Research on the Fusion Architecture and Application Mode of Quantum Cryptography and Classic Cryptography

Guochun Li, Dong Wang
State Grid Information and Telecommunication branch
Beijing, China
8613331025369
8615901524796
liguochun@sgcc.com.cn
dong-wang@sgcc.com.cn

Can Cao, Hao Qin
Anhui Jiyuan Software Co.LTD
Hefei, China
8618356098926
8613966726987
953284287@qq.com
qinhao@sgitg.sgcc.com.cn

Li Zhang, Guanghuai Zhao
State Grid Beijing Electric Power Company
Beijing, China
8613910587800
8618500139500
zhangli@bj.sgcc.com.cn
zhaoguanghuai@bj.sgcc.com.cn

ABSTRACT

Quantum private communication has promoted the progress of key distribution technology. However, the practical quantum private communication technology only realizes the secure key distribution for symmetric cryptosystem, and can't realize the safe transmission of asymmetric key directly. It is difficult to form complete application architecture of quantum cryptography, and it cannot give full play to the strong security capabilities of quantum private communication infrastructure. This paper constructs a fusion of quantum cryptography and classical cryptography, and designs an application model of quantum cryptography cloud service platform. Based on the present technology, it extends the distribution range of quantum cryptography, and can realize the effective fusion of asymmetric cryptography, cryptographic hashing and quantum cryptography. It has positive guiding significance for constructing new network security defense with quantum private communication technology.

CCS Concepts

Hardware →Emerging technologies→Quantum technologies → Quantum computation→ Quantum communication and cryptography

Keywords

Quantum private communication; BB84 protocol; Quantum cryptography; Classic cryptography; Cryptography cloud service platform.

1. INTRODUCTION

With the further development of information technology, the dependence on network environment and network resources of government agencies, enterprises and ordinary people is deepening, information disclosure, hacking, computer virus transmission and other security problems follow. As the core technology of security information security, cryptography is constantly infiltrating more and more fields. The use of cryptographic technology not only guarantees the confidentiality and integrity of information, but also prevents information from being tampered, falsified and counterfeited. In April 2017, the State Cryptography Administration announced the "The Draft of People's Republic of China Code Law", which defined the mandatory cryptography protection requirements of the national key information infrastructure.

However, the leapfrog development of current quantum technology causes enormous threats and challenges to traditional cryptography security. How to deal with the cryptography technology changes set off by quantum technology has aroused widespread concern in many domestic and foreign research institutions and scholars.

China attaches great importance to the development and research of quantum technology, the quantum technology research is regarded as one of the major scientific research program in "Outline of the national medium and long term science and technology development program"; Quantum private communication and the construction of air-ground integration information network are listed in top ten key projects to spread by "Outline of the 13th Five-Year Plan". The Ministry of Science and Technology, Chinese Academy of Sciences and other scientific research supervisor units have made strategic forward-looking plans for the field of quantum information, which has guided and planned the development of quantum information technology at the policy level.

Recently, the domestic researches in the field of quantum information are frequently reported, and the applications of quantum private communication in real scenario are also in full swing: the world's largest quantum private communication network "quantum communication experiment demonstration network in Hefei" has been completed; The "Beijing-Shanghai trunk line" is about to carry out engineering acceptance and enter the stage of business application, it will be used in finance, electricity, government and other fields to achieve private communication of key business. In 2016, the quantum science experimental satellite "Mozi" successfully launched and

ICSET 2017, October 12–14, 2017, Chengdu, China

ACM ISBN 978-1-4503-5376-2/17/10…$15.00
DOI: https://doi.org/10.1145/3157737.3157741

stabilized, recently the Chinese Academy of Sciences will publish the related experimental results of "Mozi".

2. CLASSIC CRYPTOGRAPHY SYSTEM

The classic cryptography system is generally divided into symmetric cryptosystem and asymmetric cryptosystem. The algorithm of symmetric cryptosystem is open, and the encryption key and decryption key can be easily deduced from each other. Since the United States published data encryption standard DES in the 1970s, cryptographic technique has entered a rapid development stage, the typical symmetric cryptosystem has DES, 3DES, IDEA, AES and so on. The symmetric cryptosystem has a small computational effort, fast encryption speed, and high encryption efficiency, but it still has a flaw that the safe of key distribution cannot be guaranteed, and the emergence of asymmetric cryptosystem help solve this problem.

The asymmetric cryptosystem is also called public key cryptosystem[1], the encryption algorithm and the encryption key (public key) is public, but the decryption key (private key) is confidential and cannot be derived from the public key, or it is almost impossible to derive the private key from the public key through computing, for example, the RSA algorithm which most widely used in the public key cryptosystem is based on the difficulty of large number factorization.

The cryptosystem core algorithm mentioned above were proposed by foreign scholars, considering the protection of the safe operation of commercial cryptography, the State Cryptography Administration has developed a series of domestic cryptography standards, including SSF33, SM1, SM2, SM3, SM4, SM7, SM9, the Zu Chongzhi cryptography algorithm and so on. Among them, SSF33, SM1, SM4, SM7 and Zu Chongzhi cryptography are symmetric algorithms; SM2 and SM9 are asymmetric algorithms; SM3 is a hash algorithm. Here are some of the algorithms for a brief introduction.

2.1 SM1 Symmetric Algorithm

SM1 algorithm is a block cryptography algorithm, the packet length is 128 bits, the key length is 128 bits, the algorithm security strength and related hardware and software performance equivalent with AES, and the algorithm is not public, only in the form of IP core exists in the chip.

2.2 SM2 Elliptic Curve Public Key Cryptography Algorithm

SM2 algorithm is based on the computational complexity of ECC elliptic curve algorithm, but it is different from ECDSA and ECDH in terms of signature and key exchange, it adopts a more secure mechanism. In addition, SM2 recommends a 256 bits curve as a standard curve.

2.3 SM3 Algorithm

The SM3 algorithm gives the calculation method and calculation steps of the hash function algorithm, and gives a calculation example. This algorithm is used to protect the integrity of information and the validity of digital signatures. It can realize the generation and verification of message authentication codes and generate random numbers, which can meet the security requirements of multiple applications. It is usually used in conjunction with SM2 and SM9 cryptographic algorithm.

2.4 SM4 Symmetric Algorithm

The algorithm is a packet algorithm with a packet length of 128 bits and key length of 128 bits. Both the encryption algorithm and the key extension algorithm adopt 32 rounds nonlinear iterative structures. The decryption algorithm has the same structure as the encryption algorithm, except that the decrypted round key is reverse order of encrypted round key.

Whether the cryptography system or domestic cryptography system put forward by foreign scholars, the security algorithm based on computational complexity is relatively safe for the reason that the computing capacity is limited in now time, but the concept of quantum computer to bring this algorithm serious threat, once the quantum computer into the practical stage, the current use of the cryptography algorithm will be easily broken, the communication will not have any security at all.

3. QUANTUM CRYPTOGRAPHY SYSTEM

Quantum cryptography system actually solve the key distribution problem which the classic cryptography system facing. The classic cryptography system can only achieve the computational security of key distribution rely on public key cryptography, but quantum cryptography system can achieve unconditional security, the most basic protocol of quantum cryptography system is BB84 protocol [2].

The BB84 protocol is not only a quantum private communication protocol that has gone into practical process, but also the basis of other quantum private communication protocols[3]. The protocol explicitly states how the sender and receiver generate the same quantum cryptography at both sides by transmit the polarization state. Alice uses the quantum channel to transmit the photon in polarization state and Bob measures the polarization state of the photon with basis vector. Then, Bob proofread the correctness of basis vector with Alice through a classical channel (such as the Internet), only reserve the measured effects use correct basis vectors, and the rest discarded. Finally, two sides securely get same cryptography. Theoretically, in the case of transmitting enough photons, the bit error rate of quantum key tends to 25%. Don’t worry about the security of classic channel, the threat that both of the channels would be eavesdropped by Eve has full considered in the design of BB84 protocol [4].

In terms of the quantum channel, once Eve eavesdrops on the channel, it is necessary to measure the state of the photon. According to the quantum indivisibility, uncertainty principle and no-cloning theorem, Eve cannot completely reproduce the quantum state of captured photon. So Eve's measurement will inevitably increase the bit error rate. If the bit error rate of quantum key is within a certain range, error correction can be carried out by using error correction technology, then privacy amplification is used for the key after correction, above methods can eliminate the information leakage caused by the communication process and error correction process, so as to extract the unconditional security keys [5]. If the bit error rate exceeds a certain range, then give up this key. Alice and Bob regenerate the absolutely secure quantum key for communication.

This work was supported by the Program of Beijing Municipal Science and Technology (Z171100001217002).
Project title: Research of quantum key anti-interference transmission technology in power communication.
Communication author: Dong Wang (dong-wang@sgcc.com.cn)

4. COMPARISON BETWEEN QUANTUM CRYPTOGRAPHY AND CLASSIC CRYPTOGRAPHY

Current quantum cryptography can achieve the key distribution of symmetric cryptography in the practical application, but signature, verification and other security services cannot be carry out effectively with symmetric cryptography. The classic cryptography system also contains asymmetric cryptography and cryptographic hashing. Cryptography system and application scenarios are complete, but safe cryptography distribution ways are lacking.

Table 1. Compasion between quantum cryptography and classic cryptography

Contrast content	Classic cryptography	Quantum cryptography
Type	Symmetric cryptography; Asymmetric cryptography; Cryptographic hashing	Symmetric cryptography
Transmit content	Encrypted information	Quantum signal
Anti-eavesdropping function	Eavesdropping cannot be detected	Once eavesdropping must be found
Transport channel	Ordinary fiber channel	Independent fiber channel
Eavesdropper gains	Get encrypted information that can be cracked by immediate or post-operational.	The eavesdropping of quantum information is a useless signal that is discarded by both parties and does not participate in the assembly of the key, and has no association with the key.

5. FUSION OF QUANTUM CRYPTOGRAPHY AND CLASSICAL CRYPTOGRAPHY

Shannon proposed an OTP encryption method in his paper: the encryption key is generated randomly, its length is as same as plaintext, and they do exclusive-or operation to achieve the encryption of plaintext. The encryption key is destroyed after used just once. Whether it is symmetric key or asymmetric key, the quantum key distribution system is absolutely secure that it can realize the secure key distribution.

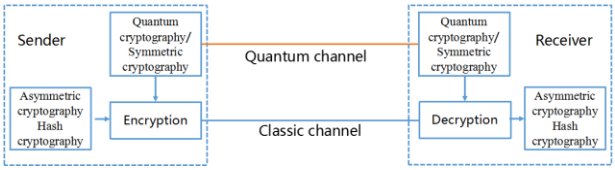

Figure 1. Fusion of qumtum crtyptography and classical crtyptography.

However, the current technology of quantum private communication can only achieve the safe distribution of symmetric key in practical application. It can only do point-to-point encryption and cannot full display its powerful security capability of quantum communication network infrastructure. In the traditional PKI technology, the asymmetric cryptography algorithm can not only be used for information encryption, but also can be used for digital signature and authentication. The sender use private key to sign the information, the receiver use public key to decode to authenticate the reality of the signature. The asymmetric key pair can be generated online and the public key is exposed to the public after CA sign for it. However, the private key distributing online faces the threat of monitoring and theft. Therefore, the private key is usually stored and distributed offline by physical media, but the efficiency of this way is too low to satisfy the increasingly high requirements for cryptography applications [6].

Hash function is able to change any long input message string into a fixed long output string, it can be used for integrity checking, and improve the validity of digital signature. The use of quantum cryptography in asymmetric cryptography and cryptographic hashing for one-time pad distribution can expand the application of quantum cryptography.

On the basis of Shannon's one-time pad theory and quantum private communication key distribution system, based on the technique of cloud computing and the concept of hierarchical design, this paper designs a kind of easy-to-use, safe and efficient commercial cryptography cloud service architecture to realize the unified specification, unified interface, unified service of various cryptographic applications such as identity authentication, digital signature, data encryption and so on. The cryptography services provided by the technology architecture system have following characteristics:

1）Centralized generation: According to the provisions of the State Cryptography Administration management, the cloud cryptography machine generate domestic cryptography based on SM series centrally, asymmetric algorithm SM2, SM9 can combined with hash algorithm SM3 and symmetric encryption algorithm SM4 for different security application scenarios.

2）Unified management： After the cryptography being generated centrally, the management module is used for unified management. Then corresponding services are provided for different cryptography requirements.

3）Secure distribution： The cryptography management module stores the cryptography generated by the cryptography machine and distributed it through the quantum key distribution system to the users, to ensure the security of the cryptography in the distribution process.

4）Standard application：The cryptography requirements of the users are reported through the cryptography service interface

of the middleware. The cryptography infrastructure is virtual and transparent to user. Cryptography is only a service to achieve the user's requirements like online identity authentication, digital signature, data encryption and so on.

6. QUANTUM CRYPTOGRAPHY SERVICE CLOUD CLATFORM

According to the fusion architecture of quantum cryptography and classical cryptographic, relying on cloud computing platform and the infrastructure of quantum private communication network to form a quantum cryptographic service computing resource pool, then building an application model based on SaaS to achieve cryptographic service system. That is, through the cryptography unified production, security distribution by quantum private communication, and standard cryptography service in cloud environment, to construct a cloud service platform of domestic cryptography algorithm based on quantum private communication [7].

Quantum cryptography service platform contains:

1）Key generation center：Make the cryptography devices, universal cryptography resources and cryptography applications abstract, it can provide high reliable, high availability and scale scalable cryptography service to meet the requirements of a variety of cryptography applications. According to the regulations of State Cryptography Administration, the cryptography machines in cloud environment generate domestic asymmetric key, symmetric key and hash key unified. Distribute the keys through quantum key distribution system. The cloud computing SaaS mode provides quantum cryptography operations and service interfaces to guarantee cryptography security for service application systems in whole life cycle.

2）Security middleware：The security middleware provides interfaces to access the service of cryptography machine for cloud users. It supports the access control code protection, the load balancing, the fault-tolerant mechanism, the state collection, the log report and so on. The use of cryptography service should be authorized, so the identity of cloud users should managed unified. The use of cloud cryptography services need to have a corresponding security policy and according to the appropriate security policy to license cloud users, only authorized customers can access the use of cloud cryptography services. We can use the management method based on the role, according to the characteristics of cloud users delineated several types of user roles, different role have different cryptography service permission.

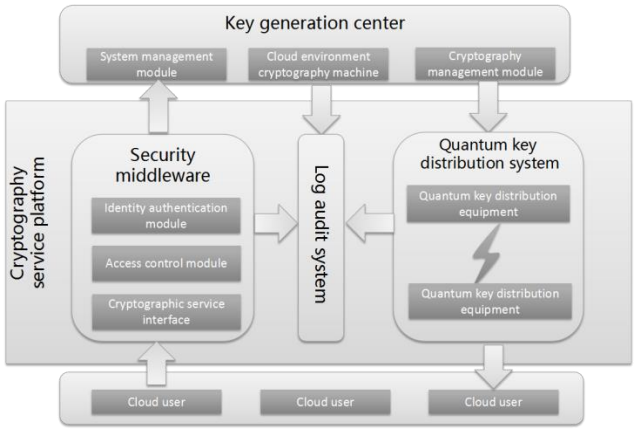

Figure 2. Quantum cloud cryptography service platform.

3）Quantum key distribution system：Provide the functions of quantum key generation, quantum key management, classic key distribution and so on, ensure the absolute security of the classic key in the distribution process.

4）Log audit system：For key management, the use of key (encryption, decryption, signature, etc.), system load, business system access calls and operational abnormalities, conduct detailed log records and provide visual management.

Quantum cloud cryptography service platform provide data and file encryption interface, signature and verification interface through the security middleware. Cloud applications system can use these interfaces implement such as authentication, digital signature, verification, file encryption and decryption, streaming encryption and decryption, channel encryption and other security applications easily[8].

7. BUSINESS APPLICATIONS

The following will use the electrical power system as an example to describe the business applications of quantum cryptography cloud service platform. in detail. The power business system is clearly classified as a key information infrastructure by the Ministry of Public Security and mandatory cryptography protection must be implemented. In accordance with the provisions of the State Cryptography Administration, the SM2/3/4/9 application key and user key would be unified generated from the cryptography machines in cloud environment. The asymmetric algorithm SM2 and SM9 can be combined with hash algorithm SM3, symmetric encryption algorithm SM4 to use in different security application scenes[9].

The power system is divided into production control area and information management area, physical isolation between two areas. So we need to build two sets of quantum cryptography cloud service platform, applied to the production control area and information management area respectively. Take the three places disaster recovery in the information management area as an example, the information of production, management, configuration in power production system all need to be transferred to the disaster recovery center for backup. At present, the backup mode is mostly using plaintext transmission mode, the security level is very low and the external threat is very serious. Building a quantum cloud platform to provide cryptography services could protect the transmission process of disaster recovery business in the cloud environment. The

deployment architecture of quantum cloud platform for three places disaster recovery services as shown below:

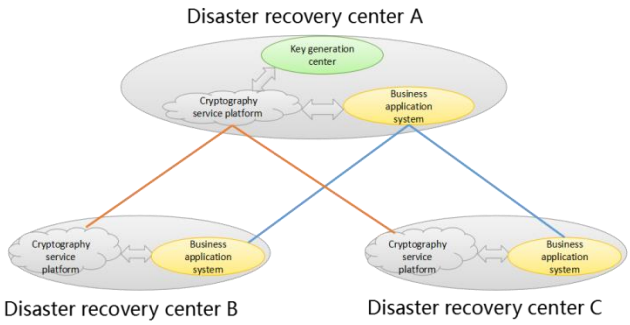

Figure 3. The deployment architecture of quantum cloud platform for three places disaster recovery.

8. SUMMARY

This paper constructs the fusion architecture of quantum cryptography and classical cryptography, and designs an application mode of quantum cryptography cloud service platform. Quantum cryptography cloud service platform provides cryptography service based on domestic cryptography algorithm. Cloud users can realize security applications such as data encryption, authentication, digital signature and verification, file encryption and decryption, streaming encryption and decryption, channel encryption and so on through cryptography service interfaces. The proposed fusion architecture and application model of cloud service platform is based on the concept "Password as a service", which can expand the application scope of quantum cryptography in key distribution, reduce the difficulty of cryptographic technology application, and meet the needs of key information infrastructure diversification cryptography protection application.

9. ACKNOWLEDGMENT

This work was supported by the Program of Beijing Municipal Science and Technology (Z171100001217002).

10. REFERENCES

[1] Li, Z.L, Cui, Y.D, Jin, Y.H, and Xu, H.M. 2011. *Parameter Selection in Public Key Cryptosystem based on Chebyshev Polynomials over Finite Field,Journal of Communications*, vol. 6, no.5, pp.400-408. DOI=10.4304/jcm.6.5.400-408

[2] Bennett, C. H and Brassard. 2014. *Quantum cryptography: public key distribution and coin tossing, Theoretical Computer Science*, vol. 560, pp.7-11.

[3] Hsu, J. L, Chong, S. K. and Hwang, T.2013. *Dynamic quantum secret sharing*, Quantum Inf. Process, vol. 12, pp. 331-344.

[4] Shor, P. W and Preskill, J. 2000. *Simple proof of security of the bb84 quantum key distribution protocol*, Physical Review Letters, vol. 85, pp. 441-447.

[5] Wang, J. and Guo, J. H. 2015.*Review on information and communication key technologies of energy Internet,* Smart Grid, vol.3, pp. 473-485.

[6] Lydersen, L and Wiechers, C.2010. *Hacking commercial quantum cryptography systems by tailored bright illumination*, Nature Photonics, vol.4, pp.686-693.

[7] Gottesman, D and Lutkenhaus, N.2004. *Security of quantum key distribution with imperfect devices*, Quantum Information and Computation, vol. 4(5): 325-360.

[8] Maurya, A. K, Mishra, M. K and Prakash, H.2016. *Two-way quantum communication: Generalization of secure quantum information exchange to quantum network*. Pramana, vol. 86(3), pp. 515-526.

[9] Zhang, Y. Y and Zhang, S. X. 2016. Q*uantum communication and its application in power communication*, Electric Power Information and Communication Technology, vol.14, pp. 7-11.