GTI Analysis of Post-Quantum Cryptography Migration in Telecommunication Networks

White Paper

GTI Analysis of Post-Quantum Cryptography Migration in Telecommunication Networks White Paper

Version:	v_1
Deliverable Type	□ **Procedural Document** ☑ **Working Document**
Confidential Level	□ **Open to GTI Operator Members** □ **Open to GTI Partners** ☑ **Open to Public**
Program	5G ENS
Working Group	5G ENS
Project	Technology development
Task	Vertical industry green and safety
Source members	CMCC
Support members	
Editor	CMCC: Bangling Li, Yan Zhang, Ailiang Ma, Yang Zhang, Ti Zhang, Huaxi Peng, Songquan Shi, Kai Yang, Li Su, Shen He
Last Edit Date	18-4-2025
Approval Date	

Document History

Date	Meeting #	Version #	Revision Contents

Table of Contents

1 Executive Summary

The rapid development of quantum computing technology poses a threat to the security of classical cryptosystems. Gartner predicts that large-scale quantum computers capable of cracking traditional asymmetric cryptographic algorithms will emerge around 2030, threatening the normal functioning of digital infrastructure. The National Institute of Standards and Technology (NIST) has been launching a call for post-quantum cryptographic standard algorithms since 2016 and released three post-quantum encryption standards in 2024. Telecommunication networks are global information cornerstones that support economic and social operations. However, telecommunication networks mostly rely on public key cryptosystems, which can be seriously threatened by quantum attacks. Post-quantum cryptography migration is a complex process, and many difficult issues will be faced during the migration process. The migration may have a greater impact on network functions, performance, bandwidth, etc., and challenge the efficiency and availability of business services. We analyze the existing cryptographic mechanisms and the post-quantum cryptographic migration requirements of the communication network, and give constructive migration suggestions to provide guidance for the post-quantum cryptographic migration of the communication network.

2 Abbreviations

Abbreviation	Explanation
4A	Accounting, Authorization, Authentication,Audit
CA	Certificate Authority
DH	Diffie-Hellman
ETSI	European Telecommunications Standards Institute
EMS	Element Management System
MAN	Metropolitan Area Network
NIST	National Institute of Standards and Technology
RAN	Radio Access Network
SBA	Service-Based Architecture
SEPP	Security Edge Protection Proxy
SSH	Secure Shell Protocol
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
UE	User Equipment
UICC	Universal Integrated Circuit Card
VNF	Virtualized Network Function
VPN	Virtual Private Network
vSEPP	visitor Security Edge Protection Proxy

3 Introduction

Quantum computers realize parallel computing based on quantum superposition characteristics, and their computing power is exponentially improved compared with traditional computers, thus posing a huge threat to cryptographic systems. Google's Willow chip has promoted quantum computing from theoretical verification to practical application through quantum error correction and performance breakthroughs, which means that the arrival of quantum computing threats may be faster than expected.

In terms of daily communication, many key communication protocols (TLS, SSH, DH, etc) are mostly based on public-key encryption, digital signature and key exchange. Once quantum computers become practical, these communication protocols will become less secure and cannot guarantee end-to-end secure transmission.

The impact of quantum computing on common cryptographic algorithms is shown in Table 1. For symmetric cryptosystems, Grover's algorithm has an open square magnitude reduction in the search complexity of the unordered set, and can theoretically halve the security strength of symmetric cryptographic algorithms (e.g., block cipher), and hash functions. However, the quantum threat can be effectively countered by increasing the length of the security parameters, such as doubling the key length for symmetric ciphers or doubling the output length for hash ciphers. For public-key cryptosystems, Shor's algorithm can decompose large integers as well as solve discrete logarithms in polynomial time, which can theoretically completely break the current widely used RSA and elliptic curve public key cryptography algorithms.

Table 1. The impact of quantum computing on common cryptographic algorithms

cryptographic algorithm	**Algorithm type**	**function**	**Affected by quantum computing**
AES	Symmetric Cryptography	Encryption	Requires double the key length
SHA-2, SHA-3	Cryptographic Hash Function	Hash	Requires double output length
RSA	Asymmetric Cryptography	Signature，Key Agreement	Insecurity
ECDSA, ECDH	Asymmetric Cryptography	Signature、key exchange	Insecurity
DSA	Asymmetric Cryptography	Signature、key exchange	Insecurity

The focus of guaranteeing network security and information system security in the era of

quantum computers lies in the development of cryptography. The cryptography community collectively refers to cryptographic algorithms that can resist quantum computing attacks as Post-Quantum Cryptography (PQC). The standardisation of PQC is the basis for promoting the migration of existing cryptosystems to PQC. Stage-by-stage progress has been made in the standardisation of Post-Quantum Cryptography. On 13 August 2024, NIST has officially released three post-quantum cryptographic standards, specifically FIPS 203, FIPS 204, and FIPS 205. FIPS 203 utilises the Crystals-Kyber algorithm, which can be used for transport-layer security protocols, and provides an effective alternative to traditional methods in terms of its fast performance despite the larger public key and ciphertext. FIPS 204, based on the Crystals-Dilithium algorithm, is designed for digital signatures, and is particularly suitable for application scenarios that require larger signatures and public keys, and excels in verification speed. FIPS 205, based on SPHINCS+, is suitable for applications such as firmware updates that require fast verification, with its small public key and large signature.

On October 24 2024, NIST announced the second round of candidate algorithms for quantum resistant digital signature schemes. In this round, NIST selected a variety of quantum resistant algorithms with different technical routes, laying the foundation for the diversification of quantum resistant digital signature schemes. The announcement of the second round of candidate additional digital signature schemes marks an important step in the standardization process of quantum resistant cryptography. These diverse signature schemes will provide strong technical support for quantum-resistant migration in the future and accelerate the global transition to a quantum resistant security system.

Table 2. PQC: Round 2 Additional Signatures

Technical routes	Code-based Signatures	Isogeny Signatures	Lattice-based Signatures	MPC-in-the-head Signatures	Multivariate Signatures	Symmetric-based Signatures
Algorithm	CROSS、LESS	SQIsign	HAWK	Mirath、MQOM、PERK、RYDE、SDitH	MAYO、QR-UOV、SNOVA、UOV	FAEST

4 Analysis of cryptography applications and migration requirements

The telecommunication network contains many systems. In this paper, we take the key systems in the telecommunication network, such as 5G core network, signaling network, optical transport network, time synchronization network and bearer network as cases. The several networks we have selected all have their specific functions and importance, and together they form the basic architecture of modern telecommunication networks. The 5G core network relies on the signaling network for intelligent control, achieving physical connectivity through the transport network, while the bearer network optimizes traffic management based on this; meanwhile, the synchronization network provides an accurate time reference, ensuring coordinated operations across all layers to collectively construct a communication environment that is both robust and flexible.

The 5G core network is the backbone of the telecommunications network, which is responsible for handling key tasks such as call processing, data transmission, mobility management, and session management. The signaling network is responsible for the transmission of the signaling information in the telecommunications network, which controls the establishment, maintenance and release of calls. The optical transport network is responsible for the actual transmission of data between different parts of the network. The time synchronization network ensures that devices in a telecommunications network can maintain time consistency. The bearer network is used to carry user data and signaling, which is usually an IP-based network that can support a variety of services and applications.

Cryptographic mechanisms in the 5G core, signaling, optical transport, time synchronization and bearer networks are key technologies to ensure the security of telecommunications network. In the 5G core network, cryptographic mechanisms are mainly used for user authentication, data encryption and integrity protection. Signaling network, optical transport network, synchronisation network and bearer network cryptographic applications are mainly focused on the authentication and remote management of equipment. In addition, the bearer network carries user data and signaling, and cryptographic applications also include encryption of user

data and protection of bearer paths.

4.1 5G Core Network

The 5G core network plays a crucial role in all 5G networks and is mainly responsible for handling various data transmission, session management, mobility management and other functions. It introduces a service-based architecture (SBA), comprising various Network Functions as Services such as the AMF (Access and Mobility Management Function) and SMF (Session Management Function). 5GC enables dynamic resource allocation and management through network slicing. Leveraging Software-Defined Networking (SDN) and Network Functions Virtualization (NFV), it offers unprecedented flexibility and adaptability, swiftly responding to diverse business scenarios. The 5G core network architecture is shown in Figure 1.

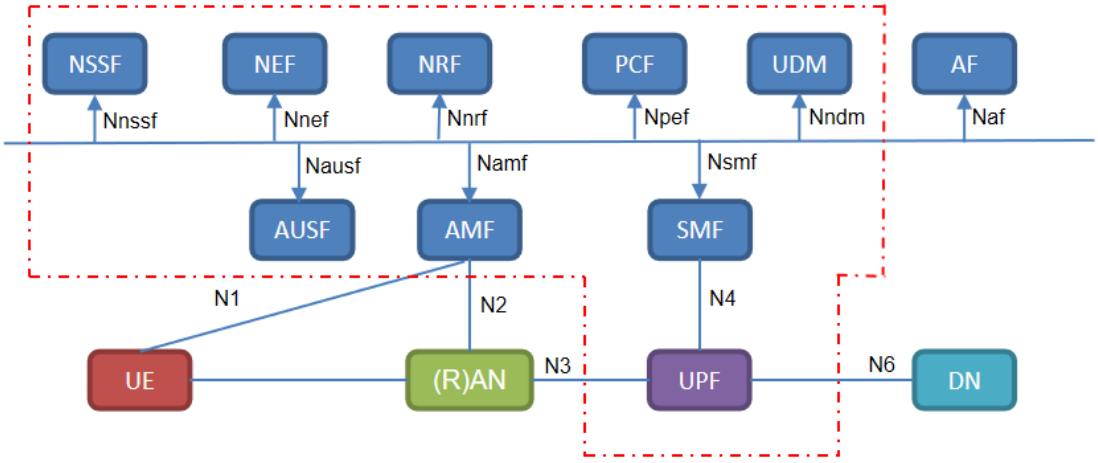

Figure 1. 5G core network architecture

The cryptography application of the 5G core network is relatively comprehensive, involving three technical levels, as shown in Table 3.

Table 3. Cryptography mechanism analysis of the 5G core network

Layer	Object	Cryptographic mechanisms	Algorithms vulnerable to quantum threats in cryptographic mechanisms
Equipment and computing layer	Channel between EMS and the managed equipment	SSH protocol	— DH — RSA, DSA — SHA-2 — AES-128
	Channel between 4A and EMS	SSL VPN	— DH, ECDH — ECDSA, RSA, DSA

			— SHA-2 — AES-128
	Network function authorization access	OAuth 2.0	— RSA — HMAC-SHA256 — AES-128
Network and communication layer	User access authentication	5G-AKA and EAP-AKA' authentication mechanism	— AES-128
	Communication channels between UPF and RAN, and between UPF and DN	Support for the IPSec protocol	— IKE(DH) — RSA, ECDSA — HMAC — AES-128
	Communication channels between the NFs	TLS protocol	— DH — ECC, RSA — SHA-2 — AES-128
	Communication channels between the different operators	TLS protocol	— DH — ECC, RSA — SHA-2 — AES-128
	Transmission channel between UE and RAN, and communication channel between UE and AMF	AES, SNOW 3G, ZUC	— AES-128, SNOW 3G-128, ZUC-128
Application and Data Layer	SUPI	ECC/ECIES	— ECIES — ECC

4.2 Signaling Network

The signaling network acts as a crucial command system within communication systems, not directly involved in data transmission but focusing on conveying control commands to ensure smooth network operation. With the evolution of the communication network, the technology of the signal network is developing continuously. NO.7 Signaling networks are widely used in public switched telephone networks (PSTN) and mobile communication networks (2G). The Diameter protocol is an IP-based signaling protocol commonly used in mobile communication networks such as 3G and 4G. The 5G signaling network is the signaling infrastructure for the fifth generation of mobile communications technology, using a series of new signaling protocols and architectures, such as SBA and SMF.

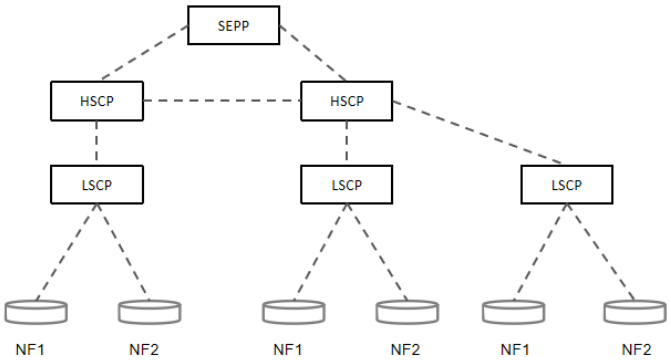

Figure 2. 5G signaling network

Taking the 5G signaling network as an example, composed of the first level consists of high-level signaling transfer points HSCP, the second level consists of low-level signaling transfer points LSCP, and the third level consists of service NFs.

Since in-network signalling is carried out within a controlled security domain, its cryptographic applications are mainly concerned with remote operation and maintenance management channel at the device and computing layers, as shown in Table 4.

Table 4. Cryptography mechanism analysis of the signaling network

Layer	Object	Cryptographic mechanisms	Algorithms vulnerable to quantum threats in cryptographic mechanisms
Equipment and computing layer	Channel between EMS and the managed equipment	SNMPv2c/v3	— SHA-1 — AES-128
	Channel between 4A and EMS	SSL VPN	— DH, ECDH — ECDSA, RSA, DSA — SHA-2 — AES-128

4.3 Time Synchronization Network

Time synchronisation network is the key infrastructure for insuring the time synchronisation of network devices, which is mainly responsible for providing accurate time and frequency signals for each system in the communication network to ensure the synchronization of communication in the network. The composition of the time synchronisation network is shown in Figure 3. The time synchronisation network is divided into two levels, where first level nodes use Level 1 time synchronisation devices TSN1, second level nodes use Level 2 time synchronisation devices TSN2,

and clients use time service units. TSN1 must have the functions of time signal tracking and locking, and time allocation. TSN2 must have the functions of time signal tracking and locking, time distribution, frequency tracking and locking function, and timekeeping. Time service units shall be capable of obtaining time signals from the primary or secondary time synchronisation equipment through various time interfaces, and of providing time services for various business network network management systems and business network equipment.

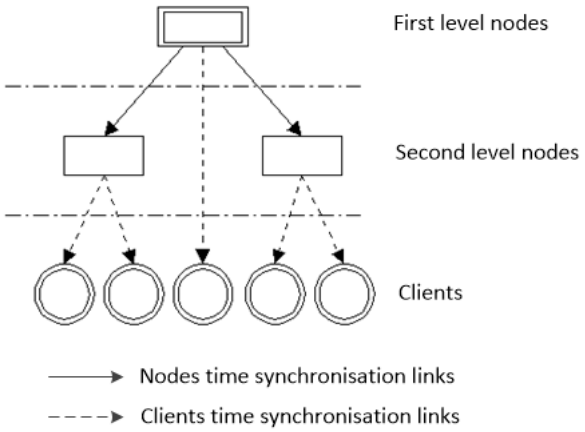

Figure 3. Hierarchical structure of synchronous network

Cryptographic applications for synchronisation networks mainly involve device and computing layer and network and communication layer. Table 5 presents an analysis of the cryptographic mechanisms involved in synchronous networks.

Table 5. Cryptography mechanism analysis

Layer	Object	Cryptographic mechanisms	Algorithms vulnerable to quantum threats in cryptographic mechanisms
Equipment and computing layer	Channel between EMS and the managed equipment	None (SSH is supported later)	— DH — RSA, DSA — SHA-2 — AES-128
	Channel between 4A and EMS	SSL VPN	— DH, ECDH — ECDSA, RSA, DSA — SHA-2 — AES-128
Network and communication layer	Communication channel between time-synchronization network node and clients	NTP protocol	— MD5 — SHA-1
	Communication channel	NTP protocol	— MD5

	between TSN1 and TSN2		— SHA-1
	Communication channel between the client time service unit and various service network management systems and service network devices	NTP protocol	— MD5 — SHA-1

4.4 Optical Transport Network

The Optical Transport Network (OTN) is an advanced telecommunication-grade transmission network built using fiber optic technology. A key strength of the OTN lies in its highly configurable architecture, enabling effective transmission, multiplexing, routing, management, monitoring, and survivability of signals. Additionally, its powerful error detection and correction mechanisms ensure high reliability in data transmission. The optical transport network network structure is shown in Figure 4, consisting of the client layer, electrical transport layer, optical transport layer, as well as the network management system and control plane. This hierarchical design simplifies network maintenance and management while enhancing system flexibility and scalability.

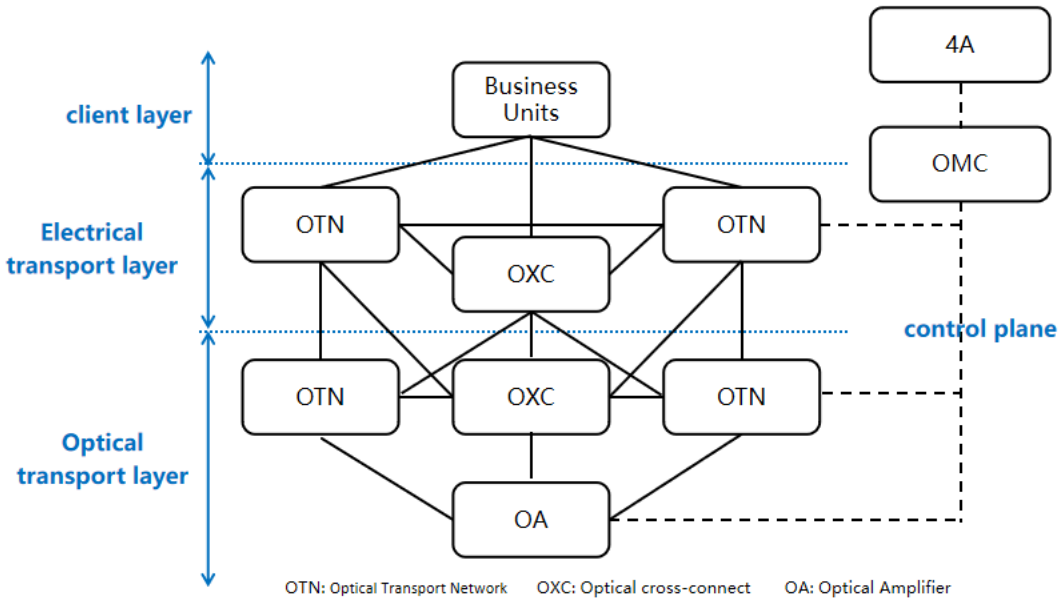

Figure 4. Hierarchical structure of Optical Transport Network

Optical transport network cryptographic application mainly focuses on equipment and computing level. The cryptographic application capability of OTN equipment at the electric and optical

transport layers will be strengthened in the future.

Table 6. Cryptography mechanism analysis

Layer	Object	Cryptographic mechanisms	Algorithms vulnerable to quantum threats in cryptographic mechanisms
Equipment and computing layer	Channel between EMS and the managed equipment	SSHv2/TLS1.2 /TLS1.3/SFTP/ SNMPv3	— DH — ECC, RSA, DSA — SHA-2, SHA-1 — AES-128
	Channel between 4A and EMS	SSL VPN	— DH, ECDH — ECDSA, RSA, DSA — SHA-2 — AES-128
	Communication channel between 4A and transmission workbench	SSL VPN	— DH, ECDH — ECDSA, RSA, DSA — SHA-2 — AES-128
	Communication channel between EMS and transmission workbench	VPN Security Gateways	— DH — RSA — SHA-2 — AES-128

4.5 Bearer Network

Bearer network serves as the cornerstone of modern information networks, primarily tasked with transporting data traffic from sources to destinations across a broad range. The design of carrier networks emphasizes high bandwidth, high availability, and low latency to ensure smooth operation of various business applications. They typically incorporate a variety of transmission media, such as fiber optics, microwaves, and satellites, along with critical equipment like routers, switches, and multiplexers. Bearer network generally is a two-level multilayer structured as shown in Figure 5. The two levels are backbone network level and provincial network level. Multilayer means that each level is divided into multiple levels according to different functions. The backbone network is divided into backbone core layer, backbone access layer and interconnection layer. The provincial network is divided into provincial network convergence layer, provincial network access layer or metropolitan area network (MAN) core layer and MAN service access control layer.

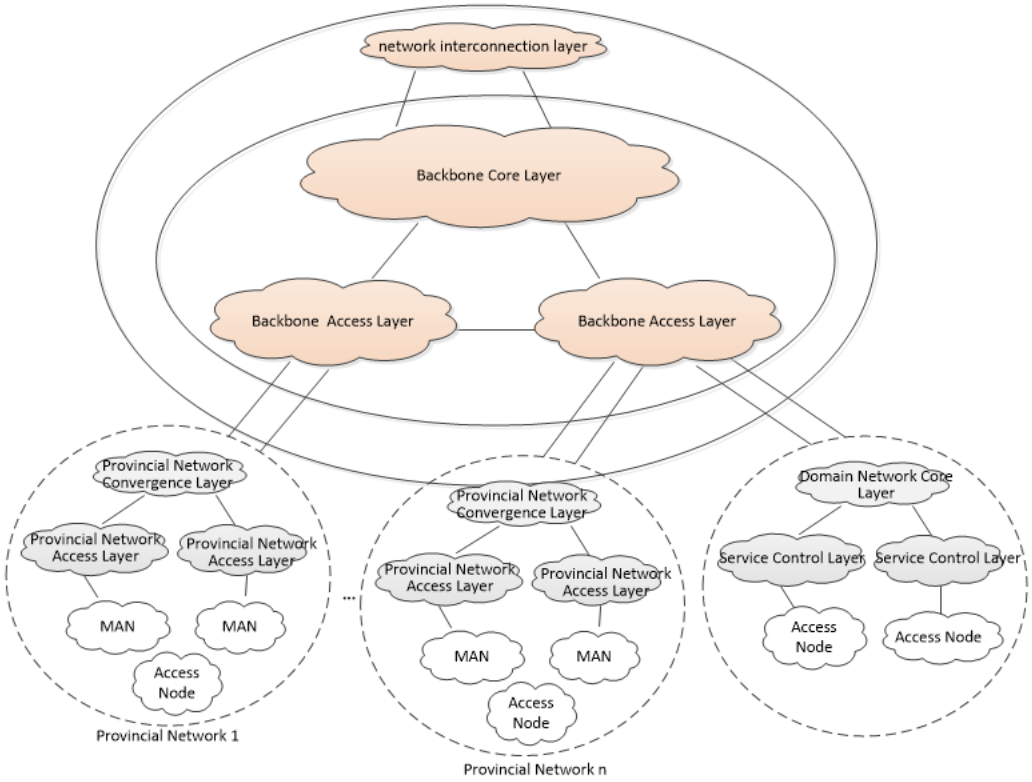

Figure 5. Schematic diagram of Bearer network architecture

Bearer network cryptographic applications mainly focus on the device and computing layer, network and communication layer. Table 7 presents an analysis of the possible cryptographic mechanism involved in the bearer network.

Table 7. Cryptography mechanism analysis

Layer	Object	Cryptographic mechanisms	Algorithms vulnerable to quantum threats in cryptographic mechanisms
Equipment and computing layer	Channel between 4A and network equipment	SSH protocol	— DH — RSA, DSA — SHA-2 — AES-128
	Channel between EMS and the managed equipment	SNMPv2c/v3	— SHA-1 — AES-128
	Channel between 4A and EMS	SSL VPN	— DH, ECDH — ECDSA, RSA, DSA — SHA-2 — AES-128
Network and communica	Authentication between routing device domains	MD5/SHA-1	— MD5 — SHA-1

tion layer	Confidentiality of inter-service router communication data	MPLS VPN combines security protocols (IPSec, SSL)	— DH, ECDH — ECDSA RSA, DSA — SHA-2 — AES-128

5 Key issues in post-quantum migration process and countermeasures

5.1 Key difficult issues faced during the migration process

Authentication, encryption, and integrity are the main security function requirements in telecommunication networks, which all need to have the ability to resist quantum attacks. Among them, authentication and encryption use public key cryptography technology, which is more severe with the security threat of quantum computing. Among them, authentication and encryption use public-key cryptography, which face more severe security threats from quantum computing, and need to migrate to post-quantum cryptography, expanding the service capability to support post-quantum cryptographic algorithms on the basis of the original digital signature and encryption scheme.

(1) Certification needs to address issues such as certificate extension and management

In Public Key Infrastructure (PKI), authentication is achieved based on digital certificates, the validity of which is verified by digital signature techniques. Digital signatures are also widely used to achieve non-repudiation during network communication. The current digital certificate format generally follows the X.509v3 international standard and the corresponding domestic standards. Most of the signature algorithms used in the certificate are RSA, ECDSA, SM2. X.509v3 certificates utilise an object identifier (OID) to identify the signature algorithm used.

To expand the support for post-quantum signature algorithms, fields such as OID, post-quantum signature public key, and post-quantum signature need to be added in the X.509v3 certificate extension domain to form a hybrid certificate supporting classical algorithms and post-quantum algorithms. The extension process involves: how to define the new certificate format and ensure that it is compatible with the existing certificate format; Upgrade the digital certificate issuing equipment to support the certificate format after the transformation of quantum cryptography

related algorithms; Upgrade the verification device to support the verification and storage of new certificates; After the quantum extension of the certificate, the old certificate needs to be replaced, which involves the management of the certificate, including the implementation of the correct certificate issuance, renewal and revocation process to ensure the credibility and legitimacy of the certificate.

(2) Authentication and encryption need to address issues such as bandwidth usage and computational performance.

Based on encryption and key negotiation technologies, the secure channel protects the information exchanged over the public network from being leaked. In general, the public key algorithms are not used to encrypt and decrypt a large amount of data, but often deal with the session key or some special data fields in the process of network communication. Common public key encryption algorithms include RSA and SM2. Key agreement is mainly implemented based on Diffie-Hellman protocol or RSA key exchange protocol.

Compared with traditional cryptography algorithms such as RSA and SM2, post-quantum cryptography algorithms usually have larger key or ciphertext size. For example, when the signature function is provided using RSA-2048, the public key, private key and signature sizes are all 256 bytes, while the public key, private key and signature sizes of CRYSTALS-Dilithium, a lattice-based signature algorithm in the NIST post-quantum cryptography standard, are 1312 bytes, 2528 bytes and 2420 bytes respectively. Security services using such algorithms may need to expand the length of protocol fields according to the algorithm requirements. Meanwhile, the increase in the scale of keys and ciphertext also requires higher storage space and transmission bandwidth, resulting in further propagation latency, transmission latency, and processing latency.

Post-quantum public key cryptography algorithms of different technical routes have huge differences in performance. Applicable algorithms need to be selected based on the characteristics of the scenario. For example, lattice-based cryptographic algorithms strike a good balance among security, public/private key sizes, and computational speed, making them suitable for high-security domains. Code-based cryptography algorithms have large public key size, slow key generation, but fast encryption/decryption speed, which is ideal for speed-sensitive scenarios. Algorithms with slow key generation and slow computation speed increase the execution time of

security services, including the time of connection establishment, which may affect the efficiency of business services, especially for some latency-sensitive edge computing-type services, where service availability may be affected.

5.2 Countermeasures to face challenges

The performance requirements of the telecommunication networks are extremely high, and the effectiveness of post-quantum cryptography needs to be included in the assessment. The communication field covers the whole country and carries many types of communication services, with many types of systems, large numbers of devices, complex business functions, and harsh requirements for performance and stability. The key length of post-quantum cipher algorithm becomes longer, and the computation time and arithmetic power consumption are generally tens of times higher than those of traditional cipher algorithms, which will have a greater impact on the network function, performance, bandwidth, etc., and will have a greater impact on the efficiency and availability of the existing network business services while improving the security, which will bring greater difficulties for the migration of post-quantum cipher in the communication network.

The post-quantum cryptographic industry chain is difficult to support the implementation of post-quantum cryptographic migration, and it is necessary to promote the construction of the industry chain. The lack of uniform standards in the industrial chain may affect product development and interoperability, thus restricting the progress of migration implementation. Post-quantum cryptographic algorithms differ significantly from traditional cryptographic algorithms, requiring adjustments to existing protocols to ensure compatibility and interoperability between old and new systems. This requires joint efforts and synergy between the upstream and downstream of the industry chain, but at present there may be a lack of effective coordination mechanisms and unified technical specifications. Algorithm replacement will also face problems such as large differences in calling methods and difficulties in hardware interface interoperability, and post-quantum cryptographic migration will require extensive compatibility testing with network facilities.

6 Recommendations for further work

Research in advance on the response to the evolution and migration of post-quantum cryptography, design a network architecture with agile introduction of post-quantum cryptography in next-generation networks such as 6G, and lead the formation of a standardised scheme compatible with the existing cryptographic system and post-quantum cryptographic system.

Encourage the industrial chain to increase investment, and gradually form a perfect cryptographic support capability system including standardisation capability, evaluation and verification capability, productisation capability and supply chain capability, etc., so as to form a synergy to support the implementation of post-quantum cryptography migration and give full play to the role of cryptography as a security cornerstone.