Application of Quantum Key in Secure Communication for Power Distribution and Utilization

Dongshan Wang, Jian Gao, Huifeng Bai, Licheng Wang, Chao Huo, and Jianan Yuan

***Abstract*—The power distribution and utilization network is an important link between the grid and the user. The data privacy protection is related to the secure and stable communication of the whole network. Based on quantum secure communication and combined with existing power security protection measures, this paper proposed a quantum key application solutions. The system architecture contained the primary station layer, access layer and terminal layer. Through the quantum key distribution network, the key generation devices of both sides of the communication negotiated to generate the quantum key, which was used to encrypt the transmitted data. In the aspect of quantum key distribution, the paper proposed the distribution mode of online distribution and offline distribution, which promoted the flexible distribution of the terminal side quantum key, and realized the low-cost application. The feasibility of the scheme was verified through the pilot application.**

***Index Terms*—Power distribution and utilization, communication security, quantum communication, quantum key distribution.**

I. Introduction

In order to adapt to intelligent electricity systems such as distribution automation, power consumption information collection, and distributed energy, the power grid company has deployed a large number of various types of service terminals and communication terminals. For all kinds of terminals with wide use and wide open environment, the security protection measures are relatively weak. So the attacker can attack the main station through the terminal, as a result of a wider range of security threats [1]-[3].

Quantum secure communication technology is based on the principle of quantum uncertainty and the non-replicable property of quantum state to carry out security key distribution. Attackers cannot measure and replicate the key (quantum state), and it will be found once eavesdropping is carried out [4], [5]. So the quantum secure communication has higher security level than the traditional key distribution mechanism.

However, the existing quantum secret communication system has a low key generation rate and a high cost of quantum key distribution equipment, which is not conducive to the wide application of distributed energy access terminal data security transmission [6], [7].This paper explores the low-cost application of quantum secure communication in the field of distribution electricity by combining the online distribution and offline supplement.

Manuscript received April 15, 2019; revised June 17, 2019.

The authors are with the Beijing Smartchip Microelectronics Technology Co., Ltd, China (e-mail: wangdongshan@sgitg.sgcc.com.cn, gaoj6666@163.com, wanglicheng@sgitg.sgcc.com.cn, baihuifeng@sgitg.sgcc.com.cn, baihuifeng@sgitg.sgcc.com.cn, yuanjianan@sgitg.sgcc.com.cn).

II. Quantum Communication Theory

A. The Properties and Advantages

Compared with traditional communication methods, quantum communication has advantages of high timeliness, strong anti-interference ability, good concealment and low signal-to-noise ratio. Quantum bits have the following properties [8], [9]:

(1) Superposition
For a quantum bit $|\psi\rangle$, it could be either |0 >, or |1 >, or it's superposition.

(2) Imprecision measurement
Heisenberg's uncertainty principle determines that quantum bits cannot be precisely measured.

(3) Non-cloning
Non-cloning ensures that quantum bits cannot be copied by eavesdroppers during communication.

(4) Non-orthogonal state with undistinguishable

If the inner product $\langle\varphi|\psi\rangle$ of two quantum bits $|\psi\rangle$ and $|\varphi\rangle$ is equal to 0, then both are orthogonal. If the inner product is not equal to 0, then both are non-orthogonal. The indivisibility D of $|\psi\rangle$ and $|\varphi\rangle$ can be defined as:

$$D = \left|\langle\varphi|\varphi\rangle\right| = cos\theta \tag{1}$$

where θ is the angle of quantum bit $|\psi\rangle$ and $|\varphi\rangle$, $0<\theta<\pi/2$, if $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal, then they can be distinguished. Adversely they are indistinguishable [10].

B. The Process of Quantum Key Generation

The signal photons sent by Alice and Bob are stored in the quantum memories QMA and QMB respectively. When both memories complete the writing and storage of the photon state, the third party extracts the corresponding bits for BSM. Alice and Bob according to the MDI - QKD base extracted the original security keys. The original key can be passed through the privacy amplification and data coordination process to obtain the final generated key. The generation rate can be expressed as [11], [12]:

$$\begin{cases} R \geq 1/\langle T\rangle \{Q_{11}^{QM}[1-h(e_{11;X}^{QM})]-h(e_{11;Z}^{QM})\} \\ \langle T\rangle = Rs\dfrac{1}{P_{BSM}}\dfrac{3-2P_0}{(2-P_0)P_0} \end{cases} \tag{2}$$

doi: 10.18178/ijiee.2024.14.3.1

where 1/<T> is the original key generation rate. eQM11;Z is the single-photon bit error rate under the Z basis, eQM11;X is the single-photon bit error rate under the X basis, QQM11 is the single-photon gain, Rs is the frequency of laser pulse emitted by both sides of the communication, PBSM is the probability that the third party successfully educe BSM, P0 is the probability that the photon state sent by A and B can successfully reach the third party and conduct quantum storage.

C. Quantum Key Distribution Protocol

Through quantum channel transmission, the quantum key is generated through the negotiation between the two sides of communication, and the classical information is encrypted with this key, which can achieve theoretical secure communication. At present, only two key distribution protocols such as BB84 and B92 are used. BB84 protocol is relatively complex and costly in hardware implementation. In 1992, Bennett put forward the B92 protocol, which realized QKD with two non-orthogonal quantum bits [13], [14].

D. Security Requirements for Power Communication Network

Power communication network is an information and digital network. It's safe and stable operation is the key to ensure power production and distribution. The security requirements in power communication network can be divided into four aspects, data confidentiality, message integrity, non-repudiation and availability [15], [16].In order to ensure the security of the power system, special attention should be paid to the information security of the power grid data, to ensure the security of the information transmission between the headquarters and the deployment stations and units, and to protect the information from being stolen or seen by irrelevant personnel.

III. System Structure Design

At present, the system is configured with ESAM module and encryption machine respectively in the business terminal and the main station. And symmetric key encryption algorithm is used to realize bidirectional identity authentication and data encryption between terminal and main station. In this paper on the basis of the original system, the structure scheme of the power distribution secure communication system was realized by quantum encryption technology as shown in Fig. 1. On the main station side, the encryption and authentication device based on quantum technology was deployed to replace the original encryption and authentication device to encrypt and decrypt business data. Correspondingly, the quantum key encryption module was integrated or external in the terminal device, and the quantum key was used instead of the existing symmetric key to encrypt and decrypt the service data of the distribution terminal.

The system supported the online and offline distribution modes of quantum keys to complement each other. When used as a session key, the quantum key can be injected into the cipher machine of the master station or the encryption module of the terminal to replace the original symmetric key.

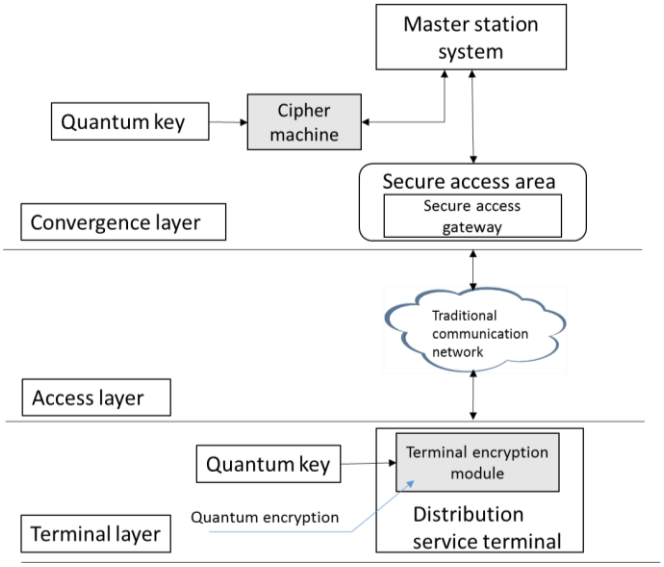

Fig. 1. The structure scheme of electric quantum encryption system.

IV. Quantum Key Distribution Network

A. Online Distribution Network Architecture

The quantum key distribution network was established on the fiber optic network, and the quantum key generation control device and the quantum key management device were integrated into the quantum key server. Among which the quantum key management device provided the functions of quantum key distribution control, quantum key management, key storage, key output and so on.

The quantum cryptographic network was integrated into the power data network, as shown in Fig. 2. A quantum key management device on both the main station side and the aggregation side was built in the key management system. The quantum key management device was connected with the QKD layer quantum key distribution network to realize the key distribution and storage functions. The quantum key management device was connected with the upper quantum key encryption and decryption system to realize key injection and application.

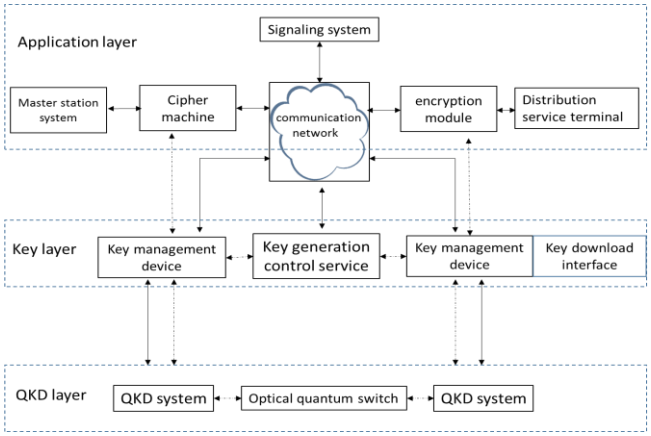

Fig. 2. The architecture of quantum key distribution network system.

In quantum QKD network, it is necessary to adopt trusted relay, quantum relay and so on to realize long-distance transmission. Quantum switch and so on are used to adapt to large-scale network requirements and increase the flexibility of the network.

B. Offline Distribution Network Architecture

For the distribution service equipment with a wide range of points, quantum key equipment can't be directly connected to many service terminals through online mode due to the constraints of volume, cost and other factors. It was supplemented by offline distribution of quantum key mobile storage equipment.

For the master station layer equipment, the pre-application mode could be adopted to realize the quantum key injection. The quantum key generation terminal can inject a certain number of quantum keys into the master station layer equipment for symmetric key matching with the quantum keys injected into the business terminal. Correspondingly, for the access layer quantum key management device, the notification reading mode was adopted to output the quantum key from the device download interface to the third-party security storage medium. And then the third-party security storage medium connected with the physical interface of the distribution terminal one by one to output the quantum key to the distribution terminal. Each distribution terminal had multiple quantum keys, and the quantum keys obtained by each terminal were completely different. In the subsequent business encryption communication process, these pre-stored quantum keys could be used to conduct encrypted communication with the main station business system without the quantum key distribution network. In the "off-line" distribution method, a certain number of quantum keys would be stored in the main station business system and distribution terminals to form a quantum key pool for use in encrypted communication of business data.

V. Quantum Key Application Process

Quantum cryptographic network introduced the process of quantum negotiation, which was used to negotiate whether the quantum key was used as the encryption key or the authentication key, whether the OTP algorithm was used, etc. According to the application requirements, the quantum key server requested and read the key from the quantum server. After receiving the request, the quantum key server determined whether it met the requirements of the request and whether it immediately started the key distribution process, etc. The quantum key application process was shown in Fig. 3 below, including five links and nine steps.

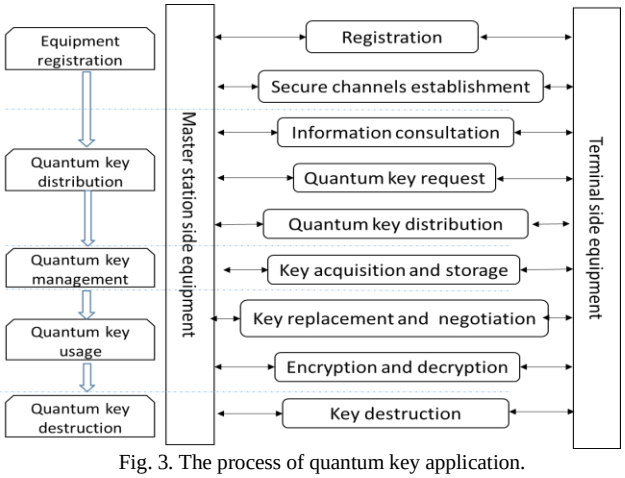

Fig. 3. The process of quantum key application.

VI. Application Validation

In order to verify the performance of the system in the practical application environment, this project selected a distribution website under the jurisdiction of a substation for demonstration application. And the access services included distribution automation and electricity consumption information gathering services [17]. The specific deployment scheme was shown in Fig. 4.

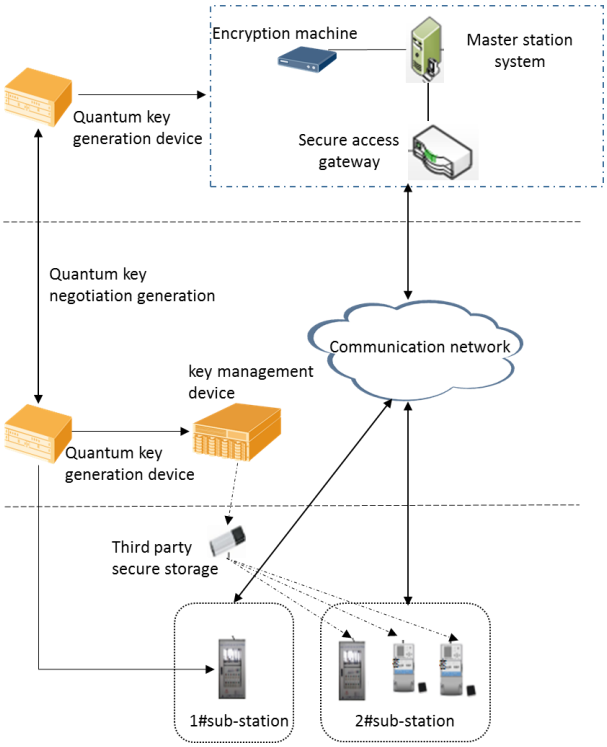

Fig. 4. Application verification of quantum key in power distribution and utilization.

Taking the distribution electricity data service as an example, the end-to-end online key distribution was established as 11kbit/s first, and the initial offline key quantity is 3Mbit, the maximum key capacity is 8Mbit. The minimum unit T of packet sending interval was set as one minute. After the service was launched, the encryption strategy of OTP was adopted to test the encrypted communication performance of the system.

TABLE I: Application Parameters Test Results of Different User

User Category	access delay (s)	Cipher rate (Kbit/s)	Key use rate	Packet loss rate (%)
A(Large special transformer)	0.05	9.78	0.889	＜2.03
B(medium special transformer)	0.05	9.12	0.829	＜1.85
C(Three-phase industry and commerce)	0.06	8.64	0.785	＜1.62
D(Single-phase industry and commerce)	0.06	4.58	0.416	＜1.05
E(Residential users)	0.09	4.18	0.380	＜0.96

For different types of users, on the premise of meeting the requirements of cipher text transmission rate, the access delay, cipher text transmission rate and packet loss rate

were shown in the Table I. The packet loss rate of the whole network was less than 2%, and the access delay fluctuates were within the range of 0.5-0.9, meeting the requirements of power system communication design technical regulations.

Due to the complexity of communication system and the electricity business terminal points widely and density, so we need to improve system capacity to meet the needs of vast users, Set the standard transmission rate was: 9.6, 19.2, 38.4, 56.0, 64.0 Kbit/s [18]. The result of system capacity test was show as Table II.

TABLE II: SYSTEM CAPACITY TEST

Transmission rate class (kbit/s)	Access delay (s)	Packet loss rate (%)
9.6	＜1	＜1.98
19.2	＜1	＜2.15
38.4	＜1	＜2.42
56.0	＜2	＜2.63
64.0	＜2	＜3.36

The actual measurement data of the equipment were basically consistent with the theoretical value of the design. The average uplink transmission rate measured in the field could reach 64kbit/s under the condition of meeting the requirements of QOS index, with the potential for further improvement. At the same time, the feasibility of the scheme was verified and the practical level of the system was improved.

VII. SUMMARY

In the power industry, quantum communication had been included in the national power information system construction plan as an effective way to guarantee the information security of the industry, Identity authentication, data encryption and other security measures were implemented by using quantum secure communication technology. It is of great significance to improve the security and protection ability of service data.

Based on quantum communication technology, in view of the electrical terminal with the characteristics of large number, wide distribution, the quantum key distribution pattern of online and offline was put forward. The system architecture and deployment met with electric business safety requirements, and realized the quantum secret communication technology with lower cost and large-scale application in electrical business. It can effectively enhance the ability of power system to resist communication destruction and invasion by high performance computer.

ACKNOWLEDGMENT

Project Supported by the Science and Technology Project of State Grid Corporation of China: (Research and Development of Power Quantum Secret Chip, 546816180014)

REFERENCES

[1] L. Zhenya, *Smart Grid Technology*, Beijing: China Electric Power Press, 2010.
[2] State Grid Corporation of China. "Q/ GDW480-201 Distributed power supply access grid technical regulations," Beijing: China Electric Power Research Institute, 2010.
[3] State Grid Corporation of China. "State grid corporation of China's "13th five-year" communication network planning," Beijing: State Grid Corporation of China, 2016.
[4] Z. Dongxia, Y. Lliangzhong, and M. Wenyuan, "Development strategy of smart power grid at home and abroad," *Chinese Journal of Electrical Engineering*, pp. 31:1-16, 2013.
[5] D. Fuguo, "Research on quantum communication theory [D]," Beijing: Tsinghua University, 2004.
[6] W. Hua, W. Xiangbin, and P. Jianwei, "Current situation and prospect of quantum communication," *Chinese Science: Information Science*, vol. 44, no. 3, pp. 297-310, 2014.
[7] X. Huaxing, "Overview of the development of quantum communication network," *Journal of China Academy of Electronics and Information Technology*, vol. 9, no. 3, pp. 259-271, 2014.
[8] L. Junwen, Z. Ziyan, X. Huiming *et al.*, "Application of quantum communication technology in secure transmission of power information system," in *Proc. 2016 Annual Conference of Power Industry Informatization*, 2016.
[9] W. Shuang, "Research on key technologies of optical fiber quantum key distribution," Hefei: University of Science and Technology of China, 2011.
[10] Z. R. Rui, Z. Jing, and C. N. Xi, "Application prospect of optical fiber quantum key distribution technology in power grid," *Telecommunications for Electric Power System*, vol. 33, no. 10, pp. 1-4, 2012.
[11] C. Han, L. Xing, J. Xinyi, S. Tianyu, L. Wen, and L. Peishun, "Application of quantum communication technology in Transmission system," *The Grid Technology*, vol. 3, no. 39, pp. 301-304, 2018.
[12] S. Ying, Z. Shanghong, and D. Chen, "Measurement device independent quantum key distribution network based on quantum memory and entangled photon sources," *Acta Optica Sinica*, vol. 3, no. 36, pp. 1-3, 2016.
[13] M. Muller, S. Bnunnuar, K. D. Jnns *et al.*, "On demand generation of indistinguishable polarization-entangled photon pairs," *Nature Photonics*, vol. 8, no. 3, pp. 224-228, 2014.
[14] M. Sasaki, M. Fujiwara, H. Ishizuka, *et al.* "Field test of quantum key distribution in the Tokyo QKD Network," *Quantum Electronics Conference&Lasers and Electro-Optics*, IEEE, 2011, pp. 506-510.
[15] C. Hua, "Principle experiment and technical research on quantum key distribution," Hefei: University of Science and Technology of China, 2016.
[16] K. Mets, "Combining power and communication network simulation for cost-effective smart grid analysis," in *Proc. IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1771-1796, 2014.
[17] W. Yong, L. Shaocong, and C. Baoren, "Application and development analysis of power communication service," *Power System Communicatio*n, vol. 31, no. 217, pp. 44-47, 2012.
[18] H. Yahui and L. Guofeng, "A cross-layer video transmission scheme with guaranteed end-to-end qos over mimo ofdm systems," in *Proc. IEEE International Conference on Multimedia and Expo*, 2012, pp. 207-210.

Dongshan Wang was born in 1965 in Jiangsu, he is a senior engineer. He is the deputy chief engineer of Beijing Smart Chip Microelectronics Company Limited. The main research area is information communication.

He won the second prize of group science and technology progress award and the first prize of China electric power science and technology award.

Jian Gao was born in Shandong in 1982, he is a senior engineer with a doctor's degree. He graduated from China University of Petroleum in 2011, majoring in power system automation.

Through participating in and presiding over the project, he obtained a number of authorized patents and published more than 10 high-level academic papers.

Huifeng Bai was born in Fujian province in 1982. He is a senior engineer with a doctor's degree, and he graduated from Beijing University of Posts and Telecommunications in 2011, majoring in information and communication.

He has won the national electric power workers science and technology achievement award, the first prize of Liaoning province science and technology achievements.