



Quantum-Secure 5G/6G Networks

July 2026

Introduction

The emerging quantum computers represent a paradigm shift, harnessing quantum-mechanical effects to run certain algorithms exponentially faster than today's computers, thereby potentially threatening the encryption algorithms that are the bedrock of mobile communication networks.

Their power comes from quantum bits ("qubits"), which permit superposition of both 0 and 1 at the same time by assigning weighted probabilities to 0/1, and entanglement, where the state of one qubit is intrinsically linked to that of another, even when they are physically far apart. Because of these properties, qubits can perform many calculations simultaneously, giving quantum computers the potential to solve certain problems much faster than classical machines.

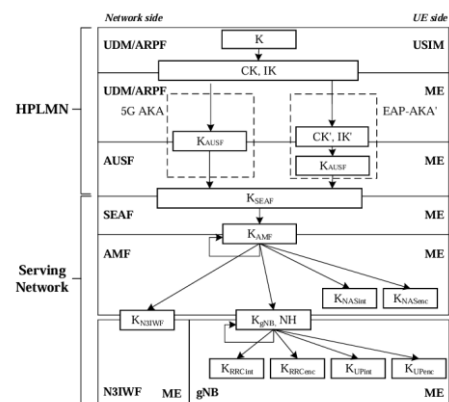
This paper outlines the quantum threat to 5G and its mitigation using Lekha's solution, designed to evolve seamlessly to 6G.

The Quantum Threat to 5G/6G

Quantum computing could pose a challenge to 5G/6G security by undermining cryptographic algorithms that safeguard subscriber authentication, privacy, data confidentiality, and data integrity.

5G authentication (5G-AKA) relies on a pre-shared K key to generate an authentication vector (RAND, AUTN, XRES, CK, IK). While the mechanism itself is not broken by quantum computers, the symmetric algorithms used to derive these values are weakened by Grover's Algorithm, making longer key sizes advisable.

Asymmetric cryptographic systems such as ECC — used in TLS for communication within 5GC Network Functions, in IKEv2/IPsec for traffic protection, and in 5G's SUCI mechanism to protect subscriber identities — will become vulnerable to quantum attacks using Shor's Algorithm. Similarly, symmetric systems such as AES or Snow 3G, used for over-the-air encryption and integrity protection, will be weakened by Grover's Algorithm and will require larger key sizes (e.g., 256-bit) to remain secure.



Source: 3GPP Rel-15, 33.501, Figure 6.2.1-1

Why Now?

While large-scale quantum computer deployments may still be a few years away, the threat to sensitive mobile communications - such as those used by the government, military, and homeland security - is immediate due to the risk of "harvest now, decrypt later" (HNDL) attacks, in which adversaries intercept and store encrypted communications today with the expectation of decrypting them once practical quantum computers become available.

It is therefore essential that 5G/6G equipment providers, private network managers, and public telecom service providers begin pilot projects for quantum-secure networks now, to build the necessary understanding, expertise and operational readiness for a future in which large-scale quantum computing is deployed.

Quantum-Safe Key Management with 5G

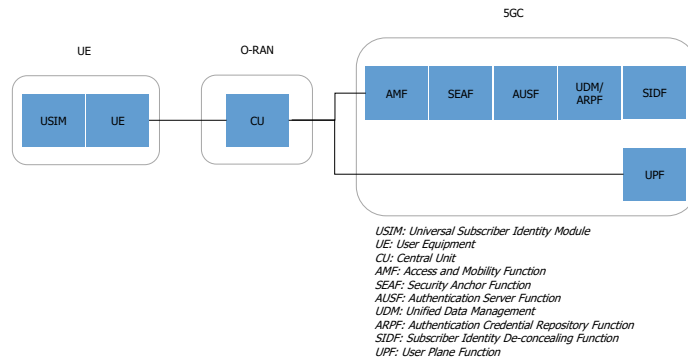
Symmetric keys are not distributed in 5G — they are derived from the user-specific pre-shared K key, in the USIM and 5GC. So post-quantum key distribution techniques are not needed over-the-air or over the terrestrial transmission network to/from the 5GC. Key distribution is required for 5GC inter-NF communication and, if deployed, for user data tunneling over backhaul networks, where asymmetric key exchange is used.

The National Institute of Standards and Technology (NIST), USA, is leading global efforts to standardize Post-Quantum Cryptography (PQC) algorithms. PQC provides secure alternatives for asymmetric key exchange, and for 5G, CRYSTALS-Kyber is the leading candidate to replace ECC-based mechanisms in TLS, IKEv2 and SUCI. As well,

symmetric cryptography algorithms used in 5G (AES and Snow 3G) will require migration to 256-bit keys to ensure data confidentiality and integrity protection.

These enhancements are expected to be incorporated in later 3GPP specifications, likely from Release 20 (the 6G baseline) onwards.

Note that per 3GPP standards, while user traffic is always encrypted over the air, encryption over the backhaul network is an operator deployment option, typically implemented using IPsec tunnels. Also, NAS signaling is required to be encrypted, while NGAP signaling over the backhaul is an operator option. (Access Stratum (AS) signaling is also generally encrypted by operators to prevent eavesdropping, while not strictly required by 3GPP.)



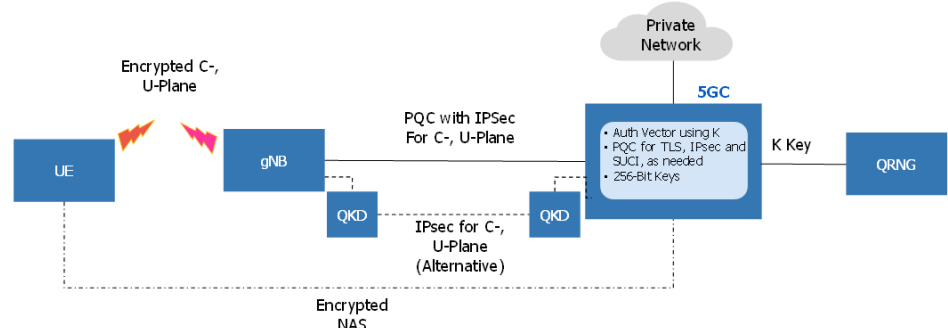
Security-Related 5G Functional Elements

As an alternative, emerging Quantum Key Distribution (QKD) systems could be integrated with IPsec or TLS to securely distribute symmetric keys, which can then be used to encrypt all signaling and traffic on backhaul networks.

Quantum-Secure Lekha 5G

Lekha's 5G solution can be extended with post-quantum security, evolving seamlessly to 6G. Built using Lekha's and other indigenous network elements, it supports mobile voice, video, and data communications, as well as private network access. The solution includes the following:

1. A 3GPP-compliant 5G testbed with a 5GC and Open RAN network elements based on the O-RAN Alliance's 7-2x Split
2. A Quantum Random Number Generator (QRNG) to generate subscriber root keys (K) with true randomness, ensuring maximum entropy in key generation
3. The CRYSTALS-Kyber PQC algorithm to securely distribute subscriber root keys (K) to USIM programmers and the UDM, making root key provisioning quantum-safe from the outset
4. CRYSTALS-Kyber for key establishment in TLS within the 5GC, in IKEv2/IPsec backhaul tunnels, and as a replacement for ECIES in SUCI protection. Alternatively, as a technology demonstrator, a Quantum Key Distribution (QKD) system can be used to securely distribute AES session keys for backhaul IPsec tunnels
5. Migration to 256-bit symmetric keys (e.g., AES-256) for enhanced encryption and integrity protection.



Conclusion

Quantum computing will fundamentally reshape mobile network security. By extending our indigenous 5G solution with post-quantum security technologies, Lekha is well positioned to deliver a sovereign, quantum-resilient communications platform, with a seamless evolution path to 6G.

Abbreviations

Abbreviation	Description
5GC	5G Core
AKA	Authentication and Key Agreement – protocol to authenticate subscribers and generate keys
AS	Access Stratum – signalling and data between the device and the RAN (gNB)
COTS	Commercial-Off-The-Shelf
CU	Central Unit
CK	Cipher Key – key from authentication used for encryption
DU	Distributed Unit
ECIES	Elliptic Curve Integrated Encryption Scheme – public-key encryption used for SUCI protection
ECDH	Elliptic Curve Diffie–Hellman – asymmetric key exchange algorithm
ECDHE	Elliptic Curve Diffie–Hellman Ephemeral – ECDH variant with forward secrecy, used in TLS
ECC	Elliptic Curve Cryptography – cryptography based on elliptic curves (used in ECIES, ECDH)
ESP	Encapsulating Security Payload – IPsec protocol providing encryption and integrity
FDD	Frequency Division Duplex
gNB	Next Generation Node B (gNodeB)
IKEv2	Internet Key Exchange v2 – protocol to negotiate keys for IPsec tunnels
IK	Integrity Key – key from authentication used for integrity protection
K	Subscriber Root Key – long-term key stored in USIM and UDM
KDF	Key Derivation Function – algorithm to derive new keys from an existing key
MAC	Message Authentication Code – ensures data integrity and authenticity
NAS	Non-Access Stratum – signalling between UE and 5GC (via gNB), encrypted once security is activated
NEA	5G Encryption Algorithm – over-the-air encryption algorithms (AES, Snow 3G, ZUC)
PQC	Post-Quantum Cryptography – algorithms secure against quantum computers
QKD	Quantum Key Distribution – uses quantum mechanics to securely distribute symmetric keys
QRNG	Quantum Random Number Generator – device producing truly random numbers
RES/XRES	(Expected) Response – values in authentication vector used to verify the subscriber
SUCI	Subscription Concealed Identifier – encrypted form of SUPI to protect identity
SUPI	Subscription Permanent Identifier – subscriber’s permanent identity (like IMSI)
TLS	Transport Layer Security – protocol securing 5GC network function communication
TSDSI	Telecommunications Standards Development Society, India

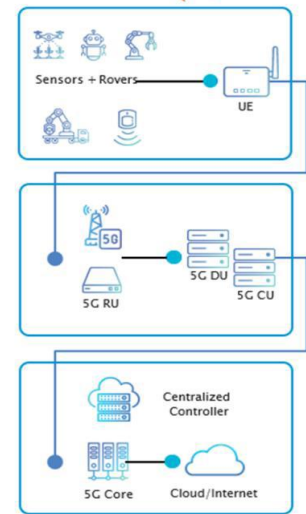
About Lekha 5G

Lekha 5G is an open, interoperable 5G solution built to O-RAN Alliance and 3GPP standards, that eliminates vendor lock-in and scales easily using disaggregated functional components from Lekha and 3rd parties.

Lekha's maRUt Radio Unit (RU) portfolio includes a range of products in multiple form factors suitable for various deployment scenarios – rugged high-power and mid-power units for outdoor use, and lightweight low-power units indoors. All popular FDD and TDD bands are supported. The Distributed Unit (DU) and Central Unit (CU) are fully disaggregated, feature open interfaces, and deployed on commercial off-the-shelf (COTS) servers for scalability. Lekha's Service Management and Orchestration (SMO) software also runs on COTS servers and provides RAN network management capability. It can be integrated with third party network elements using REST APIs.

Lekha Wireless is a deep-tech company that designs and manufactures 5G, 4G and dot16 RAN infrastructure for private, public and defence networks. Founded in 2010, Lekha is focused on R&D of these wireless connectivity technologies and actively participates in 5G-Advanced and 6G standardization. Lekha is a member of the TSDSI SDO and is a founding member of the Bharat 6G Alliance.

For more information or a demonstration, please send a request to business@lekhawireless.com. For details on other products please visit www.lekhawireless.com.



O-RAN Compliant RU, DU, CU and SMO