Whitepaper

CORAN LABS

CORANLABS Quantum-Safe Telecom Solutions

Advanced Quantum-Safe Solution for Robust Security against Quantum Attacks

Content

1. Introduction

In the rapidly evolving field of telecommunications, staying ahead of potential security threats is essential for maintaining the integrity and reliability of network infrastructure. With the advancement of quantum computing technology, classical security algorithms defined by the 3rd Generation Partnership Project (3GPP), which form the foundation of current security methods, face significant challenges. Quantum computers have the potential to solve problems that are practically unsolvable by classical computers, rendering these traditional algorithms obsolete and highly vulnerable to attacks.

This whitepaper aims to provide a comprehensive overview of the necessary changes required to migrate the telecom network to a post-quantum secure framework. The focus will be on transforming key components of the network, including the Core, Radio Access Network (RAN), and User Equipment (UE), to ensure they are resilient against the emerging threats posed by quantum computing.

The whitepaper delves into the intricacies of upgrading to a Quantum-secure Core, discussing the implementation of quantum-resistant algorithms and protocols capable of withstanding quantum attacks. It also covers the necessary modifications in the Open Radio Access Network (O-RAN) interfaces to support secure and efficient communication. Additionally, it explores the enhancements required in User Equipment (UE) to ensure end-to-end security for users.

By understanding and adopting the post-quantum cryptographic solutions presented by CORAN LABS, telecom networks can safeguard sensitive data and ensure secure communications in the face of quantum advancements. This introduction sets the stage for a detailed exploration of the technologies and strategies necessary for migrating to a post-quantum telecom network, thereby ensuring robustness and future-proofing against the evolving quantum threat landscape.

2. Background

Security in 5G networks is crucial due to their expanded capabilities and increased attack surface. Unlike previous generations, 5G networks offer enhanced encryption, stronger privacy measures, and advanced authentication protocols. These improvements address existing vulnerabilities while introducing new security features, making it essential to protect sensitive data and maintain user privacy. Ensuring a secure 5G deployment is vital for the safe operation of users, safeguarding their identities, and securing the data packets transmitted over the 5G network.

The classical 5G Network is vulnerable to quantum threats, as quantum computers can break traditional cryptographic algorithms like RSA and ECC by solving complex problems exponentially faster. This renders current encryption methods insecure. To safeguard against these threats, 5G networks must adopt quantum-proof measures. Post-Quantum Cryptography (PQC) offers encryption methods resistant to future quantum threats, ensuring long-term security and privacy for 5G infrastructure. PQC addresses current vulnerabilities, paving the way for a more secure 5G network.

2.1. 5G Network

In the traditional/classical 5G network, security is a crucial aspect achieved through both symmetric and asymmetric key cryptography.

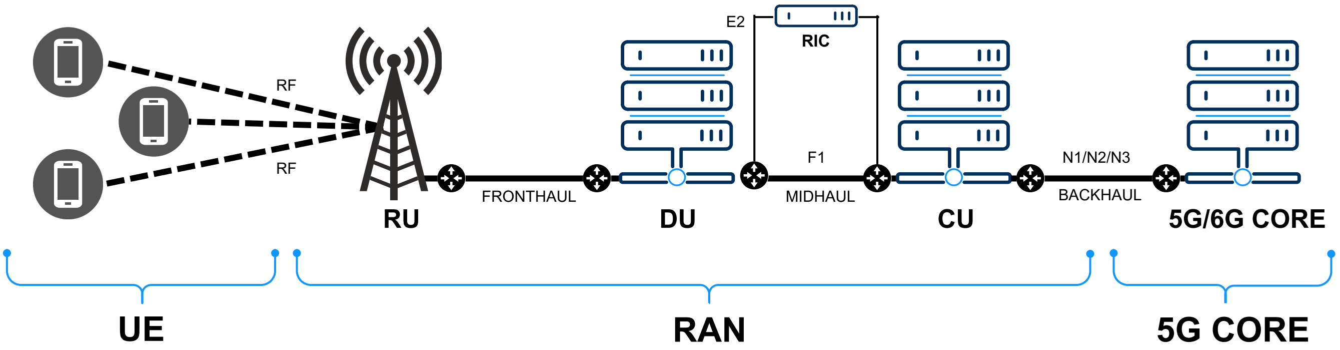


Figure: E2E Connection of a 5G Network

The main areas where these security measures are applied in 5G include:

2.1.1. Long-Term Key (K) Protection

Long-term keys are keys used for security purposes that typically remain unchanged in the device where they are stored. These keys are essential for repeated security transactions. In 3GPP standards, detailed in TR 33.834, long-term keys serve as the foundation for authentication, authorization, and secure management.

Specifically, these keys are used for authenticating the connection between the 3GPP network and the UE, as well as for authorizing services. The long-term keys are securely stored in the Universal Subscriber Identity Module (USIM).

2.1.1.2. SUPI to SUCI Conversion

In 5G networks, the 3GPP enhances subscriber privacy by introducing encryption for the International Mobile Subscriber Identity (IMSI). The 5G system replaces IMSI with the Subscription Permanent Identifier (SUPI), a globally unique identifier. To ensure enhanced privacy, the Subscription Concealed Identifier (SUCI) is used, which is an encrypted version of the SUPI. This encryption prevents International Mobile Subscriber Identity (IMSI) Catching Attacks, effectively protecting subscribers from being identified and tracked.

2.1.1.2.1. SUPI

The 3GPP specifications define various types of SUPIs. Here, we focus on the IMSI-based SUPI, equivalent to the traditional IMSI. According to TS 23.003, this identifier is a number with up to 15 digits: the first 3 digits are the Mobile Country Code (MCC), the next 2-3 digits are the Mobile Network Code (MNC) identifying the network operator, and the remaining digits represent the Mobile Subscriber Identification Number (MSIN).

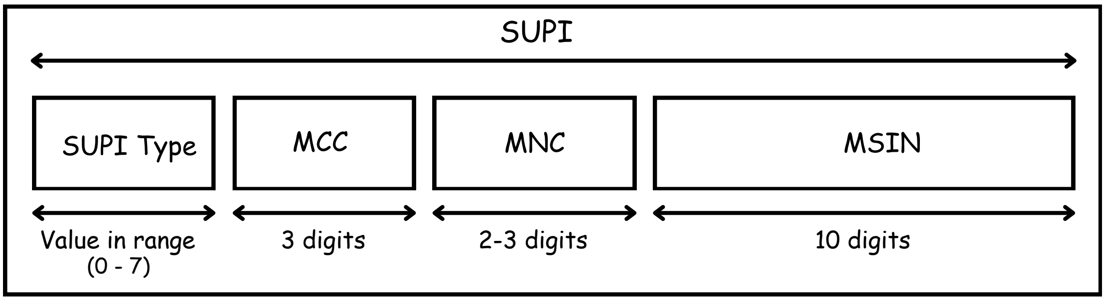


Figure: SUPI

2.1.1.2.2. SUCI

As part of the authentication process, a subscriber sends their SUCI to the network. The SUCI, derived from the SUPI, consists of six parts: the type of SUPI, the Home Network Identifier (MCC and MNC for IMSI-based SUPIs), and the Routing Indicator for internal network routing. It also includes the Protection Scheme ID, indicating the encryption scheme used, the Home Network Public Key ID, identifying the operator's public key, and the encrypted output of the chosen Protection Scheme. These details are specified in 3GPP TS 23.003.

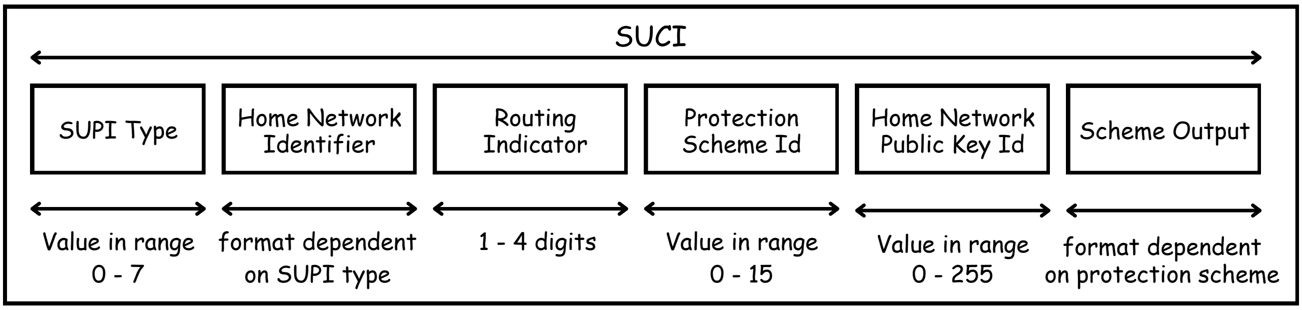
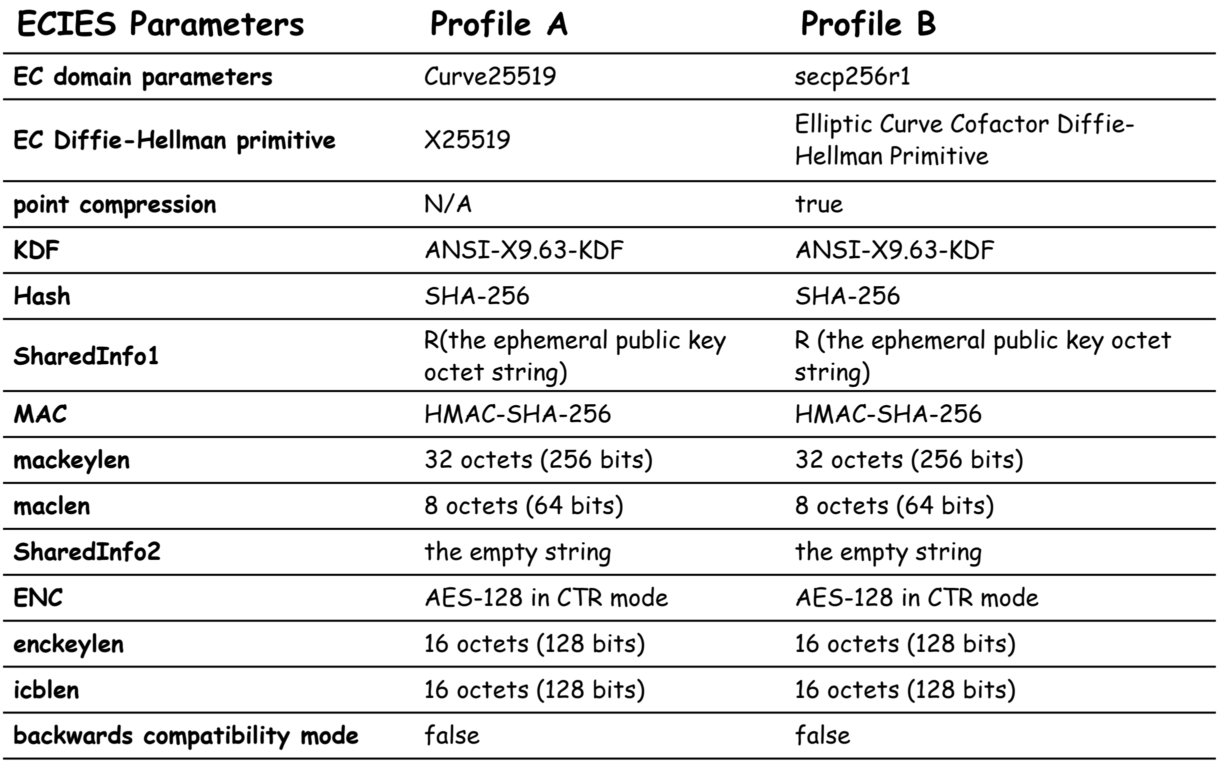


Figure: SUCI

In the SUCI, the MNC and MCC are directly included, leaving only the MSIN for encryption. While subscribers can still authenticate by sending their MSIN in plaintext using the null-scheme, 5G introduces encrypted transmission for enhanced security. This encryption uses one of two predefined Elliptic Curve Integrated Encryption Scheme (ECIES) profiles, Profile A and Profile B, which differ mainly in their elliptic curve parameters.

2.1.1.2.3. ECIES

The ECIES is a public key encryption method that combines Elliptic Curve Cryptography (ECC) with symmetric encryption. It is a standard method used for the concealment of the SUPI and is followed by every 3GPP-compliant 5G Core.



ECIES Parameters	Profile A	Profile B
EC domain parameters	Curve25519	secp256r1
EC Diffie-Hellman primitive	X25519	Elliptic Curve Cofactor Diffie-Hellman Primitive
point compression	N/A	true
KDF	ANSI-X9.63-KDF	ANSI-X9.63-KDF
Hash	SHA-256	SHA-256
SharedInfo1	R(the ephemeral public key octet string)	R (the ephemeral public key octet string)
MAC	HMAC-SHA-256	HMAC-SHA-256
mackeylen	32 octets (256 bits)	32 octets (256 bits)
maclen	8 octets (64 bits)	8 octets (64 bits)
SharedInfo2	the empty string	the empty string
ENC	AES-128 in CTR mode	AES-128 in CTR mode
enckeylen	16 octets (128 bits)	16 octets (128 bits)
icblen	16 octets (128 bits)	16 octets (128 bits)
backwards compatibility mode	false	false

Table: ECIES profiles

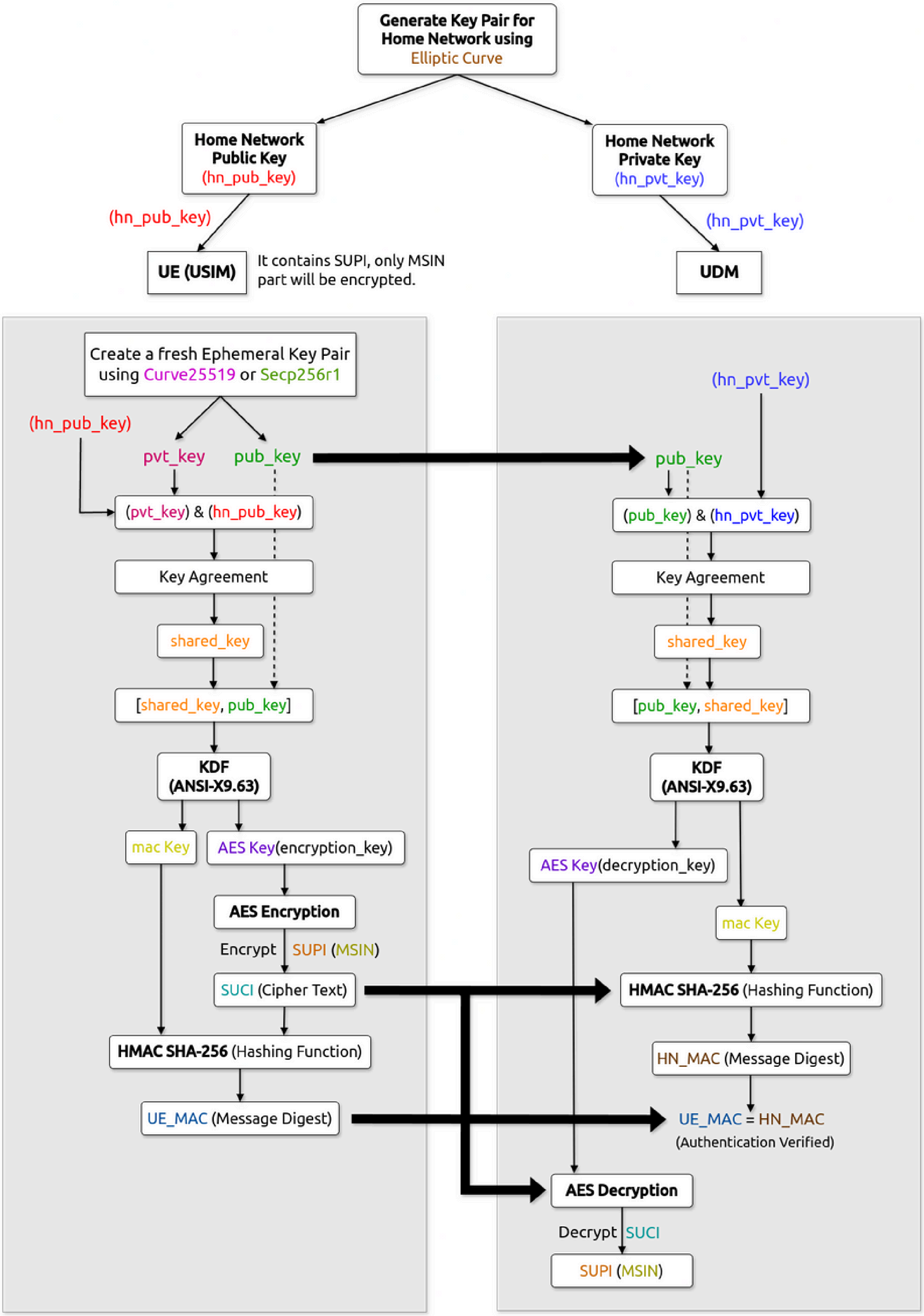


Figure: ECIES Implementation in 5G

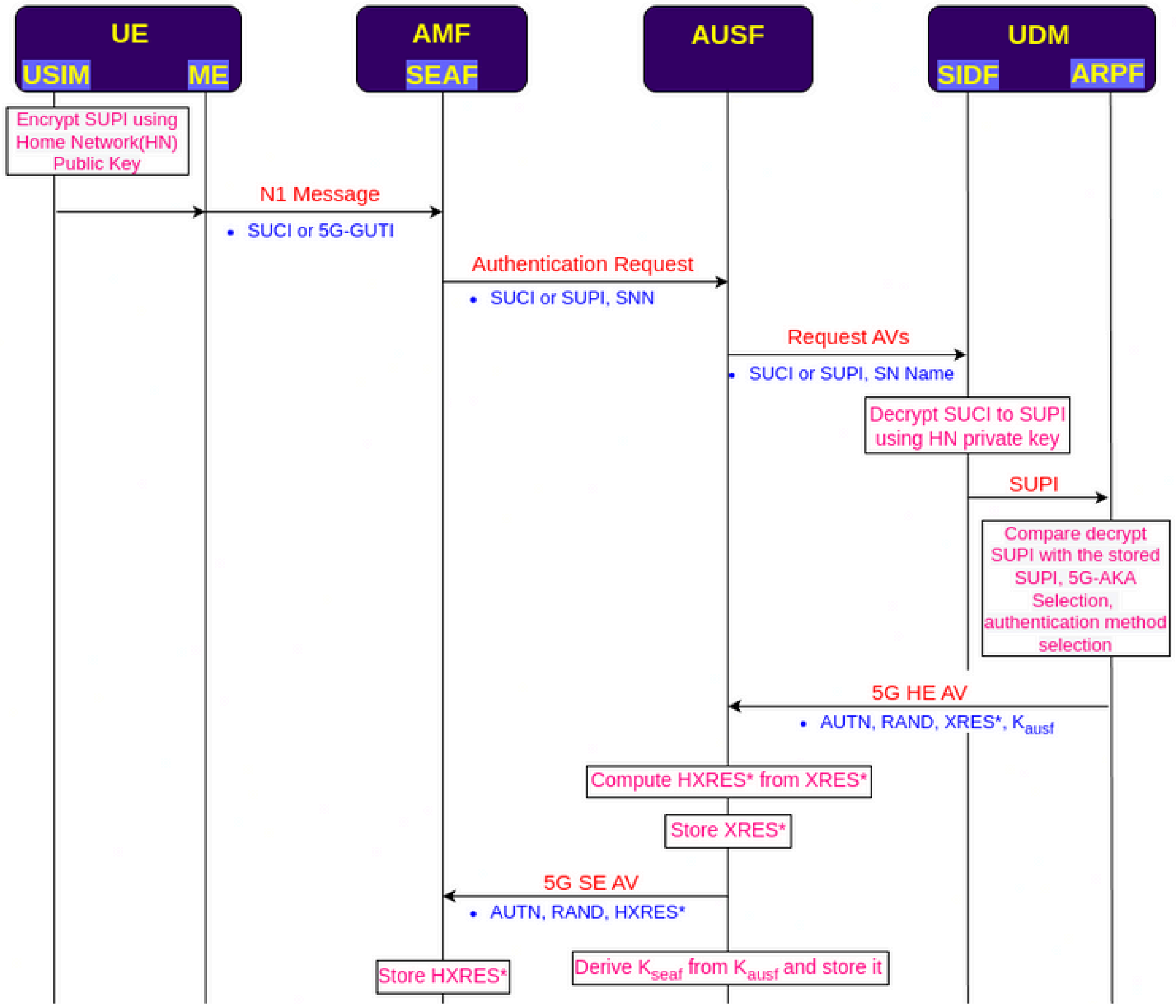
The process begins by generating a Home Network Key pair using Elliptic Curve cryptography. The home network public key is stored in the USIM, and the home network private key is kept in the UDM's Subscription Identifier De-concealing Function (SIDF). The UE then generates an ephemeral key pair for a single transaction. A Shared Key is created using the home network public key and the ephemeral private key.

This Shared Key is used to derive an AES encryption key and a MAC key through the ANSI-X9.63 Key Derivation Function (KDF). The AES key encrypts the MSIN (SUPI), producing the SUCI ciphertext, while the MAC key generates the UE_MAC for message authentication.

The ephemeral public key, SUCI ciphertext, and UE_MAC are sent to the home network (UDM). The UDM uses the ephemeral public key and the home network private key to recreate the Shared Key and regenerate the AES decryption key and MAC key. Message authentication is verified by comparing the UE_MAC and HN_MAC. If they match, the SUCI is decrypted back to the MSIN (SUPI) using the AES key. Once this decryption is successful, UE authentication is confirmed, thereby completing the ECIES process.

2.1.1.3. Authentication Mechanisms

The primary authentication protocols in 5G, namely 5G-AKA (Authentication and Key Agreement) and EAP-AKA′(Extensible Authentication Protocol AKA), enable mutual authentication between UE, such as a mobile phone, and a Home Network (HN), such as a service provider's network. These protocols, detailed in 3GPP TS 33.501, facilitate the exchange of key materials, like anchor keys, to secure all subsequent 5G communications.


UE
USIM
ME
AMF
SEAF
AUSF
UDM
SIDF
ARPF
Encrypt SUPI using Home Network(HN) Public Key
N1 Message
• SUCI or 5G-GUTI
Authentication Request
• SUCI or SUPI, SNN
Request AVs
• SUCI or SUPI, SN Name
Decrypt SUCI to SUPI using HN private key
SUPI
Compare decrypt SUPI with the stored SUPI, 5G-AKA Selection, authentication method selection
5G HE AV
• AUTN, RAND, XRES*, K_{ausf}
Compute HXRES* from XRES*
Store XRES*
5G SE AV
• AUTN, RAND, HXRES*
Store HXRES*
Derive K_{seaf} from K_{ausf} and store it

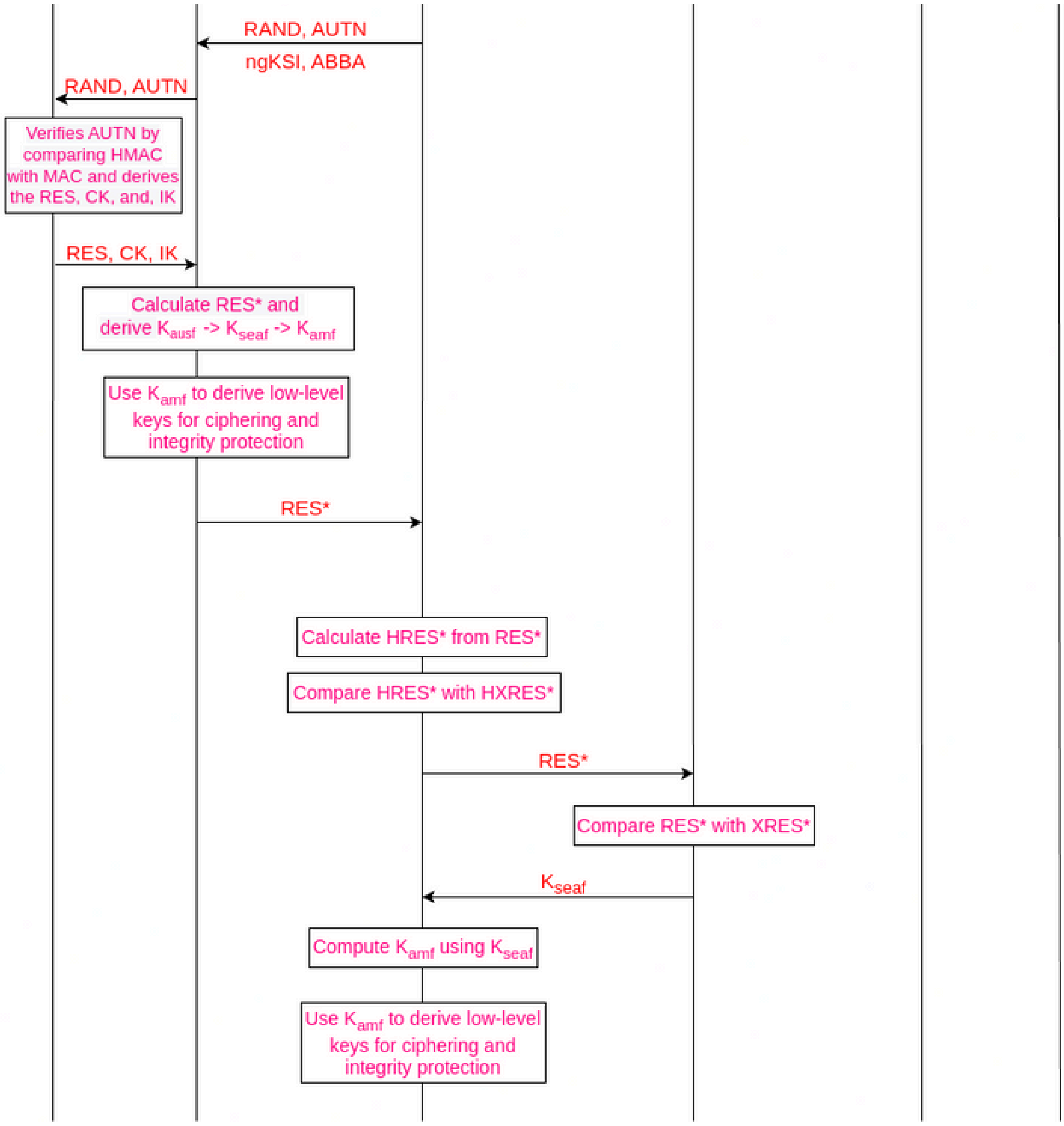

RAND, AUTN
ngKSI, ABBA
RAND, AUTN
Verifies AUTN by comparing HMAC with MAC and derives the RES, CK, and, IK
RES, CK, IK
Calculate RES* and derive K_{ausf} -> K_{seaf} -> K_{amf}
Use K_{amf} to derive low-level keys for ciphering and integrity protection
RES*
Calculate HRES* from RES*
Compare HRES* with HXRES*
RES*
Compare RES* with XRES*
K_{seaf}
Compute K_{amf} using K_{seaf}
Use K_{amf} to derive low-level keys for ciphering and integrity protection

Figure: AKA Procedures

EAP-AKA is an EAP method based on the AKA algorithm used in 3GPP networks for user authentication and key generation. It leverages the SIM card as a secure element to store secret keys and perform cryptographic operations. The process involves 4 main steps: identity request and response, challenge request and response, success or failure indication, and master session key derivation. EAP-AKA also supports fast re-authentication, reducing message exchanges and enhancing performance.

2.1.1.4. Security Mechanism

The security mechanisms for protecting NAS and RRC signaling and data incorporate both integrity and confidentiality measures. These mechanisms employ 128-bit integrity and ciphering algorithms, as specified in TS 33.501, to ensure the integrity and confidentiality of communications.

2.1.1.5. Milenage Algorithm

MILENAGE, based on the AES (originally called Rijndael) algorithm, is a set of authentication and key generation functions proposed by 3GPP. These functions are detailed in TS 35.205 through TS 35.208, and TS 35.909.

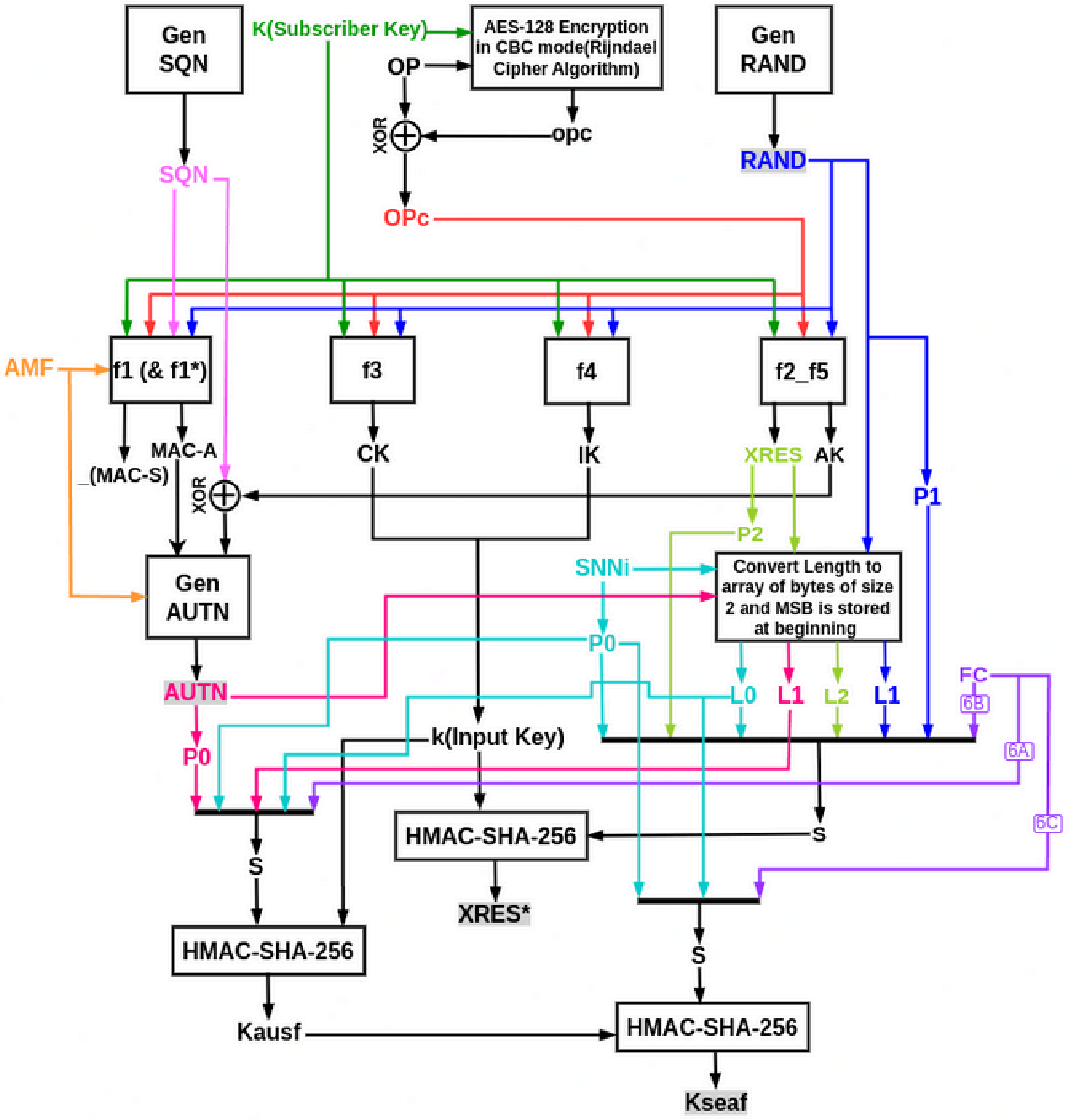


Figure: HN Milenage

2.1.1.6. Mutual Authentication

2.1.1.6.1. Between NRF and NF

The Network Resource Function (NRF) and Network Functions (NF) authenticate each other during discovery, registration, and access token requests. According to 3GPP TS 33.501 and TS 29.510, if the Public Land Mobile Network (PLMN) uses transport layer protection, the NF Service Consumer uses TLS for mutual authentication with the NRF. If transport layer protection is not used, mutual authentication relies on NDS/IP or physical security.

The NRF handles messages from unauthenticated NFs by supporting error handling and potentially sending error messages, and vice versa. After successful authentication, the NRF determines if the NF is authorized for discovery and registration. If not, the NRF handles errors and may send an error message.

2.1.1.6.2. Protection of the NEF - AF interface

For authentication between the Network Exposure Function (NEF) and an Application Function (AF) residing outside the 3GPP operator domain, mutual authentication using client and server certificates is required. This authentication is performed using TLS.

TLS provides integrity protection, replay protection, and confidentiality for the interface between the NEF and the AF. The use of TLS is mandatory. Security profiles for TLS implementation and usage must follow the provisions given in TS 33.310 and TS 33.501.

2.1.1.6.3. O-RAN Interfaces

mTLS and OAuth 2.0 are used for mutual authentication across the O-RAN interfaces, including O1, A1, R2, and the O-FH (M-plane), as outlined in the O-RAN Security Requirements Specifications [16] and O-RAN Security Protocols Specifications [17].

2.1.1.7. Roaming Security

In roaming, SEPPs use PRINS over N32, establishing TLS (N32-c) connections to secure HTTP messages, as specified in TS 33.517. They negotiate N32-f security parameters, exchange encryption, and modification policies, and share IPX security information. SEPPs export keying material from the TLS session to derive session keys and IVs. A second TLS connection is established for mutual authentication, enabling secure NF service-related signaling over N32-f.

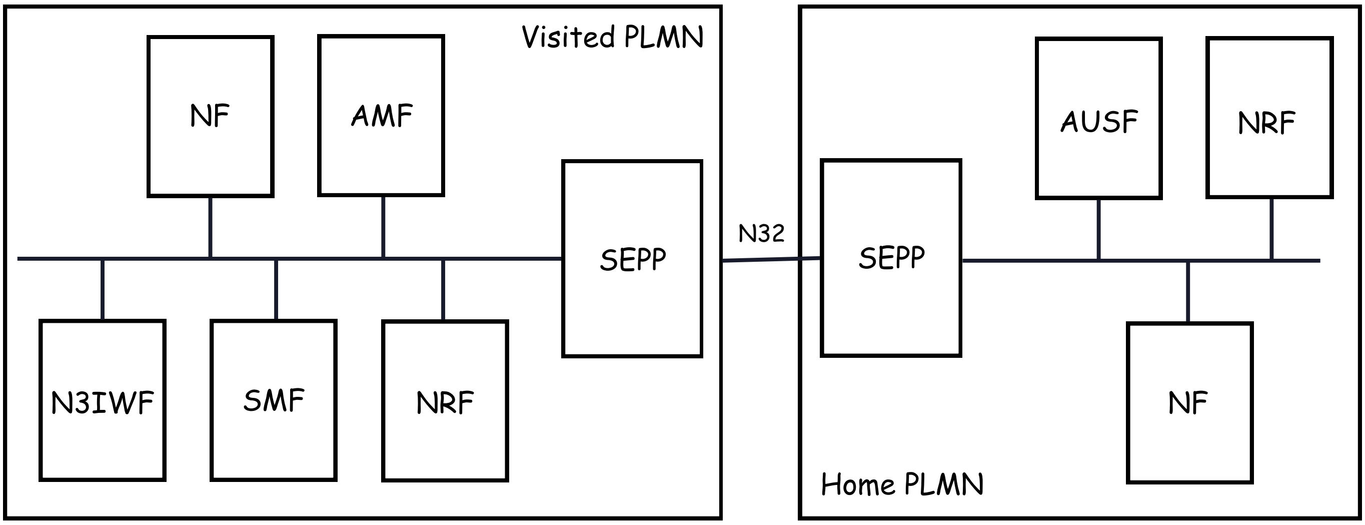


Figure: 5G Roaming with SEPP

2.1.1.8. IPsec and DTLS

2.1.1.8.1. IPsec ESP and IKEv2 in NDS/IP

IPsec provides security services through Security Associations (SAs) that define the protocol, mode, and endpoints. In NDS/IP networks, the Internet Key Exchange protocol (IKEv2) is used for negotiating and managing these SAs, ensuring secure communication.

The Encapsulating Security Payload (ESP) in IPsec offers confidentiality, integrity, and authentication of data. IKEv2, as defined in RFC 7296, negotiates and establishes IPsec SAs, creating a secure bi-directional communication channel between nodes. The 3GPP IKEv2 profile in 3GPP TS 33.210 of the relevant specifications outlines mandatory and optional features for 3GPP interfaces, ensuring a streamlined and secure implementation for NDS/IP.

2.1.1.8.2. DTLS

In 5G networks, DTLS, as specified in RFC 6083, provides mutual authentication, integrity protection, replay protection, and confidentiality. Its implementation follows the TLS profile in TS 33.210 and the certificate profile in TS 33.310.

Identities in end-entity certificates are used for authentication and policy checks. DTLS supports mutual authentication over the N2/F1AP/Xn/E1AP interfaces and can be used alongside IKEv2, as detailed in TS 33.501. While DTLS secures the transport layer, IPsec can also be used for network layer protection, offering topology-hiding advantages.

2.1.1.9. Token Based Authentication

The NRF offers the Nnrf_AccessToken service for OAuth2 authorization, following the "Client Credentials" grant as specified in 3GPP TS 33.501. NF Service Consumers can request an OAuth2 access token from the NRF's "Token Endpoint." This service allows NF Service Consumers to obtain access tokens for secure authorization from the NRF.

2.1.1.10. Security Mechanism

The NRF offers the Nnrf_AccessToken service for OAuth2 authorization, following the "Client Credentials" grant as specified in 3GPP TS 33.501. NF Service Consumers can request an OAuth2 access token from the NRF's "Token Endpoint." This service allows NF Service Consumers to obtain access tokens for secure authorization from the NRF.

These implementations demonstrate the extensive use of classical cryptographic techniques to secure various aspects of the 5G Core, ensuring robust protection against potential threats and vulnerabilities.

2.2. Post Quantum Cryptography

Post-Quantum Cryptography (PQC) encompasses cryptographic algorithms specifically designed to withstand the potential threats posed by quantum computers. Algorithms such as ML-KEM, ML-DSA, Key Encapsulation Mechanisms (KEM), Learning with Errors, and lattice-based cryptography offer quantum-resistant security.

As quantum computing continues to evolve, it presents a significant challenge to existing cryptographic methods. Quantum computers have the capability to break widely used security algorithms that currently protect our data. Here’s why transitioning to post-quantum security is imperative:

- **Quantum Computing Power**: Quantum computers can perform complex calculations at unprecedented speeds, making traditional encryption methods vulnerable. Algorithms like RSA and ECC, which rely on the difficulty of factoring large numbers or computing discrete logarithms, can be easily broken by quantum computers using Shor’s algorithm.
- **Lack of True Randomness**: Keys generated for existing cryptographic methods are often not truly random, rendering them predictable and susceptible to quantum attacks. Quantum algorithms can exploit patterns in key generation, thereby compromising security.
- **Symmetric Key Size**: In symmetric cryptographic methods, key sizes must be significantly larger to remain secure against quantum attacks. For instance, while a 128-bit key is secure against classical attacks, a quantum computer may require a minimum of a 256-bit key to provide equivalent security.

To address the threat of quantum attacks, it is essential to adopt Post-Quantum Cryptographic algorithms and Quantum Random Number Generators (QRNGs). Below are some of the key algorithms and technologies that will be employed:

2.2.1. ML-KEM

NIST has specified a key encapsulation mechanism known as the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), which is based on the computational difficulty of the Module Learning with Errors (MLWE) problem. Currently, ML-KEM is considered secure even against adversaries equipped with quantum computers. The standard defines three parameter sets for ML-KEM, each offering different levels of security and performance: ML-KEM-512, ML-KEM-768, and ML-KEM-1024. These sets increase in security strength but decrease in performance as the parameters scale up.

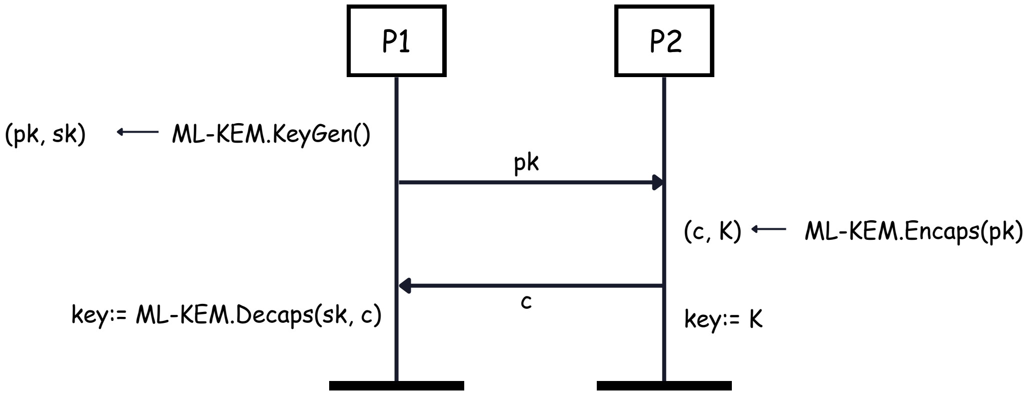

P1
P2
(pk, sk) ⟵ ML-KEM.KeyGen()
pk
(c, K) ⟵ ML-KEM.Encaps(pk)
c
key:= ML-KEM.Decaps(sk, c)
key:= K

Figure: ML-KEM

2.2.2. ML-DSA

NIST has specified Module-Lattice-Based Digital Signature Algorithm (ML-DSA), a suite of algorithms designed for generating and verifying digital signatures. ML-DSA is considered secure even against adversaries with access to large-scale quantum computers. This algorithm provides robust digital signatures, ensuring the integrity and authenticity of messages in a post-quantum world.

2.2.3. PQ-TLS

Post-Quantum Transport Layer Security (PQ-TLS) secures communication channels by utilizing homogeneous and hybrid post-quantum cryptographic algorithms, ensuring that data transmitted over networks remains confidential and tamper-resistant, even in the presence of quantum adversaries. By integrating these post-quantum algorithms, PQ-TLS significantly enhances the security of internet communications, protecting against future quantum threats

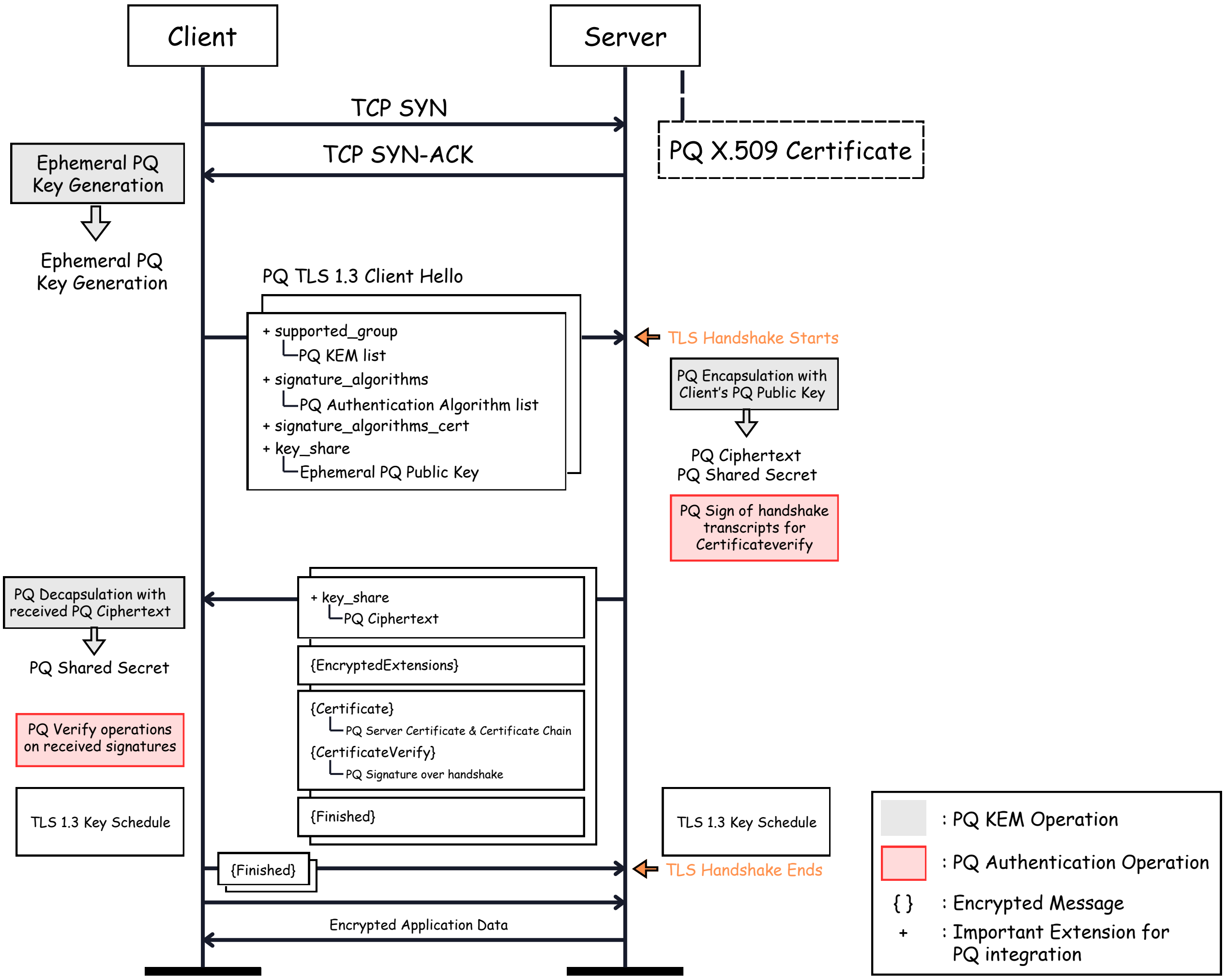

Client
Server
TCP SYN
TCP SYN-ACK
PQ X.509 Certificate
Ephemeral PQ Key Generation
Ephemeral PQ Key Generation
PQ TLS 1.3 Client Hello
+ supported_group
└PQ KEM list
+ signature_algorithms
└PQ Authentication Algorithm list
+ signature_algorithms_cert
+ key_share
└Ephemeral PQ Public Key
TLS Handshake Starts
PQ Encapsulation with Client's PQ Public Key
PQ Ciphertext
PQ Shared Secret
PQ Sign of handshake transcripts for Certificateverify
PQ Decapsulation with received PQ Ciphertext
PQ Shared Secret
PQ Verify operations on received signatures
+ key_share
└PQ Ciphertext
{EncryptedExtensions}
{Certificate}
└PQ Server Certificate & Certificate Chain
{CertificateVerify}
└PQ Signature over handshake
{Finished}
TLS 1.3 Key Schedule
TLS 1.3 Key Schedule
{Finished}
TLS Handshake Ends
Encrypted Application Data
: PQ KEM Operation
: PQ Authentication Operation
{ } : Encrypted Message
+ : Important Extension for PQ integration

Figure: Post Quantum TLS 1.3 Handshake

2.2.4. QRNG

Quantum Random Number Generators (QRNGs) generate seeds that are used to create Post-Quantum Cryptographic key pairs, whether for long-term or ephemeral use. QRNGs ensure true randomness in key generation, making it impossible for quantum computers to predict or break these cryptographic keys, thereby fortifying security.

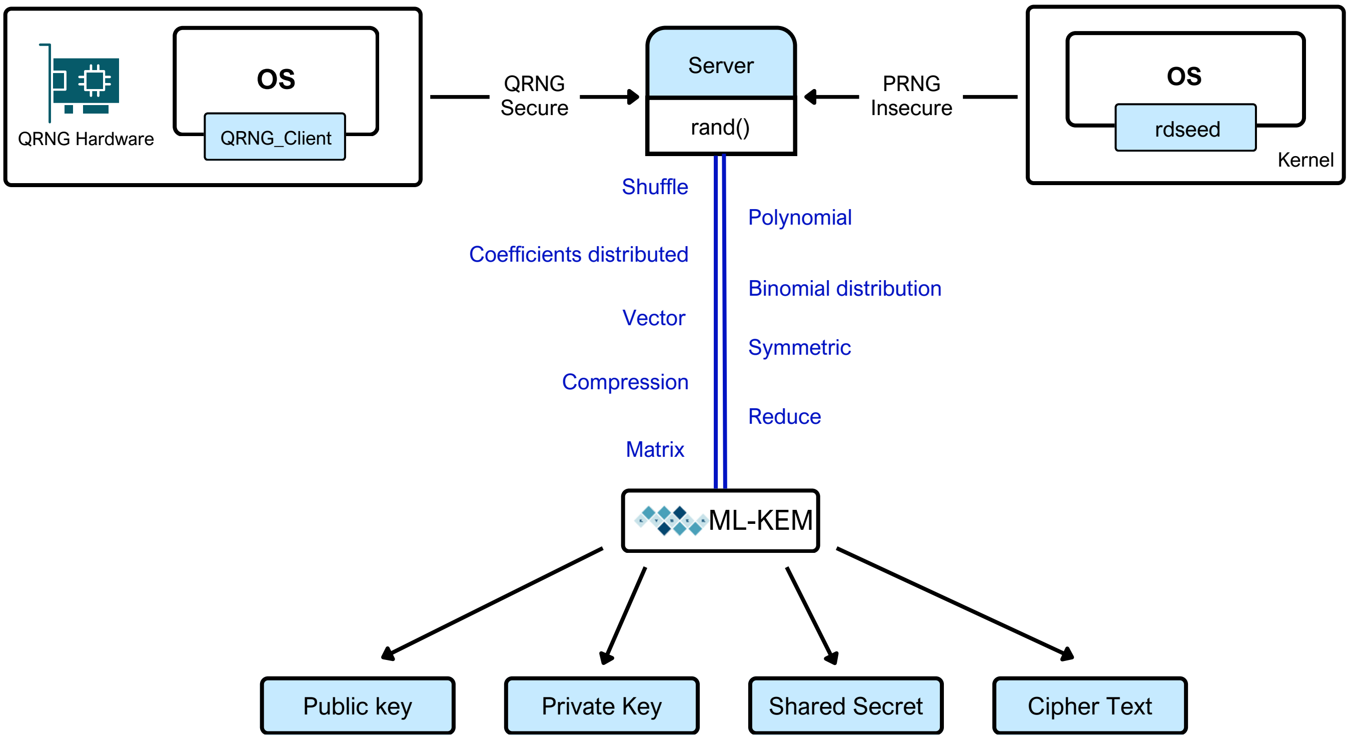


Figure: QRNG

2.2.5. AES-256

The Advanced Encryption Standard (AES) with 256-bit keys provides robust encryption. While a 128-bit key is secure against classical attacks, quantum computers necessitate the use of a 256-bit key to achieve equivalent security. AES-256 offers strong defense against quantum attacks by leveraging larger key sizes, ensuring enhanced protection.

2.2.6. PQ-IPSec

Post-Quantum Internet Protocol Security (PQ-IPSec) secures Internet Protocol communications by employing post-quantum cryptographic methods. This ensures that data packets transmitted over IP networks are both encrypted and authenticated, protecting against interception and tampering by quantum adversaries. PQ-IPSec is crucial for maintaining the confidentiality and integrity of data in a quantum-safe internet.

2.2.7. PQ-DTLS

Post-Quantum Datagram Transport Layer Security (PQ-DTLS) secures datagram communications using post-quantum cryptographic algorithms, providing a secure layer for datagram-based applications. It ensures that data transmitted over UDP is safeguarded against quantum attacks. By incorporating post-quantum security, PQ-DTLS enhances the resilience of real-time communications, such as VoIP and online gaming, against future quantum threats.

3. Migration to Quantum-Secure 5G Networks

3.1. Classical 5G Core to Post-Quantum Core

To successfully transition from a classical 5G Core to a post-quantum Core, several critical areas and protocols must be updated. The table below outlines the necessary changes across different components of the 5G core network to ensure quantum-resistant security.

Functionality	Classical Encryption	Post Quantum Encryption
Random Number	PRNG (Pseudo Random Number Generator)	QRNG (Quantum Random Number Generator)
SUPI to SUCI	ECIES(Elliptic Curve Integrated Encryption Scheme)	ML-KEM
		Hybrid Post Quantum Mechanism
SBI Communication	mTLS	PQ-TLS
Digital Certificates	Classical Cryptographic Algorithm	ML-DSA
Symmetric Key	AES-128	AES-256
N3 User Data	IPSec	PQ-IPSec
N3 User Data	DTLS	PQ-DTLS

Table: Migration from Classical Core to Post Quantum Core

3.1.1. Random Seed Generation using QRNG

QRNGs leverage quantum processes to produce truly random numbers, ensuring high unpredictability and entropy. This level of randomness is crucial for cryptographic key generation, as it significantly enhances security by making it nearly impossible for attackers to predict or reproduce keys. In a post-quantum world, QRNGs become essential for maintaining robust security in telecom networks.

In the 5G Core, several critical operations require the use of quantum-secure cryptographic keys. These keys must be generated with true randomness to ensure the highest level of security. Here are the key areas in the Core where QRNGs will be utilized:

- **Keys for AKA Procedure**: The AKA Procedure is essential for verifying user identities and establishing secure communication. QRNGs can be used to generate keys, ensuring the highest level of security during this process.
- **Long-Term Keys**: These keys are critical for maintaining secure communications over extended periods. QRNGs can provide the necessary randomness to generate these keys, protecting them from quantum attacks.
- **Home Network Public and Private Keys**: The home network relies on secure public and private key pairs for various cryptographic operations. QRNGs can ensure these keys are truly random, significantly enhancing the security of network communications.
- **Ephemeral Key Pairs**: Ephemeral keys are used for short-term sessions and are vital for ensuring forward secrecy. QRNGs can generate these keys with high entropy, making them resistant to prediction or reuse by attackers.

- **Certificate Generation Between Different NF**: Certificates are crucial for authenticating and establishing trust between different NFs. QRNGs can be instrumental in generating secure certificates, ensuring the integrity and authenticity of communications across the network.
- **Secure SBI Communication Between NFs**: The Service-Based Interface (SBI) enables communication between various network functions. QRNGs can generate keys for secure SBI communication, ensuring data integrity and confidentiality throughout the network.

3.1.2. SUPI to SUCI Conversion using PQC

In 4G networks, the International Mobile Subscriber Identity (IMSI) was transmitted in plain text from the UE to the core network, making it susceptible to man-in-the-middle attacks. To address this vulnerability, 5G networks introduced the SUPI. The SUPI is encrypted and converted into the SUCI before being transmitted to the core network, enhancing security. This encryption process is currently performed using the ECIES.

However, since ECIES relies on elliptic curves that are vulnerable to quantum attacks, integrating PQC is essential. This integration can be achieved through two approaches: homogeneous and hybrid methods.

3.1.2.1. Homogeneous Method

This method employs a single type of post-quantum cryptography method throughout the communication process, for the conversion of SUPI to SUCI, delivering a robust and secure encryption method.

3.1.2.2. Hybrid Method

This method will combine classical and post-quantum cryptographic methods, providing an additional layer of security by leveraging the strengths of both approaches.

3.1.3. Transition to AES-256

Upgrading from AES-128 to AES-256 allows telecom networks to substantially enhance their symmetric encryption, offering robust protection against the emerging threats posed by quantum computing. This transition is a crucial component of the broader migration to post-quantum security, ensuring that all cryptographic operations within the Core are secure and future-proof.

In the following areas where AES-128 is utilized, it can be upgraded to AES-256 for enhanced encryption strength:

- **Encryption of SUPI and SUCI**: The encryption and decryption processes for SUPI to SUCI conversions using the shared secret can be migrated from AES-128 to AES-256, enhancing encryption strength and ensuring the confidentiality of subscriber identities.
- **AKA Procedure:** Within the AKA procedure, AES-128 can be replaced with AES-256 to improve security. This ensures that the authentication process remains robust against potential quantum attacks, protecting user credentials and session keys.
- **Milenage Function**: The Milenage function, used in various cryptographic operations, can adopt AES-256, including for generating the Operator's Permanent Key (oPc) value. This transition enhances the security of cryptographic operations, ensuring that key generation and verification processes are resilient against quantum threats.

3.1.4. PQ-TLS based SBI Communication between NFs

Communication between NFs currently uses mTLS which is not secure against quantum attacks. To address this vulnerability, PQ-TLS can be implemented for secure and quantum-safe communication across the network.

PQ-TLS leverages advanced cipher suites that integrate post-quantum cryptographic algorithms. These cipher suites include both homogeneous and hybrid post-quantum algorithms, similar to the approach used in SUPI to SUCI conversion, ensuring a robust and adaptable security framework for future-proofing network communications.

Key components of PQ-TLS implementation include:

- **Need for a CA**: A Certificate Authority (CA) is essential for issuing and managing digital certificates for NFs. These certificates ensure that only authorized entities can communicate within the network. Post-quantum certificates are exchanged between the Network Repository Function (NRF), the Service Communication Proxy (SCP), and other NFs, with each certificate being verified to maintain the authenticity and integrity of all communications.
- **Certificate Verification**: The process of certificate verification is crucial for ensuring secure and trustworthy communication between NFs. It involves validating the authenticity and validity of post-quantum certificates. By leveraging post-quantum cryptographic algorithms for certificate generation and verification, the network protects itself against quantum-capable adversaries, ensuring the security of all communications.
- **Encrypted Data and Messages**: PQ-TLS encrypts data and messages transmitted between NFs, ensuring that the information remains confidential and tamper-proof, safeguarding it from interception and unauthorized access. The integration of post-quantum cryptographic algorithms within PQ-TLS provides an additional layer of security, guaranteeing that data remains secure even if quantum computers eventually become capable of breaking classical encryption methods.

3.1.5. PQ-DTLS/ PQ-IPsec for User Plane Data Exchange

PQ-DTLS is specifically designed to secure datagram communications against quantum attacks, utilizing post-quantum cryptographic algorithms to ensure that data transmitted over UDP (User Datagram Protocol) remains confidential and tamper-resistant.

Similarly, PQ-IPSec enhances the security of IP communications by integrating post-quantum cryptographic methods. It ensures that data packets transmitted over IP networks are both encrypted and authenticated, safeguarding them from interception and unauthorized access.

Both protocols function as "Secure Communication" mechanisms, establishing a protected "tunnel" between two endpoints to ensure data is safeguarded with Confidentiality, Integrity, and Authentication. This is especially important for securing data in transit between the gNB and User Plane Function (UPF), where high-speed and high-volume data exchanges take place.

By transitioning to PQ-DTLS/ PQ-IPSec, telecom networks can fortify their security measures on the N3 interface, ensuring that data exchanges between the gNB and UPF are protected from quantum attacks. This migration is a crucial step in adapting to post-quantum security requirements and maintaining the overall resilience of the Core network.

3.2. Classical O-RAN to Post-Quantum O-RAN

The advancement to Post-Quantum O-RAN is crucial in protecting against the looming threats posed by quantum computing. Traditional O-RAN relies on classical cryptography, which is increasingly vulnerable to quantum attacks. The goal is to transition from O-RAN to Quantum-Secure O-RAN by employing PQC and QRNG to secure all interfaces and protocols.

Ensuring quantum security across the Backhaul, Midhaul, and Fronthaul segments of the network is paramount. Key protocols and interfaces, including RRC, F1AP, E1AP, N2 and N3, Xn, E2, O-FH (Control, User, and Synchronization Planes), O-FH (Management Plane), O1, and A1, must be fortified with quantum encryption to maintain confidentiality, integrity, and authenticity of communications.

The primary focus will be on migrating the cryptographic foundations of these protocols from classical to post-quantum standards. This includes deploying quantum-resistant algorithms to secure the transmission of data, signaling information, and control messages across the various segments of the network. Moreover, symmetric key protocols within O-RAN will undergo modifications to increase key sizes, enhancing their resistance to quantum-based attacks.

Interfaces/ Protocols	Between Nodes	Existing Security Mechanisms	Post Quantum Security Mechanisms	Specified By
RRC	UE & gNB	128-NEA/128-NIA (AES-128)	256-NEA/256-NIA (AES-256) (QRNG Based Key Generation)	3GPP
F1AP	O-CU-CP & O-DU (F1-C) O-CU-UP & O-DU (F1-U)	NDS/IP (IPsec ESP & IKEv2) or DTLS	PQ-IPsec or PQ-TLS (QRNG Based Key Generation)	3GPP
E1AP	O-CU-CP & O-CU-UP			3GPP
BackHual (N2 & N3)	O-CU-CP & 5GC (N2) O-CU-UP & 5GC (N3)			3GPP
Xn	Source gNB & Target gNB			ORAN WG11
E2	Near-RT RIC(xAPPs) & O-CU-CP			ORAN WG11
O-FH (CUS-Plane)	O-DU & O-RU	IEEE 802.1x with EAP-TLS	MACsec alongwith PQ based EAP-TLS (QRNG Based Key Generation)	ORAN WG11
O-FH (M-Plane)	O-RU & O-DU/SMO	mTLS, SSHv2	PQ-mTLS (QRNG Based Key Generation)	ORAN WG4
O1	SMO & O-RAN Managed Elements	mTLS		ORAN WG11
A1	Near-RT RIC & Non-RT RIC	mTLS		ORAN WG11

Table: Migration from Classical O-RAN to Post Quantum O-RAN

3.2.1. AES-128 to AES-256 in RRC

The Radio Resource Control (RRC) protocol, responsible for the control plane signaling between the UE and the gNB, must be upgraded to enhance its resistance to quantum attacks. Traditionally, RRC has used AES-128 for encryption, which is secure against classical attacks but potentially vulnerable to quantum decryption techniques. By migrating from AES-128 to AES-256, the encryption strength is significantly increased, providing a higher level of security.

AES-256 uses a larger key size, which makes it exponentially more difficult for quantum computers to break the encryption. This transition ensures that the control plane signaling, which includes critical information such as handover commands, connection setups, and resource allocations, remains secure even against the most advanced quantum threats.

3.2.2. PQ-IPsec/ PQ-TLS at F1AP/ E1AP/ Xn/ N2/ N3/ E2

The F1 Application Protocol (F1AP) manages the communication between the O-CU (Central Unit) and the O-DU (Distributed Unit) within the O-RAN architecture. The F1AP is split into two segments: F1-C for control plane messages and F1-U for user plane data.

The E1 Application Protocol (E1AP) handles the communication between the O-CU Control Plane (O-CU-CP) and the O-CU User Plane (O-CU-UP). Securing this interface is crucial as it deals with control plane data, which is vital for the proper functioning of the network.

The Xn interface is used for communication between source gNB and target gNB, facilitating handovers and other inter-gNB communications.

The N2 and N3 interfaces connect the O-CU-CP and the 5G Core Network. The N2 interface handles the signaling between the O-CU-CP and the Access and Mobility Management Function (AMF), while the N3 interface manages the user plane data between the O-CU-CP and UPF.

The E2 interface facilitates communication between the Near-Real-Time RAN Intelligent Controller (Near-RT RIC) and the O-DU and O-CU. This interface handles critical operational and control data, making it a prime target for securing against quantum threats.

Traditionally, IPsec or DTLS has been used to secure these interfaces' communications. However, these methods are vulnerable to quantum attacks. Transitioning to PQ-IPSec/ PQ-TLS is essential to protect the control and user plane messages. PQ-TLS provides enhanced security through the use of post-quantum cryptographic algorithms, which are resistant to quantum decryption techniques. This migration includes:

- **Utilizing PQ-TLS cipher suites** that include both homogeneous and hybrid post-quantum cryptographic algorithms to ensure robust encryption.
- **Utilizing QRNGs to generate cryptographic keys**, providing maximum security and true randomness, making it nearly impossible for quantum computers to predict or compromise the keys.

3.2.3. PQ-based MACSec and EAP-TLS at O-FH (CUS Plane)

The O-FH (Control, User, and Synchronization Plane) is responsible for the communication between the O-DU and the O-RU. Traditionally, this communication has been secured using IEEE 802.1x with EAP-TLS. However, this method is not sufficient to withstand quantum attacks.

Transitioning the O-FH (CUS Plane) to a MACSec algorithm with PQ-based EAP-TLS is crucial to enhance the security of these communications. This includes:

- **Implementing MACSec with PQ-based EAP-TLS** to secure the control, user, and synchronization plane communications.
- **Using QRNG-based key generation** to ensure the highest level of security for these critical communication links.

3.2.4. PQ-based Algorithms at O-FH (M-Plane)

The O-FH (Management Plane) handles the management communications between the O-DU and O-RU. Securing this plane is vital to protect the integrity and confidentiality of management data.

Upgrading the O-FH (M-Plane) protocols to use post-quantum cryptographic algorithms ensures secure management communications.

3.2.5. PQ-mTLS at O1/ A1 Interface

The O1 interface facilitates communication between the Service Management and Orchestration (SMO) system and O-RAN components, including the O-DU, O-CU, and O-RU.

The A1 interface connects the Near-RT RIC and the Non-Real-Time RIC (Non-RT RIC), facilitating communication between these two critical components of the O-RAN architecture.

Migrating these interfaces from mTLS to PQ-mTLS ensures robust protection against quantum-based attacks. This involves:

- **Implementing PQ-mTLS** to secure the communication at O1/ A1 interface.
- **Utilizing QRNG for key generation**, ensuring the highest level of security for these communications.

3.3. UE to Post-Quantum UE

The UE is a critical component of the telecommunications network, interacting directly with the network's core and access layers. As quantum computing continues to evolve, the cryptographic methods currently used by UEs, which rely on classical cryptography, are becoming increasingly vulnerable to quantum attacks. Therefore, transitioning UEs to Post-Quantum UEs is essential to maintain secure communication.

This migration involves several key updates and modifications to ensure that UEs are capable of handling post-quantum cryptographic operations. These changes include updating SIM cards to store post-quantum keys, modifying mobile equipment (ME) to support post-quantum algorithms, and enhancing encryption protocols. Additionally, QRNGs play a vital role in generating truly random keys, further enhancing security.

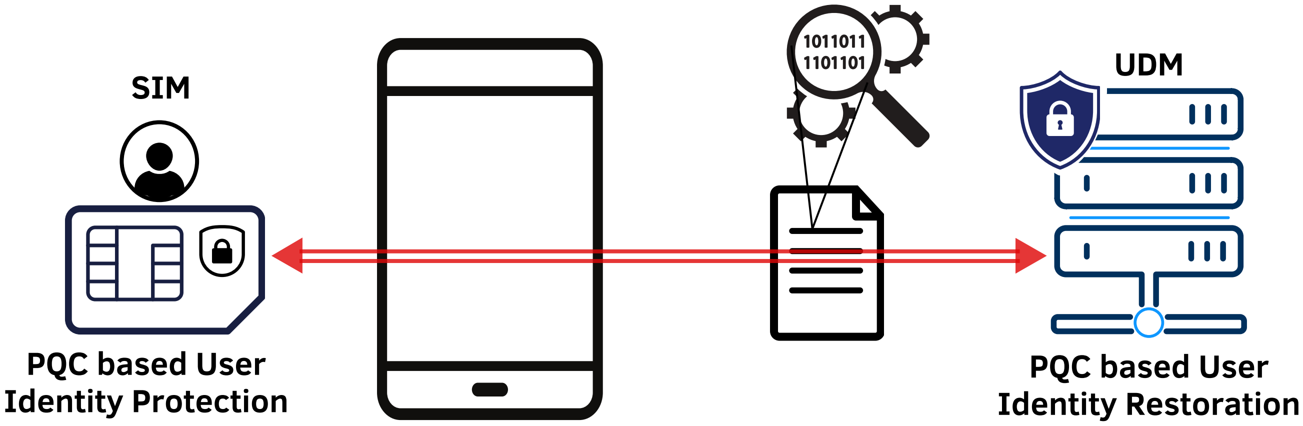

SIM
1011011
1101101
UDM
PQC based User Identity Protection
PQC based User Identity Restoration

Figure: 5G PQC SIM Card

3.3.1. SIM Card Updation to Store Post-Quantum Public Keys

One of the fundamental changes in migrating to Post-Quantum UE is updating the SIM card to store post-quantum public keys provided by the network operator. This includes:

- **Capability to Store Homogeneous and Hybrid Keys**: The updated SIM card should be capable of storing either homogeneous long-term home network public keys or hybrid long-term home network public keys, depending on the mode selected. This flexibility ensures that the UE can handle various post-quantum cryptographic algorithms as specified by the network operator.
- **Enhanced Storage and Processing Capabilities**: The SIM card needs to have enhanced storage and processing capabilities to accommodate the larger key sizes and complex

algorithms used in post-quantum cryptography. This includes secure storage for both public and private keys, as well as efficient processing power to handle cryptographic operations.

- **Secure Key Management**: Ensuring that the SIM card can securely manage these keys, including generation, storage, and usage, is crucial. QRNGs can be used to generate these keys, providing true randomness and enhanced security.

3.3.2. ME Modifications to Support Post-Quantum Algorithms

The ME must support post-quantum and hybrid post-quantum algorithms to enable quantum-secure communication. These modifications include:

- **Algorithm Support**: The ME must be capable of supporting a range of post-quantum cryptographic algorithms. This includes both homogeneous and hybrid post-quantum algorithms, which combine classical and quantum-resistant techniques to provide robust security.
- **Key Exchange and Encryption Methods**: Implementing support for new cryptographic standards, including key exchange methods and encryption protocols that are resistant to quantum attacks. This ensures that the ME can securely communicate with the network using post-quantum cryptographic methods.

3.3.3. AES-256 for Data Encryption

To enhance the security of data transmission, the UE must migrate from using AES-128 to AES-256 for encryption. This involves:

- **Updating Encryption Protocols**: All encryption protocols used by the UE for data transmission, including those for voice, text, and internet data, must be updated to use AES-256. This ensures that all data transmitted by the UE is protected by stronger encryption, resistant to quantum attacks.
- **Secure Key Management**: The UE must implement secure key management practices, including the generation, storage, and usage of AES-256 keys. QRNGs can be used to generate these keys, ensuring true randomness and enhanced security.

3.3.4. QRNG for Key Generation

QRNGs play a crucial role in enhancing the security of post-quantum UEs by providing truly random keys for cryptographic operations. This includes:

- **QRNG for Ephemeral Key Generation**: During the SUPI concealment process, QRNG seeds are used to generate ephemeral key pairs. This ensures that the keys are truly random and cannot be predicted or reproduced by quantum computers.
- **Generation of Authentication Keys**: Authentication keys can be generated using QRNG, enhancing the security of the authentication process.

There are a few commercial UEs available that have inbuilt QRNGs to provide truly random numbers. These devices are capable of generating high-entropy keys for various cryptographic operations, ensuring enhanced security.

3.3.5. SUPI Concealment using PQC and QRNG

The SUPI concealment process must be upgraded to utilize either homogeneous or hybrid post-quantum encryption methods, , ensuring that the sensitive identifiers remain secure against the advanced capabilities of quantum computers.

3.3.5.1. Homogeneous Post-Quantum Method

This method employs a single type of post-quantum cryptography method for the conversion of SUPI to SUCI, delivering a robust and secure encryption method.

3.3.5.2. Hybrid Post-Quantum Method

This method will combine classical and post-quantum cryptographic methods for the SUPI to SUCI conversion, providing an additional layer of security by leveraging the strengths of both approaches.

By implementing these changes, telecom networks can ensure that UEs are equipped to handle the threats posed by quantum computing. This transition to post-quantum UEs involves a comprehensive update of cryptographic methods, key management practices, and hardware capabilities. Ensuring quantum security for UEs is a critical step in safeguarding the entire telecommunications infrastructure against future quantum threats.

The migration from classical to post-quantum UEs not only addresses immediate security concerns but also lays the groundwork for continuous innovation and advancements in quantum security. By adopting post-quantum cryptographic methods and leveraging the power of QRNGs, telecom networks can provide robust, future-proof security for user communications, ensuring the reliability and integrity of next-generation telecommunications networks.

4. Quantum-Safe Solutions

By implementing the changes outlined in the migration section, Coranlabs has developed quantum-secure solutions for 5G networks: **QORE**, a Quantum-Secure Core, and **Q-RAN**, a Quantum-Secure RAN.

4.1. QORE: Core with PQC and QRNG

Communication between NFs is facilitated via SBI, supplemented by the SCP. This communication is secured using **PQ-mTLS**, which incorporates Hybrid Post-Quantum Signature schemes (*Ed448-ML-DSA3*) for signatures and certificates, and Hybrid PQ-KEM (*x25519-ML-KEM768*) for key exchange.

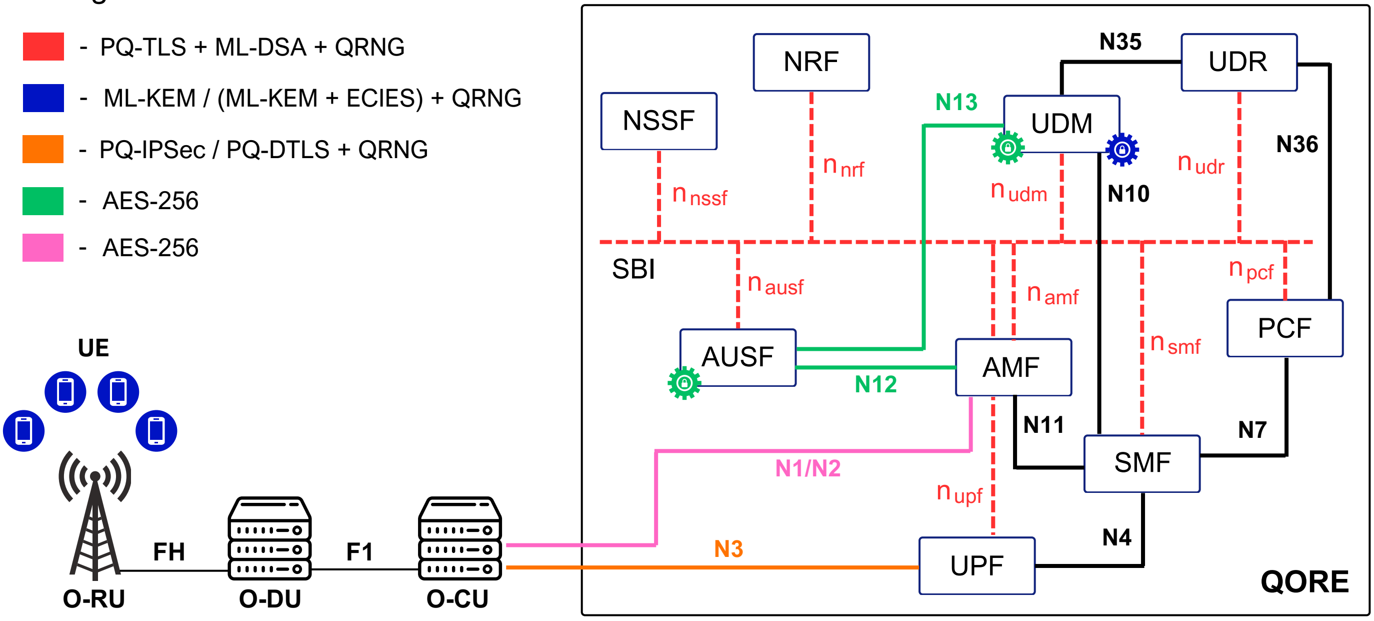


Figure: QORE: Quantumized Core Solution

4.1.1. Homogeneous Post-Quantum Encryption Mode

It employs ML-KEM exclusively, combined with key generation through QRNG, for the conversion of SUPI to SUCI and vice versa, delivering a robust and secure encryption method.

It leverages AES-256 for enhanced encryption, offering a higher level of security compared to earlier standards.

It also supports multiple encryption profiles, each designed to provide progressively stronger levels of security. These profiles are tailored to meet varying security requirements, allowing the network to adapt to different threat levels and operational needs.

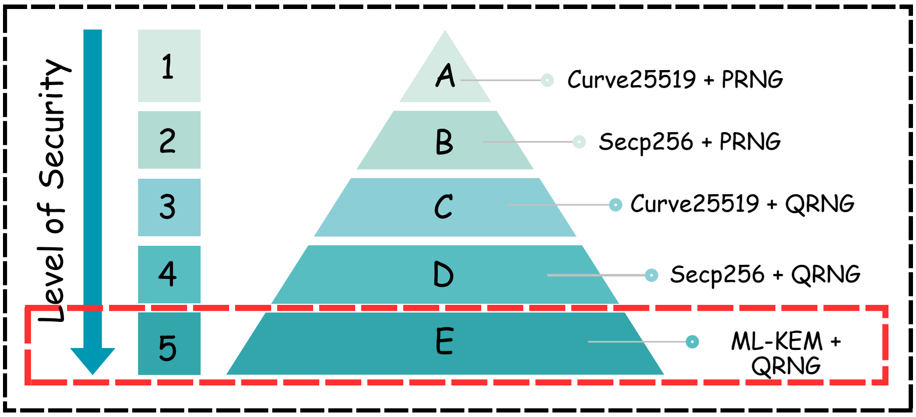


Figure: QORE-Homogeneous Mode: Encryption Profile

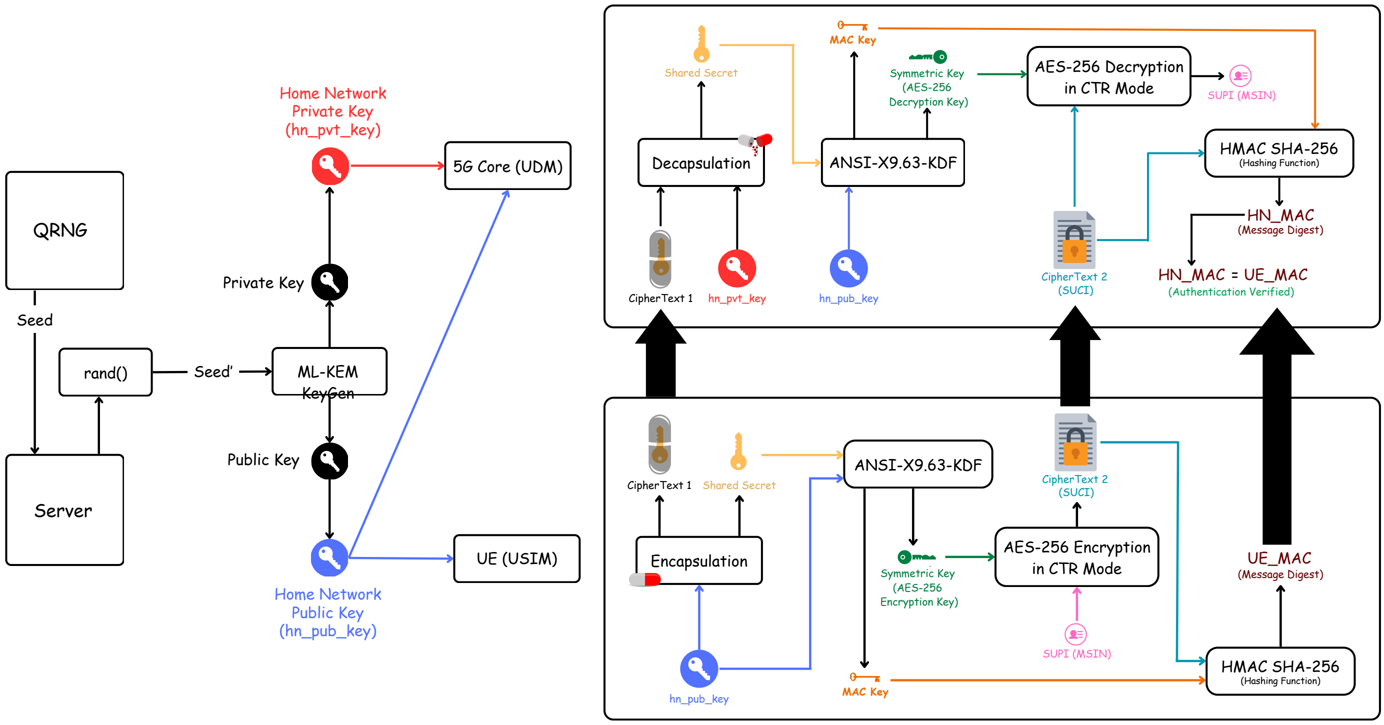


Figure: QORE: Homogeneous Post-Quantum Encryption Mode

Here are the steps involved in securing a user's identity in QORE under the Homogeneous Post-Quantum Encryption Mode:

- **ML-KEM-Keygen (Post-Quantum Algorithm) using QRNG Seeds**:
  - Random seeds generated by QRNG are used to create the home network's public key (hn_pub_key) and private key (hn_priv_key).
- **Key Distribution:**
  - The hn_pub_key is sent to the UE, while both key pairs (hn_pub_key and hn_priv_key) are securely stored in the User Data Management (UDM) module within the 5G Core.
- **Encryption at the UE Side:**
  - The hn_pub_key at the UE is used to perform encapsulation, generating a shared secret and a cipher text (ct1)
  - The shared secret and hn_pub_key are then passed through a Key-Derivation Function (ANSI-X9.63-KDF), which produces a symmetric_key and a mac_key.
  - The symmetric_key is used to encrypt the SUPI (MSIN) using the AES-256-CTR algorithm, resulting in cipher text (ct2), which is effectively the SUCI.
  - Cipher text (ct2) and mac_key are then passed through the HMAC-SHA256 hashing function to create a message digest known as UE_MAC.
  - The UE sends Cipher texts (ct1 & ct2), and UE_MAC to the UDM.
- **Decryption at the UDM Side:**
  - The UDM uses cipher text (ct1) and hn_priv_key to perform decapsulation, reconstructing the shared secret.
  - The shared secret and hn_pub_key are passed through the Key-Derivation Function (ANSI-X9.63-KDF) again to regenerate the symmetric_key and mac_key.
  - This symmetric_key will be used to decrypt SUCI (ct2) using the AES-256-CTR algorithm, revealing the original SUPI.
  - Cipher text (ct2) and mac_key are hashed using HMAC-SHA256 to produce another digest

called HN_MAC.

- **Message Integrity Verification:**
  - It involves comparing HN_MAC with UE_MAC. If they match, the message authentication is successfully verified, ensuring the integrity and confidentiality of the user's identity throughout the process.
  - After the verification, SUCI is decrypted to obtain SUPI.

4.1.2. Hybrid Post-Quantum Encryption Mode

This approach combines the post-quantum algorithm ML-KEM with classical algorithms like Curve25519 and Secp256r1, along with key generation through QRNG, for the conversion of SUPI to SUCI and vice versa. This hybrid method enhances security by leveraging both quantum-resistant and classical cryptographic techniques.

By utilizing a 256-bit key, AES-256 significantly strengthens the encryption process, ensuring that even with the advent of quantum computing, the integrity and confidentiality of communications are maintained.

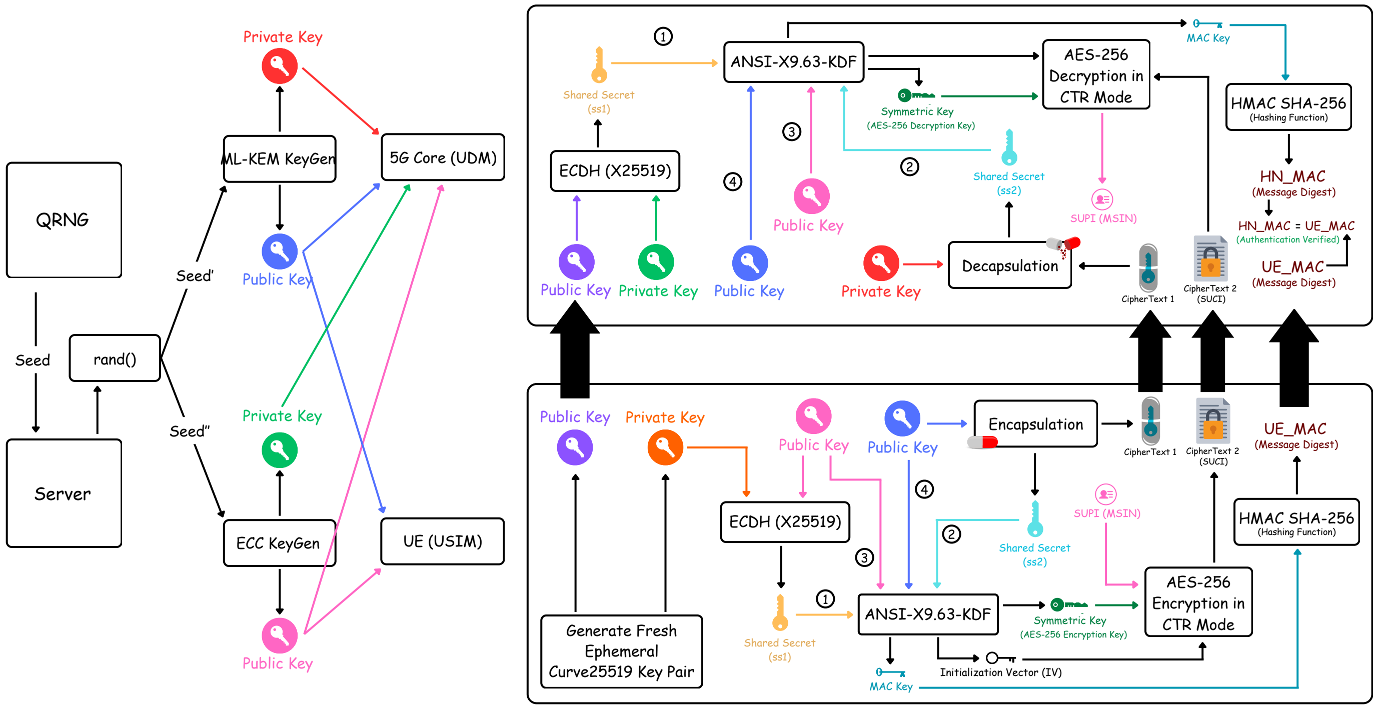


Figure: QORE: Hybrid Post-Quantum Encryption Mode

Here are the steps involved in securing a user’s identity in QORE under the Hybrid Post-Quantum Encryption Mode:

- **Long-Term Key Generation:**
  - At the Home Network (HN), a QRNG generates two seeds of 64 and 32 bytes, respectively. The 64-byte seed is used to create Long-Term (LT) ML-KEM512/768 keys: HN_ML-KEM_PRIV_KEY and HN_ML-KEM_PUB_KEY. The 32-byte seed generates a Curve25519 Private Key (HN_ECC_PRIV_KEY) and a corresponding Public Key (HN_ECC_PUB_KEY).
  - The Long-Term public keys, HN_ML-KEM_PUB_KEY and HN_ECC_PUB_KEY, are sent to the UE, while their corresponding private keys along with the public keys are securely stored in the UDM of the 5G Core.

- **Initial Registration Process:**
  - During the initial registration initiated by the UE, an ephemeral Curve25519 (ECC) Key pair is generated at the UE: eph_priv_key and eph_pub_key.
  - The eph_priv_key is combined with the HN_ECC_PUB_KEY to form a shared secret (ss1), using the X25519 Elliptic Curve Diffie-Hellman (ECDH) protocol.
  - Additionally, the HN_ML-KEM_PUB_KEY is encapsulated to obtain a ciphertext (ct1), and another shared secret (ss2).
- **Key Derivation and Encryption:**
  - The shared secrets (ss1 and ss2), are passed to the ANSI-X9.63 Key Derivation Function (KDF) in the following order: ss1 + ss2. The KDF uses HN_ECC_PUB_KEY + HN_ML-KEM_PUB_KEY as shared information, resulting in the generation of three keys: a symmetric key (enc_key), an Initialization Vector (IV), and a MAC key (mac_key).
  - The enc_key and IV are used to encrypt the critical part of the SUPI (MSIN) using the AES-256-CTR algorithm, resulting in the SUCI.
  - HMAC-SHA256 is then used to generate a MAC tag (UE_MAC) with the concealed MSIN as the data and mac_key as the key.
  - The eph_pub_key, cipher text (ct1), SUCI, and UE_MAC are sent to the UDM.
  - Any traces of cipher text (ct1), eph_priv_key, and eph_pub_key are immediately deleted from the UE.
- **Decryption and Verification at UDM:**
  - At the UDM, the eph_pub_key is combined with the HN_ECC_PRIV_KEY using X25519 ECDH to recreate the shared secret (ss1). The cipher text (ct1) is decapsulated using HN_ML-KEM_PRIV_KEY to obtain the shared secret (ss2).
  - These shared secrets (ss1 and ss2) are passed to the ANSI-X9.63 KDF (in the same order as before) along with HN_ECC_PUB_KEY + HN_ML-KEM_PUB_KEY as shared information, generating a symmetric key (dec_key), an Initialization Vector (IV), and a MAC key (mac_key).
  - HMAC-SHA256 is then applied to the SUCI with mac_key to produce the MAC tag, UDM_MAC. If UDM_MAC matches UE_MAC, the procedure continues; otherwise, it is aborted.
  - Finally, dec_key and the IV are used to decrypt the SUCI using AES-256-CTR, revealing the SUPI (including the MSIN).
  - All traces of cipher text (ct1) and eph_pub_key are immediately deleted, completing the process.

4.1.3. PQ-mTLS based SBI Communication

In this aspect of QORE, mTLS-based communication between NFs is upgraded to PQ-mTLS. QORE supports both homogeneous and hybrid post-quantum signature algorithms within its shared cipher suites. A local Hybrid Post-Quantum Certificate Authority (CA) is established to issue digital PQ-Certificates to the NFs.

Additionally, QRNG is used to generate seeds for creating both post-quantum and classical ephemeral key pairs, such as ML-KEM768 and ECC X25519. Through PQ-TLS, encrypted data and messages are exchanged between network functions, ensuring confidentiality and tamper resistance, thereby safeguarding the information from interception and unauthorized access.

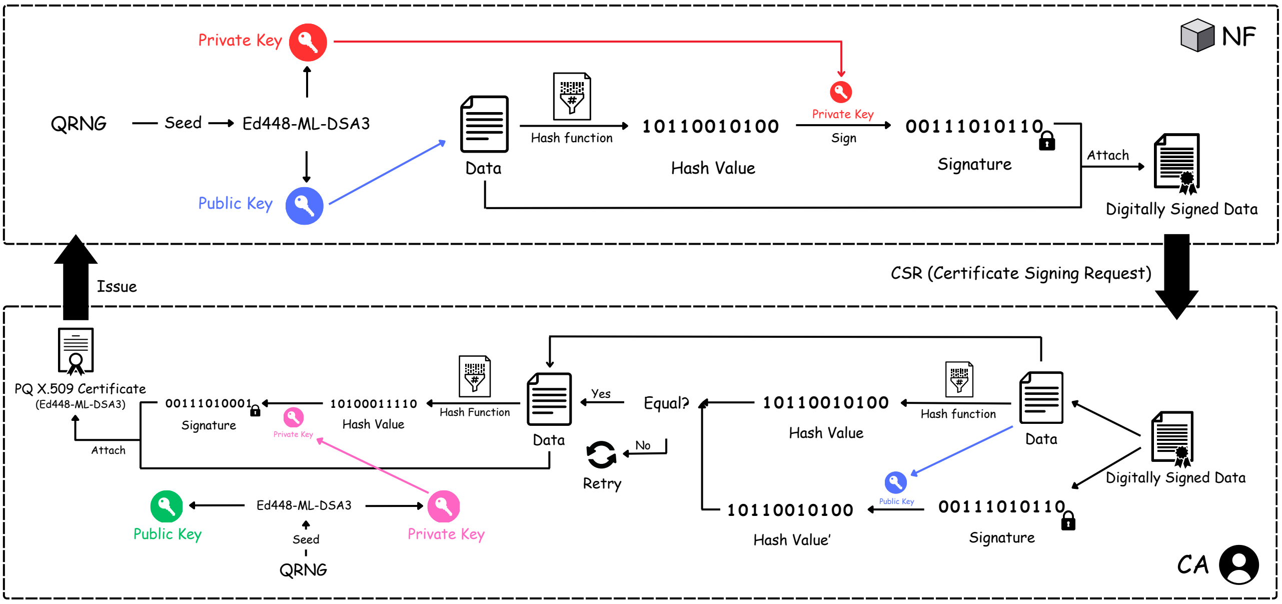


Figure: QORE: PQ X.509 Certificate Generation

Here are the message exchanges between the NRF and NF during the NF registration process with the NRF:

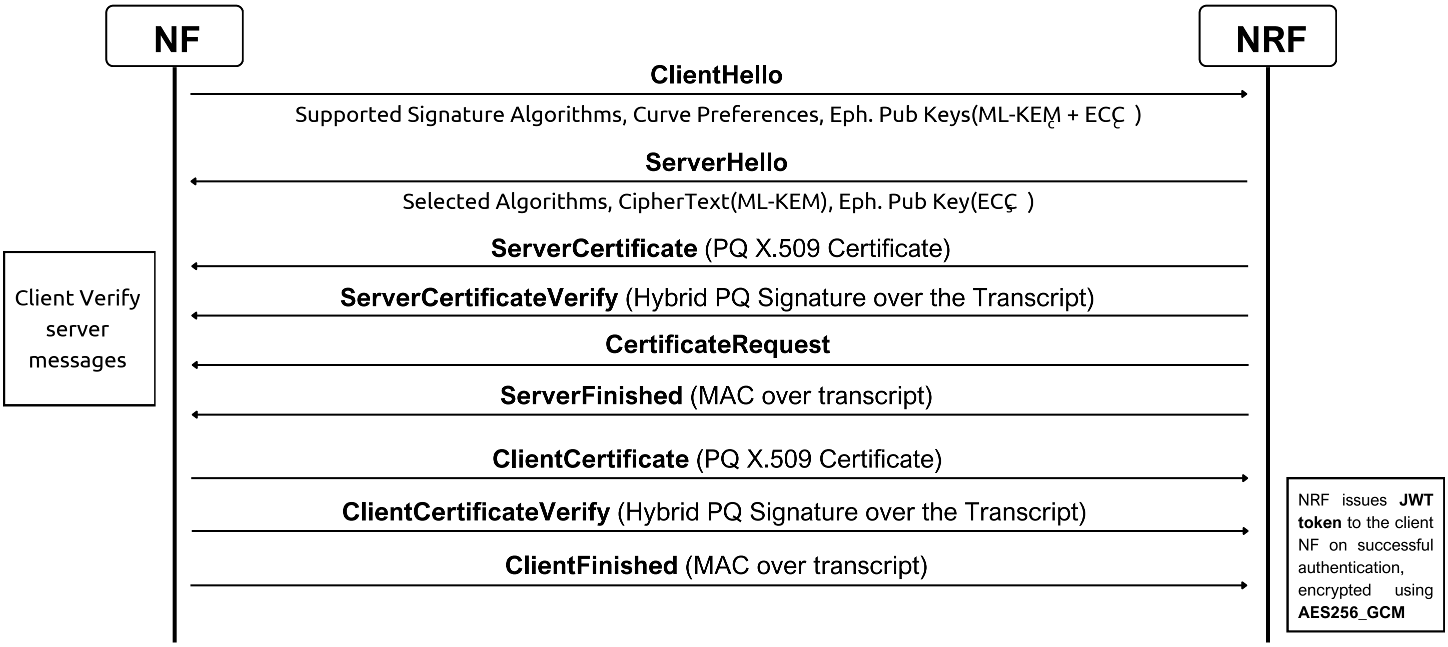

NF
NRF
ClientHello
Supported Signature Algorithms, Curve Preferences, Eph. Pub Keys(ML-KEM + ECC)
ServerHello
Selected Algorithms, CipherText(ML-KEM), Eph. Pub Key(ECC)
ServerCertificate (PQ X.509 Certificate)
ServerCertificateVerify (Hybrid PQ Signature over the Transcript)
CertificateRequest
ServerFinished (MAC over transcript)
ClientCertificate (PQ X.509 Certificate)
ClientCertificateVerify (Hybrid PQ Signature over the Transcript)
ClientFinished (MAC over transcript)
Client Verify server messages
NRF issues **JWT token** to the client NF on successful authentication, encrypted using **AES256_GCM**

Figure: QORE: PQ-mTLS Based SBI Communication

To exchange data between two NFs (excluding NRF), each NF first connects to the SCP and presents its JWT token for verification. Once verified, the SCP routes the request to the target NF. After confirming they are connected to the correct peers, the NFs perform key exchange using PQ KEMs, followed by data encryption with AES256_GCM.

4.2. Q-RAN: O-RAN with PQC and QRNG

QRAN is an advanced O-RAN solution integrated with Post-Quantum Cryptography and QRNG, designed to fortify network communications against the emerging threats posed by quantum computing.

3GPP and ORAN-based protocols and interfaces, including RRC, F1AP, E1AP, N2 and N3, Xn, E2, O-FH (CUS-planes), O-FH (M-Plane), O1, and A1, are enhanced by transitioning from classical encryption methods to quantum encryption mechanisms. This upgrade ensures the confidentiality, integrity, and authenticity of communications across the network.

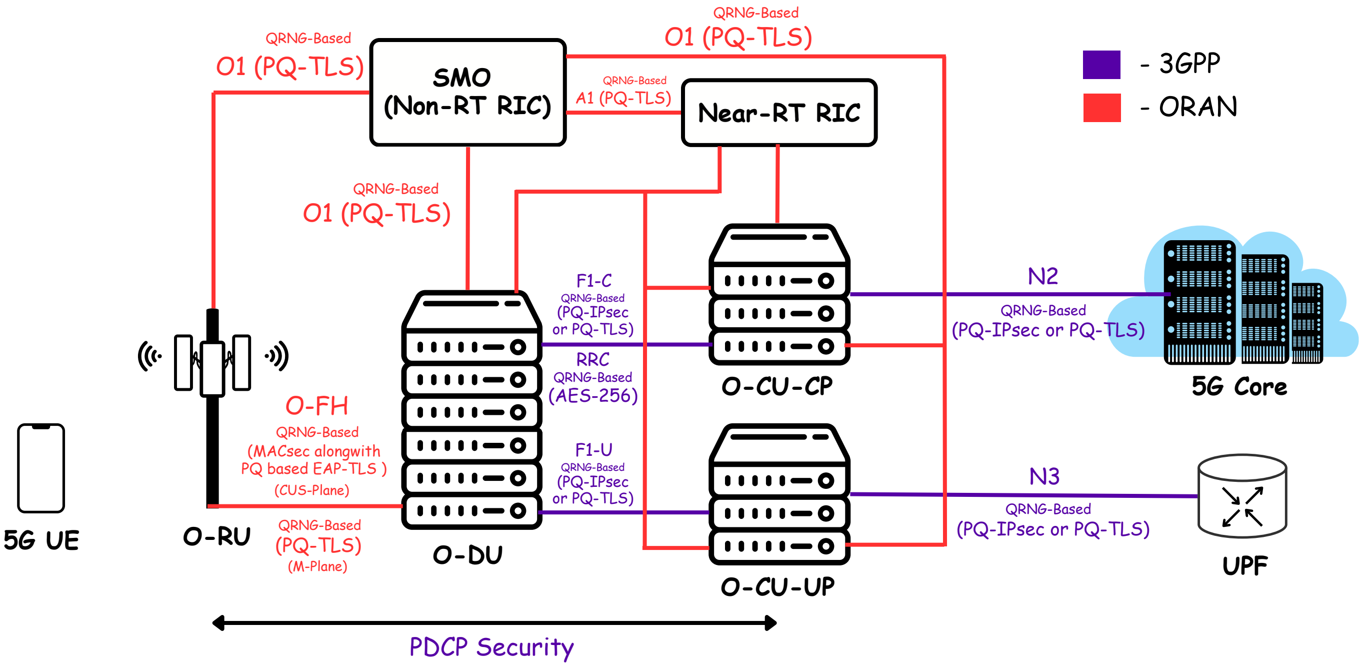


Figure: Q-RAN: Quantumized O-RAN

It leverages **Hybrid PQ-TLS** across the BackHaul, MidHaul, and FrontHaul interfaces, ensuring that communications are secure and resilient against quantum attacks. This advanced security protocol combines both post-quantum and classical cryptographic algorithms to create a robust defense mechanism, safeguarding critical network data from potential breaches by quantum-powered adversaries.

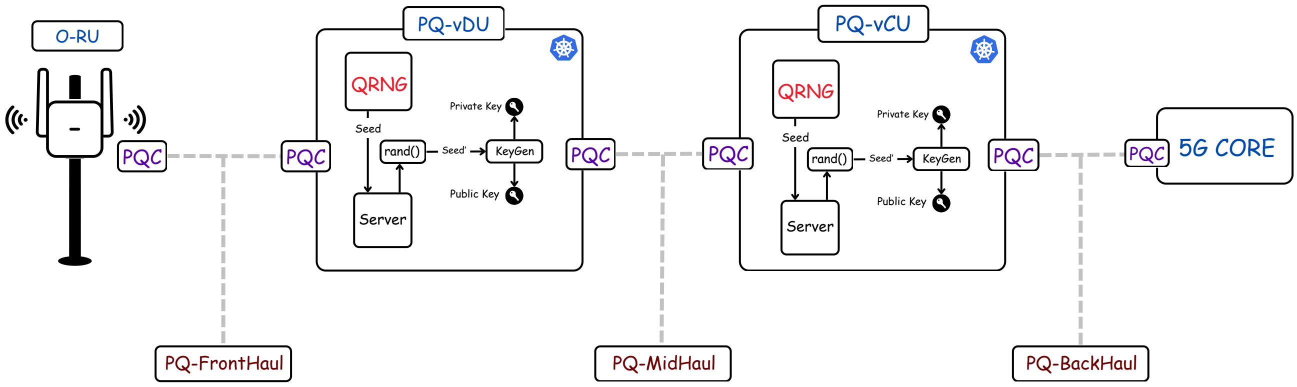


Figure: Virtualised Q-RAN

It also employs **AES-256** instead of AES-128 for advanced symmetric encryption, providing robust protection with a 256-bit key length to ensure data integrity and confidentiality.

4.3. E2E Quantum Secure Solution

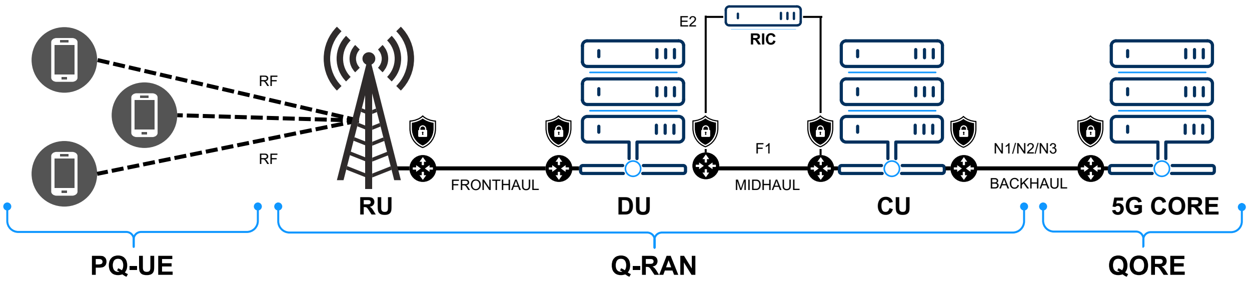


Figure: E2E Quantum Secure Connection

5. Conclusion

The migration from classical cryptography to post-quantum security in telecommunications is not just an upgrade; it is a necessity to safeguard against the impending threats posed by quantum computing. By transitioning the Core, O-RAN, and UE components to post-quantum cryptographic methods, we can ensure that our telecommunications networks remain secure and resilient in the face of future technological advancements.

As we look toward the future, the adoption of post-quantum cryptography will play a pivotal role in maintaining the trust and reliability of our telecommunications infrastructure. By proactively addressing these security challenges, we can pave the way for continuous innovation and ensure that our networks remain robust and secure in an increasingly quantum-capable world.

The journey to post-quantum security is a complex but necessary evolution, and with these steps, we are well on our way to building a secure, future-proof telecommunications network that can stand the test of time.