Application exploration of Quantum Security Service Platform based on Quantum Key Distribution

Rutong Zhang, Zhining Ye, Guoliang Yang, Xuefu Wang
QuantumCTek Co., Ltd.
No.777 Huatuo Lane, High-tech Industrial Development Zone, Hefei, Anhui, China
rutong.zhang@quantum-info.com

Abstract

Quantum key distribution can produce real-time quantum keys between nodes in different places. Its application is limited by the optical fiber environment and cannot be directly applied to mobile Internet or Internet of Things. This paper describes the application of quantum keys to mobile Internet or Internet of Things(IoT) through the preset key protection mechanism of classic cipher . And applied in specific scenarios such as email encryption, video conference encryption, and mobile terminal encryption.

Key words QKD Preset key Mobile/IoT application encryption

1. Related background

1.1 Requirements of the cipher system

The cipher system requires long-term security[1]. The cipher system needs to be able to remain secure for a long time in the future. It means that even if the attacker gets a lot of computing resources, it is still impossible to crack.

1.2 Limitations of the asymmetric cipher system

In December 2023, IBM released a quantum computing chip with 1,121 superconducting qubits. With the rapid development of quantum computing, the public key cryptography system based on difficult mathematical problems such as mass factor decomposition and discrete logarithm faces great challenges.

1.3 Limitations of Quantum Key Distribution

As an anti-quantum attack technology[2], the Quantum Key Distribution technology has the application conditions of providing OTP. Can provide solutions with the unconditional security of information theory. However, the deployment of Quantum Key Distribution should have certain optical fiber resources, which cannot be applied to application scenarios such as mobile Internet or Internet of Things.

1.4 Generation of Quantum Security Service Platform

This paper proposes to combine Quantum Key Distribution and cipher management to build Quantum Security Service capabilities, so as to provide cipher applications with

Z. Zheng and T. Wang (eds.), *Proceedings of the International Academic Summer Conference on Number Theory and Information Security (NTIS 2023)*, Advances in Physics Research 9,
https://doi.org/10.2991/978-94-6463-463-1_6

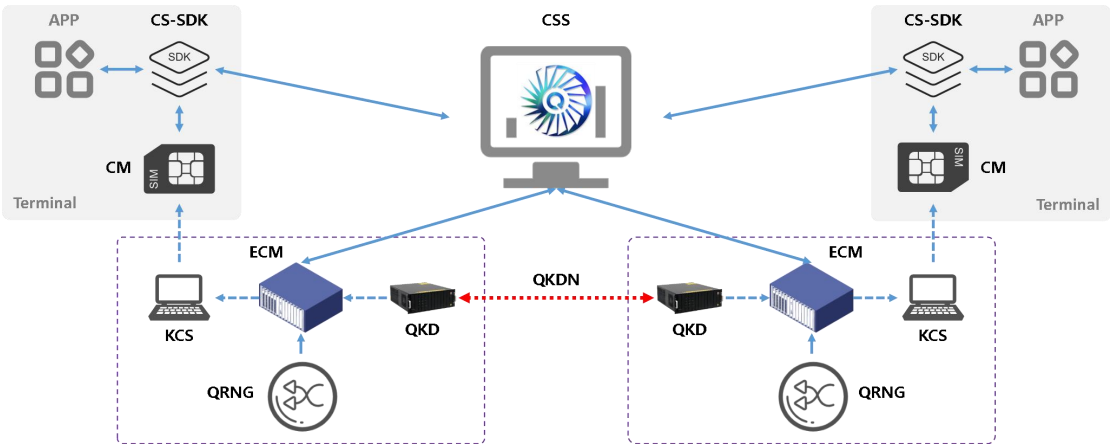
long-term security for applications such as mobile Internet or Internet of Things.
Solve the distribution problem of the last kilometer of the quantum key.

2. How the Quantum Security Service Platform works

2.1 Overall system architecture

Quantum Security Service Platform is a set of cipher service platform with quantum security features for mobile Internet, Internet of Things and other scenarios. The platform includes Quantum Key Distribution Network(QKDN), Quantum Random Number Generator(QRNG), Cipher Service System(CSS), Exchange Cipher Machine(ECM), Key Charging System(KCS), Cipher Module （CM） , and Cipher Service Software Development Kit(CS-SDK).

The architecture diagram of the Quantum Security Service Platform is shown in the figure below



2.2 Description of each component of the platform

The Quantum Security Service Platform provides the cryptographic service with quantum security characteristics for the mobile Internet or the Internet of Things through the key pre-charging technology and the one-time pad key distribution over internet technology.

The key managed by the platform[3] is generated by the Quantum Key Distribution Network or the Quantum Random Number Generator. The security and randomness of the quantum key generation are guaranteed by QKD technology, and the randomness of the quantum key is guaranteed by QRNG.

Cipher Service System is the core control and management system of the Quantum Security Service Platform. Responsible for the operation management of the whole platform, including registration and access authentication management of terminal application, Exchange Cipher Machine, and Key Charging System, full cycle management of issuing key charging, activation and offline key information management of Session Key acquisition between mobile terminals, deployment and management of Exchange Cipher Machine storage key, unified configuration management and state monitoring of the whole network.

Based on the Quantum Random Number Generator and the Quantum Key

Distribution Network and the Exchange Cipher Machine, it provides key services for mobile terminals and other devices to support custom to realize secure communication and other services.

The Exchange Cipher Machine[4] is the core equipment of the Quantum Security Service Platform. It is responsible for obtaining the key of the quantum random number or Quantum Key Distribution Network, storing and managing the key, providing the key to the key charging system, and providing the acquisition quantum key as the session key for encrypted communication.

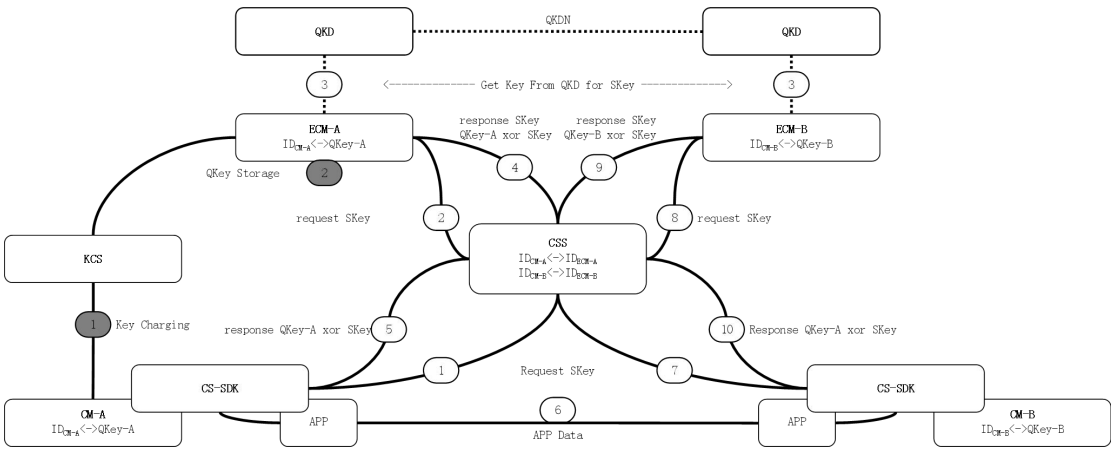
Key Charging System provide account binding and key charging function for Cipher Module.

Mobile terminals use Cipher Module[5] to provide cipher capabilities, responsible for the key storage security, and provide cipher operation. Task services on mobile terminals can use Cipher Module for cipher operation.

The Cipher Service SDK runs in the application, encapsulating the interface of the Cipher Module and the interactive interface of the Quantum Security Service Platform, and providing unified key application services to the application layer through the API, including session key acquisition, data encryption and decryption and other functions.

2.2 Brief Description of the working principle

The key management of Quantum Security Service Platform is divided into Key Charging Phase, Getting Session Key Phase and Encryption Phase. The flow chart is shown in the figure below:



Key Charging Phase:

After obtaining the quantum key Qkey from the Quantum Key Distribution Network or the Quantum Random Number Generator, it writes the key to the Cipher Module through the Key Charging System. The Exchange Cipher Machine stores the same quantum key QKey. This partial key is the protection key for the subsequent session key.

Getting Session Key Phase:

Mobile Internet applications through the Cipher Service SDK to the Cipher Service System to get session key, Cipher Service System through the Exchange Cipher Machine from Quantum Key Distribution network to get session key SKey, using the Cipher Module QKey to encryption Skey by OTP, SKey back to the Cipher Service SDK, Cipher Service SDK use Cipher Module cipher ability, import SKey to the

Cipher Module. At this point, the communication parties get the same session key SKey.

Encryption Phase:

By using the interface of the Cipher Service SDK, mobile Internet applications realize the encryption and decryption of data by using SKey in the Cipher Module.

2.3 Safety description

The key source used by mobile Internet applications is the Quantum Key Distribution network, which ensures the security of the key when distributed in the boast region. Through the Cipher Service System and the Exchange Cipher Machine and the Cipher Module, the security of the last kilometer of the key distribution is guaranteed. The cipher operation is carried out in the Cipher Module, and the key is not out of the Cipher Module, which ensures the security in use. The Quantum Security Service Platform extends the OTP capability of the Quantum Key Distribution network, enabling the application of mobile Internet or Internet of Things to easily and safely use the quantum key.

3. Practical application of the Quantum Security Service Platform

Based on Quantum Security Service Platform, expand Quantum-Security Call, Quantum-Security instant communication and Quantum-Security special line in the telecommunication field; expand Quantum-Security mail, Quantum-Security intelligent seal, Quantum-Security video conference in the field of office; expand series products of Quantum-Security intelligent power distribution in the field of electric power; expand Quantum-Security industrial Internet gateway in the industrial Internet field; expand Quantum-Security financial business to home business system in the financial field; expand Quantum-Security headset in the ToC field;

4. Development trend of the future Quantum Security Service Platform

Explore the combination of PQC and QKD, extend the cipher service, provide confidentiality, provide non-denial, tamper-proof and other cipher capabilities.

References

1.Ronald L.Rivest, Adi Shamir, and Leonard M.Adleman.Long-term security of the RSA cryptosysterm.1978.

2.SHANNON C E.Communication theory of secrecy systems[J].Bell System Technical Journal, 1949,28(4):656-715.

3.GMT 0051-2016 Cryptographic device management Symmetric key management technical specification

4.GM_T 0030-2014 Technical specifications for server cryptography machines

5.GM/T 0016-2012 Smart password Key password application interface specification