control signal transmission security problem, this paper proposes a solution for point to point quantum secure optical fiber transmission system of distribution network control signal. The solution is to combine the quantum key distribution (QKD) with one-time pad to realize the secure communication of the point to point of the distribution network control and protection signal. The simulation results show that compared with the classical key distribution system, the proposed scheme has the advantage of confidentiality, integrity and identifiability, and has the uniqueness of tightness enhanced. The security support for the interoperability of intelligent distribution network equipment is enhanced, and the security and intelligence level of the distribution network system are improved.**

***Index Terms*—Quantum secure communication, Quantum key distribution, One-time pad, Intelligent distribution network, Control signal, Optical fiber transmission system.**

I. INTRODUCTION

THE development of information and communication technology, especially the technology of quantum secret communication, provides a technological foundation for the improvement of the safety and intelligence level of distribution network system.

With the continuous development technology of isomerism, interaction and synergy for electric power plant, grid, load, energy storage, in order to achieve data sharing, service interworking and device interoperability, the safety of distribution network will be required to have strong support and support capabilities [1]–[3].

The most important feature of quantum secret communication is unconditional security, which makes cipher text-only attack (CTO) and known-plaintext attack (KPT) invalid. Compared with the classical secure communication, the quantum secure communication has the mechanism of security advantage [4].

The control signals in the distribution network include the control commands, such as the trip command, the cutting machine, and the cutting load and so on. In order to solve the problem of how to protect the confidentiality and integrity of the distribution network control signal transmission security problems, this paper proposes a solution for distribution network control signal of point to point quantum secure optical fiber transmission system. The solution combines the quantum key distribution (QKD) with one-time pad to realize the secure communication of the point to point of the distribution network control and protection signal. The simulation results show that the proposed solution can meet the security requirements of the control signal of the distribution network [5].

Xin MIAO is with the State Grid Economic and Technological Research Institute Co. Ltd. State Grid Office B412, No.18 Bin-He-Da-Dao，Beijing Future Science Park, Beiqijia Town, Changping District, Beijing 102209, P. R. China. Phone: +86 13521389761; e-mail: miaoxin@chinasperi.sgcc.com.cn.

II. RELATIVE MECHANISM

The mechanism of one-time pad is as follows. Let the $\boldsymbol{m}$ be the information bit string for the message to be encrypted, the length is $\boldsymbol{n}$, the $\boldsymbol{k}$ is the information bit string of the encryption key, the length is $\boldsymbol{n}$, the $\boldsymbol{s}$ is the encrypted information bit string (the cipher-text), the length is $\boldsymbol{n}$, then the encryption process of the one-time pad can be expressed as the no-carry module 2 plus algorithm operation.

$$\boldsymbol{s} = \boldsymbol{m} \oplus \boldsymbol{k} \tag{1}$$

The decryption process of the one-time pad can also be represented as a no-carry mode 2 addition algorithm.

$$\boldsymbol{s} \oplus \boldsymbol{k} = \boldsymbol{m} \oplus \boldsymbol{k} \oplus \boldsymbol{k} = \boldsymbol{m} \tag{2}$$

The physical meaning represented by the upper form is that at the receiving end, using the same key $\boldsymbol{k}$ as the sending end, the $\boldsymbol{s}$ cipher-text is carried out without carry on mode 2 plus algorithm operation, which can restore the message $\boldsymbol{m}$.

The idea of the point to point quantum secure optical fiber transmission system for distribution network control signal is to combine quantum key distribution with the one-time pad to realize secure communication of distribution network control signal. The task of the quantum secure communication is to complete the secure and instant transmission of the key ***k***.

The most important feature of quantum secret communication is unconditional security, which makes cipher text-only attack (CTO) and known-plaintext attack (KPT) invalid. That rely on the unconditional security of the 3 basic principle are the Heisenberg's uncertainty principle, quantum no-cloning theorem and non-orthogonal quantum states cannot distinguish between theorem. Therefore, compared with the classical secure communication, the quantum secure communication has the mechanism of security advantage.

The quantum communication system takes a single photon as a quantum signal carrier, uses the decoy state, the BB84 protocol, and uses the weak coherent laser source as the single photon source (that is to ensure that the weak coherent laser contains about 0.1 single photons per pulse). The relationship between the effective key rate and the transmission distance of the quantum key distribution system is as follows.

$$R(l) = R_0 \mathrm{e}^{-l/\lambda} \tag{3}$$

In the formula, the ***l*** is the transmission distance, the unit is km; the λ is the scale parameter related to the platform and protocol, the unit is km; the $\boldsymbol{R}_0$ is the effective key rate when the transmission distance is 0 km, and the ***R***(***l***) is the effective key rate for the transmission distance to get the ***l***.

III. System Solution

This paper presents a solution, a point to point quantum secure optical fiber transmission system for distribution network control signals, as shown in Figure 1. The non encrypted communication channel is a synchronous digital system / multi service transmission platform (SDH/MSTP) transmission network between the site A and the site B. The single directional quantum key channel is a single fiber channel in the optical fiber cable.

The encryption and the decryption unit of the one-time pad are shown in Figure 2. The electric power business password key supports Chinese and international commercial password encryption algorithms, for example, SM1, SM2, SM3, SMS4, SM6 (SCB2), SSF33, data encryption standard (DES), advanced encryption standard (AES), RSA algorithm and so on.

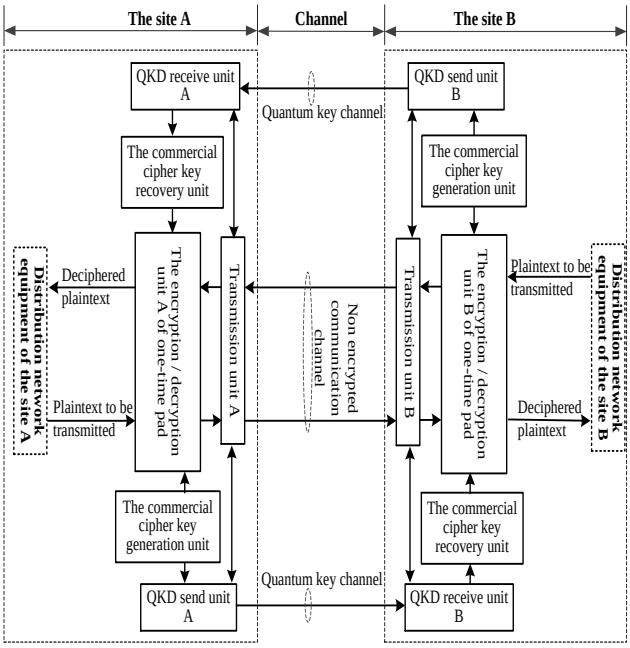

Fig. 1. Point to point quantum secure fiber-optic transmission system diagram of distribution network control signal.

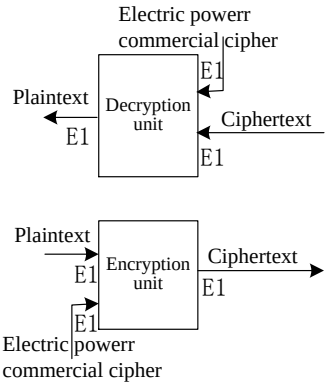

Fig. 2. The encryption / decryption unit structure diagram of one-time pad.

The selection logic for the key generation of the electric power commercial ciphers is shown in Figure 3. The ratio of the rate of cryptographic key output cipher to the quantum key distribution unit cipher key rate is the compression ratio ***r***. When the quantum key distribution system is of good quality, poor quality and poor quality, the key rate compression is 1, 128, and 1024, respectively, compared with ***r***. Usually, the larger the transmission loss of quantum key channel, the worse the quality of quantum channel of quantum key distribution system. The higher the key rate compression ratio is, the larger the ***r*** is.

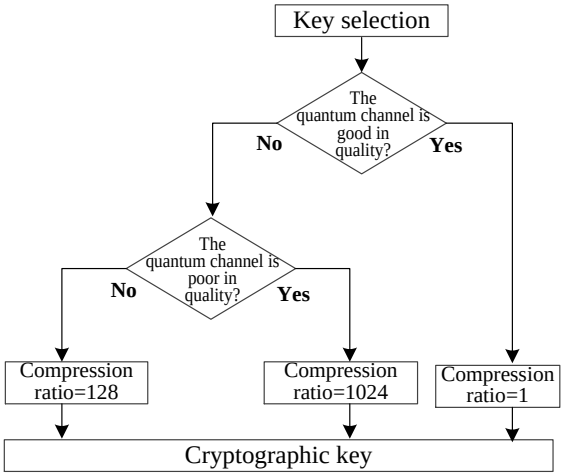

Fig. 3. The key generation selection logic process for power commercial ciphers.

The point to point quantum secure fiber transmission system of distribution network control signal proposed in this paper has the following 4 characteristics.

1) The quantum key distribution is a secure communication way based on the quantum physics principle of key distribution and distribution. It is the use of quantum characteristics to get or improve the secrecy of communication. The scheme proposed in this paper is that the modulation / demodulation mode of quantum key distribution is based on the polarization state encoding, and the quantum key distribution protocol uses a decoy state protocol.
2) The system proposed in this paper is a combination of quantum key distribution and one-time pad to realize the secure communication of distribution network control signals.
3) Based distribution system is proposed in this paper in the application of quantum key and a secret technology, support China and international standards of commercial cipher encryption algorithm, for example, China commercial password management office designated the power business password key SM1, SM2, SM3, SMS4, SM6 (SCB2), SSF33, etc., the international standard password encryption standard DES, AES, RSA, etc. It can not only meet the requirements of relevant policies and regulations, but also adapt to the application needs of individualized and private.
4) The system proposed in this paper adjusts the rate of quantum key distribution according to the quality of the channel, so it has good running characteristics.

IV. Simulation Verification

The QKD unit rate of quantum key distribution system is proposed in this paper for 2048 kb/s, using ITU-T G.652 quantum key channel single-mode fiber optic cable ultra low loss optical fiber, the working wavelength of 1550 nm, the loss coefficient of 0.16 dB/km, the single photon source transmitter with pulsed laser of 1550 nm wavelength, the receiver using M-Z interference instrument. When the key rate compression ratio is r (i.e., the ratio of the key rate to the QKD unit rate) of the power business is 1, 128 and 1024 respectively, the simulation results show that the transmission distance and the key rate of the proposed system are shown in Figure 4.

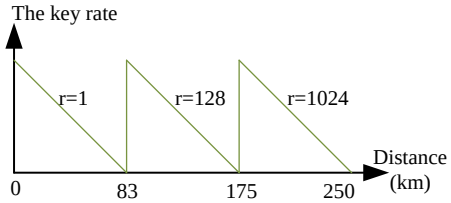

Fig. 4. The relationship between the transmission distance and the QKD key rate in this paper.

The results from the simulation, when the key rate at 1, 128, 1024 compression ratio were ***r***, quantum key distribution unit cryptographic key rate of quantum key distribution system is not less than 2048 kb/s, the maximum transmission distance of the system presented in this paper were 83, 175, 250 km. Its physical meaning is that the longer the transmission distance of the quantum key channel is, the worse the quantum channel quality of the quantum key distribution system is. The larger the key rate compression ratio is, the lower the key source rate of the transmission network is. The key is to ensure the minimum transmission rate of the control signal in the ***r***. The QKD unit rate of quantum key distribution when the system proposed in this paper is greater than 2048 kb/s, and the optical attenuation through the channel in the quantum key, the cryptographic key rate is equal to 2048 kb/s, the optical attenuation can be used as a quantum key distribution system optical attenuation reserve.

Attacks that threaten confidentiality include snooping and traffic analysis. Threat integrity attacks are modification, masquerading, replaying and repudiation. Threat identifiability includes identity authentication and nonrepudiation. The performance of the system compared with the classic key distribution system is shown in Figure 5. For the system proposed in this paper, it has advantages in confidentiality, integrity and identifiability, and has the uniqueness of privacy amplification.

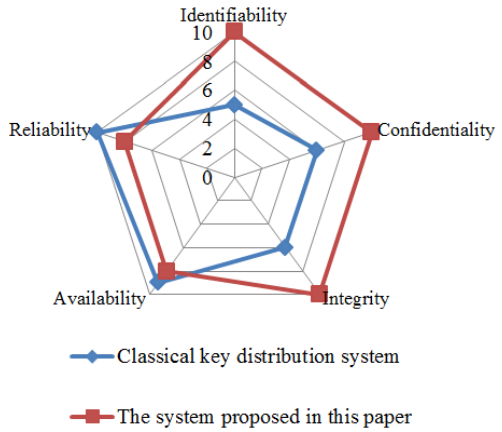

Fig. 5. The performance comparison between the classical key distribution system and the system proposed in this paper.

V. Conclusion

The interoperation of intelligent power grid equipment needs security support, especially in the security protection of distribution network control signal. For example, control commands, such as tripping commands, cutting machines, and cutting loads, need to solve the security problem of how to guarantee confidentiality and integrity of information transmission.

To solve this problem, a solution of point to point quantum secret optical fiber transmission system of distribution network control signal is proposed in this paper, which combines quantum key distribution with one-time pad to achieve point to point communication safely. The solution can meet the delay requirements of all kinds of businesses in IEC 61850, and support both Chinese and international commercial cipher encryption algorithms, which not only meet the requirements of relevant policies and regulations, but also adapt to personalized and private application requirements. It has functional advantages in confidentiality, integrity and identifiability, and has the uniqueness of tightness. The security support for the interoperability of intelligent distribution network equipment is enhanced, and the security and intelligence level of the distribution network system are improved.

References

[1] *Communication Networks and Systems for Power Utility Automation*, IEC Standard IEC 61850-2013.

[2] *Power systems management and associated information exchange-data and communication security*, IEC Standard IEC 62351-2007.

[3] *National Institute for Standards and Technology (NIST). Guidelines for smart grid cyber security: Vol.3, supportive analyses and references*, NISTIR 7628 Revision 1-2014.

[4] J.W.PAN, Z. B. CHEN, C. Y. LU, "Multi-photon entanglement and interferometry," *Reviews of Modern Physics*, vol. 84, no. 2, pp. 777-838, 2012.

[5] X. Miao, X. Chen, "A quantum error correction coding and decoding method for intelligent substation," China invention patent number: ZL201210238511.8, 2016-04-20.

Xin MIAO is a professor in State Grid Economic and Technological Research Institute Co. Ltd. His special fields are information and communication technology in power system, Smart Grid, Energy Internet. Email: miaoxin@chinasperi.sgcc.com.cn.