6G FOUNDRY

Qualcomm
Engineering Human Progress

Securing the future of mobile connectivity

Ensuring a resilient and trustworthy communication ecosystem that protects data and maintains privacy for existing and future applications

Learn more:

6G Foundry: Explore the next generation of wireless connectivity with Qualcomm experts.

Read Part 6 — Refreshing the lower-band spectrum design

As we look ahead to the next decade of mobile connectivity, now is a good time to consider how security needs could evolve:

- **Advancements in connectivity, compute and AI bring unprecedented opportunities, but they also demand robust security measures to protect our digital future.**
- **As the world's leading wireless innovator, our vision is to continue creating a secure, adaptable and trustworthy mobile ecosystem that meets today's challenges and is prepared for tomorrow's threats.**
- **We are working to establish a robust trust framework for 6G on top of the existing secure 5G foundation that would facilitate a secure, resilient and adaptable network infrastructure, capable of withstanding modern cyber threats and ensuring the integrity and confidentiality of communications.**

Since the foundation for secure connectivity was established with 3GPP Release 15, 5G security has been continuously enhanced. Each subsequent release strengthened the security of the connectivity we rely on today. With the rise of massive parallel computing, AI tools trained on large datasets and quantum computing, which all make for more capable threat vectors, the importance of securing connectivity, compute and AI has never been stronger. As efforts to shape 6G within the 3GPP ecosystem gather momentum, now is the time to look closer at securing the future of mobile connectivity.

Welcome to the seventh installment of the 6G foundry series, where we explore **6G native security, robust trust frameworks** and **quantum-safe security** to build a secure 6G on top of the existing secure 5G foundation that is resilient against known and imaginable future threats.

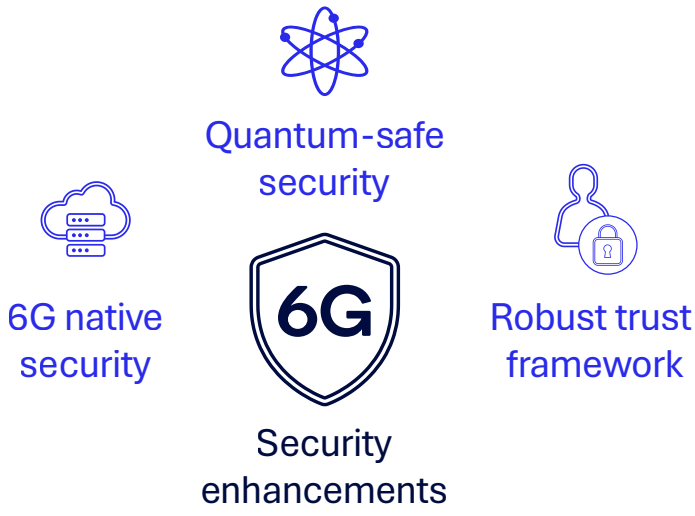

Figure 1. Security enhancements to 6G

6G native security

In this section, we look at ways to fundamentally improve security in the 6G access stratum (AS), which includes the radio access network (RAN) and the user equipment (UE). By addressing key areas such as secure control messages, enhanced mobility security, flexible user plane (UP) security termination points and user identity privacy, we aim to build a resilient 6G foundation.

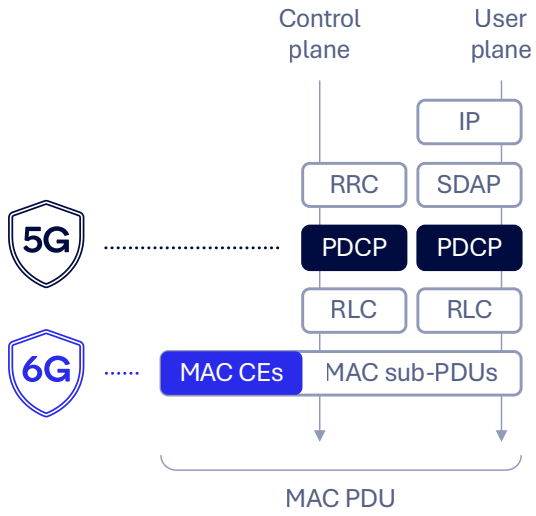

Figure 2. Ensure confidentiality, authenticity and replay protection of all control messages and user plane traffic

Secure control messages

Ensuring the confidentiality and authenticity of control messages is key to building a secure foundation for 6G. 5G AS security currently defines security at the packet data convergence protocol (PDCP) layer to safeguard control plane traffic for the radio resource control (RRC) protocol and UP traffic such as internet protocol (IP). However, there is no security protection for control messages at the lower layers, such as medium access control (MAC) elements (CEs). Manipulation of these elements can degrade or disrupt the link, such as with timing advance, transmission configuration indicator and buffer status report messages. Additionally, side channel information leakage, such as UE mobility patterns, has been shown to be possible (e.g., in the paper "Stealthy Location Identification Attacks Exploiting Carrier Aggregation (SLIC)"). Radio link control (RLC) and PDCP status reports are also currently not protected, where manipulation can potentially lead to packet loss, unnecessary duplication or radio link failure.

To counter these possible threats, 6G AS security could be improved by incorporating MAC layer security alongside the existing PDCP security to ensure comprehensive protection of all control messages and UP traffic.

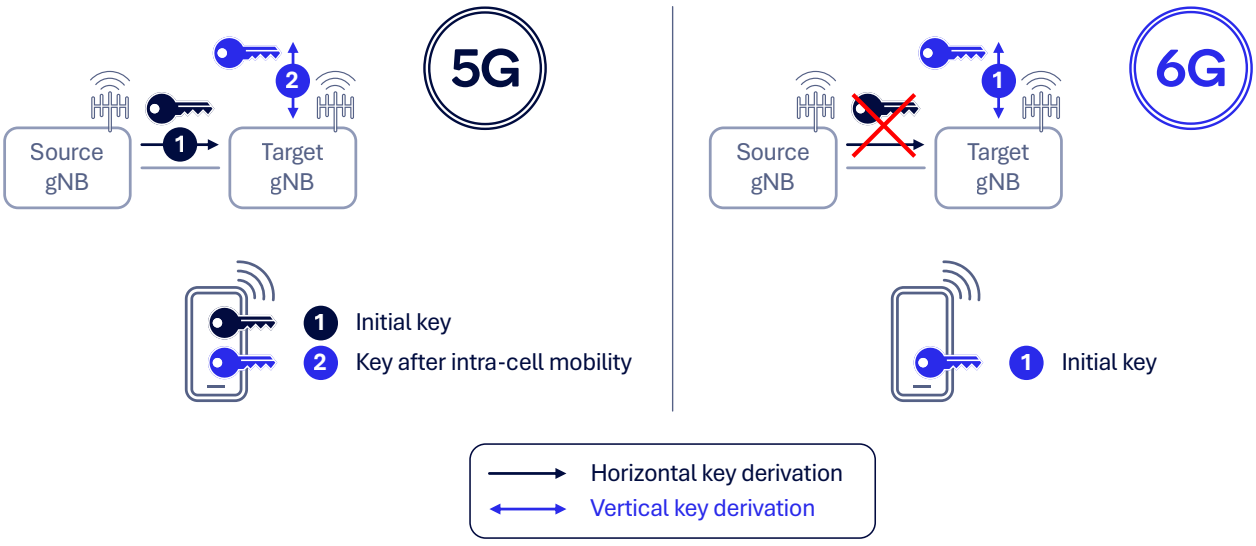

Figure 3. Enhance forward security for RAN mobility with key hierarchy

Enhance security for RAN mobility

Security for RAN mobility is a potential enhancement for 6G native security, focusing on a robust key hierarchy for enhanced forward security1 during mobility. In the current 5G framework, key changes are facilitated by the Xn interface (i.e., RAN-based mobility necessitate RRC signaling, with the source gNB supplying the key to the target gNB via the Xn interface). Additional RRC signaling for intra-cell handover at the target gNB is therefore required to support forward security. However, this process could delay key separation between gNBs and impacts the preparation of the gNB key (KgNB) at multiple gNBs for features such as subsequent L1/L2 triggered mobility (LTM).

To address these challenges, 6G key change procedures could be enhanced with forward and backward security2 by design, with vertical key derivation for a change in gNB during handover. This approach ensures the connection at the target gNB node remains secure even if the keys at the source gNB node are compromised. Additionally, supporting multiple concurrent AS key preparations at different RAN nodes (gNBs) will enhance the overall security and flexibility of the 6G network.

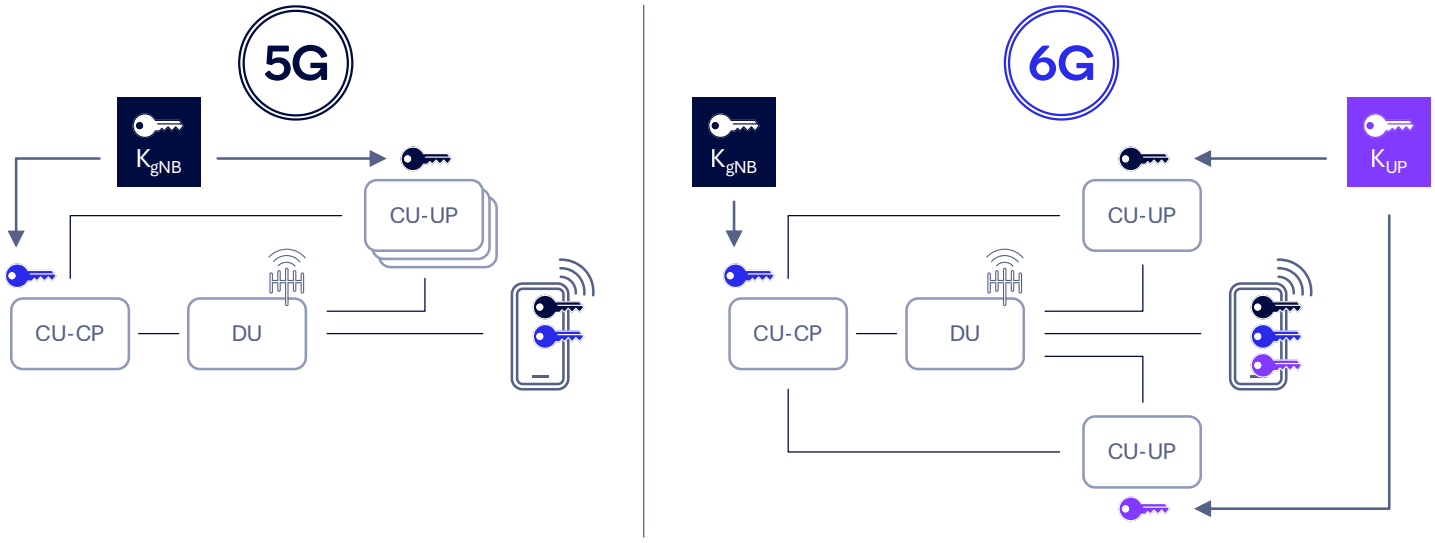

Figure 4. Serve different applications and services with different user plane security termination points

Bring flexibility to user plane security termination points

UP data could be made more secure by allowing different UP termination points tailored to specific application or service needs. In the context of 5G, a UE might connect to multiple centralized unit user plane nodes (CU-UPs) of a gNB, each corresponding to a different protocol data unit (PDU) session. However, this setup introduces potential security threats, such as the lack of key separation when multiple user planes are configured for a single UE, particularly for different PDU sessions or network slices. Moreover, binding the UP security key of a CU-UP to a centralized unit control plane (CU-CP) managed key (i.e., KgNB) can lead to frequent key changes especially for highly mobile UEs, which will incur significant signaling overhead for low-complexity Internet of Things (IoT) devices.

To resolve these issues, we propose designing 6G AS security to support key separation for different UP termination points based on network deployment, UE mobility patterns and service security requirements, while maintaining protocol consistency to the UE and enabling service-specific configurations.

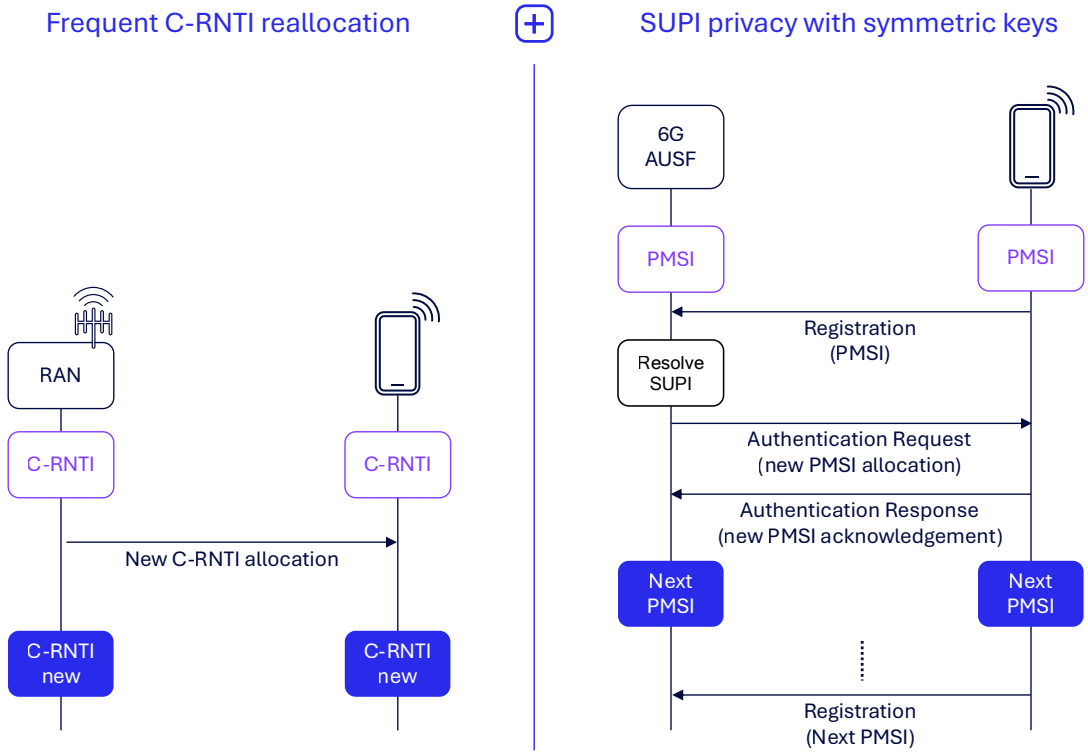

Figure 5. Enhance user identity privacy

Improve user identity privacy in the RAN

A key aspect of 6G security is keeping user identities private, which includes the **privacy of RAN temporary identities (RNTIs)**. In 5G networks, a cell-RNTI (C-RNTI) is assigned during the random access channel (RACH) procedure and updated during mobility events. However, long-lasting C-RNTIs (e.g., if the device remains connected at the same cell) can expose UEs to passive eavesdropping, revealing side-channel information such as the type of UE or active services through over-the-air traffic analysis. Additionally, targeted attacks may occur if a C-RNTI is linked to a UE's personal identifiers, like phone numbers or social media accounts.

To mitigate these risks, in addition to the strict reallocation of globally unique temporary identifiers (GUTI) and I-RNTIs for each connection introduced in 5G, we propose to support more frequent C-RNTI reallocations in 6G for connected UEs without necessitating a new RACH procedure. This is for enhancing privacy and reducing the likelihood of tracking and targeted attacks.

Also important to protecting user identity is maintaining the **privacy of subscription permanent identifiers (SUPI)**. In 5G, the subscription concealed identifier (SUCI) calculation relies on elliptic curve integrated encryption scheme (ECIES), which is expected to be replaced by post-quantum cryptography (PQC) in 6G. PQC algorithms, while promising, have large public key and cipher text sizes, resulting in substantial SUCI sizes. For example, a PQC algorithm such as Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) would result in 100s of additional bytes of overhead compared to ECIES used in 5G.

As we investigate the adoption of PQC algorithms for generating SUCI, a symmetric key-based approach for 6G that leverages USIM credentials could minimize SUCI size overhead. This method involves sending an encrypted private mobile subscription identity (PMSI) to the UE during the authentication and key agreement (AKA) procedure, with the UE using the PMSI in subsequent attach or registration processes, ensuring robust and efficient privacy protection.

Robust trust frameworks

Establishing a robust trust framework for 6G would facilitate a secure, resilient and adaptable network infrastructure, capable of withstanding modern cyber threats and ensuring the integrity and confidentiality of communications. In this section, we look at some key areas of focus at Qualcomm Technologies for achieving such a framework: isolated UE security contexts at each network function, zero trust architecture (ZTA) based on NIST tenets and robust security setup via message digest.

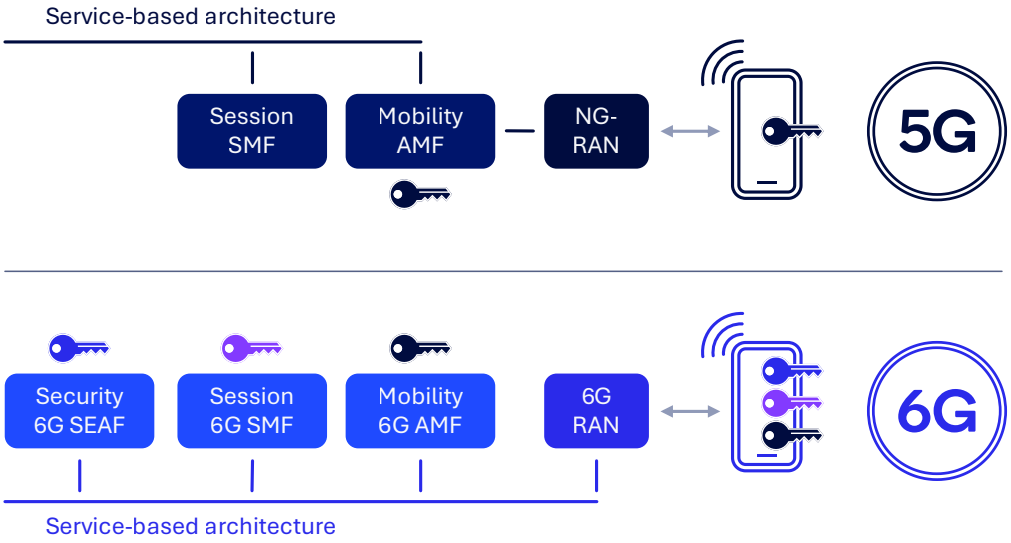

Figure 6. Isolate security contexts at each network function or service

5G NAS messages are securely exchanged between the UE and the AMF. However, the current architecture has a single NAS security termination point at the AMF, which presents limitations and potential threats. For instance, there is no generic secure communication channel between the home public land mobile network (HPLMN) and the UE when the UE is roaming, which necessitates the HPLMN relying on the visited public land mobile network (VPLMN) when delivering certain updates to the UE (e.g., UE policies). Additionally, there is no forward security with AMF relocation, meaning the source AMF knows the NAS key at the target AMF and beyond. Furthermore, the establishment of independent and isolated UE security contexts at different network functions such as the session management function (SMF) cannot be supported, resulting in a lack of end-to-end security support with the UE. Such limitations and threats are due to the 5G security anchor function (SEAF) being collocated with the AMF and only being used for initial AMF key derivation.

As with AS security supporting forward security, potential 6G NAS security enhancements include an independent 6G SEAF for supporting forward security in the AMF or, more generally, for network function relocation. Furthermore, a separate security anchor at the HPLMN would support secure communication between the UE and the HPLMN when roaming, providing a generic way for the HPLMN to configure roaming UEs and enhancing home network control. Introducing an independent SEAF can further facilitate end-to-end secure communication between the UE and various network functions.

Figure 7. Leverage the NIST zero trust tenets to build a robust trust framework

Implement zero trust architecture

Zero trust architecture (ZTA) is built on the NIST zero trust tenets. In the context of 5G, ZTA work by 3GPP is limited to the Core Network, while O-RAN's ZTA work focuses on the RAN. A gap analysis has been performed in 3GPP as well as in O-RAN Alliance, introducing some enhancements in the 5G system. For example, security event data and log collection, and exposure to a Security Information and Event Management (SIEM) system are being defined. Security evaluation and policy enforcement relies on proprietary solutions, which are out of the standard's scope.

For 6G, developing architecture and features toward enabling ZTA is important, with potential enhancements needed to meet NIST Tenet 5 and 6. This includes evaluating the security states of the 6G system and introducing new functional elements, such as a new network function (NF). A converged RAN-Core network architecture and a common architecture for 3GPP and O-RAN need to be considered for unified security management of the 6G system, keeping in mind that ZTA is an incremental and continuous process.

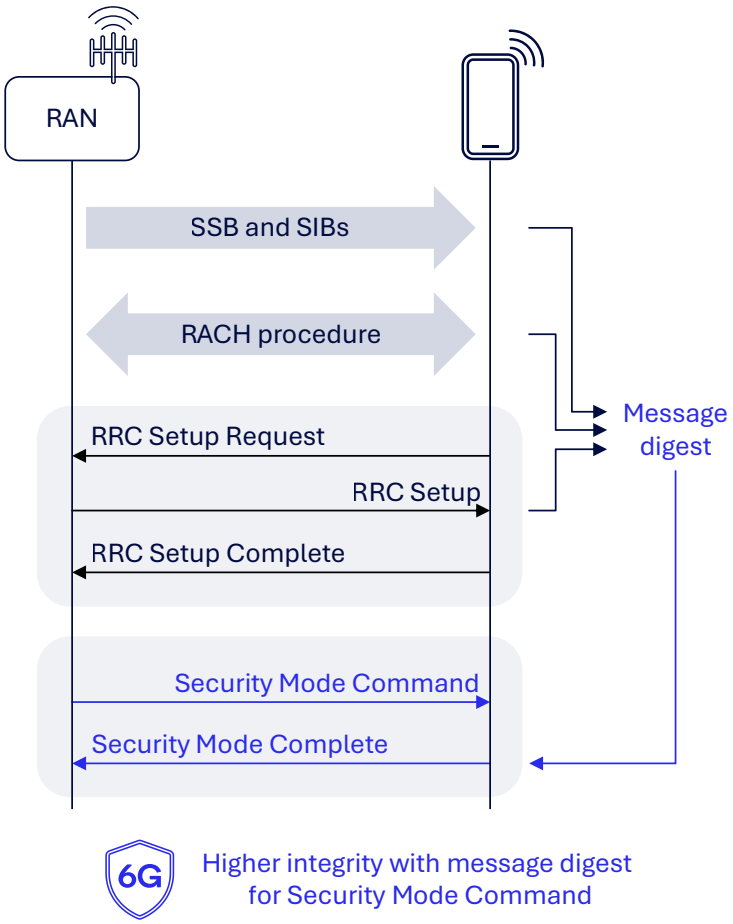

Figure 8. Ensure message integrity before activating access stratum security

Ensure robust security setup via message digest

In 5G AS security, common radio configurations and parameters, such as the master information block (MIB) and system information block (SIB), are not protected, potentially susceptible to false base station (FBS) attacks. The use of digitally signed system information has been discussed in the 3GPP as a possible solution. With the adoption of PQC algorithms, such signature will require thousands of bytes of additional overhead (e.g., at least 2420 bytes for module-lattice-based digital signature algorithm (ML-DSA)), and that compares poorly to current maximum SIB1 size being under 400 bytes. Apart from information broadcasts, RACH and RRC setup messages exchanged prior to the security mode command (SMC) are also not protected, leading to potential risks. Manipulation of message contents before the SMC can result in the UE being misconfigured, and adversaries can relay traffic without being detected by the UE or RAN, making the system susceptible to man-in-the-middle attacks.

To enhance 6G AS, we propose including a message digest computed from the messages exchanged in the SMC, similar to how TLS computes a transcript hash as described in RFC 8446 section 4.4.1. Upon detecting an error, the system can determine whether to continue or release the connection, thereby improving the overall security and integrity of the communication process.

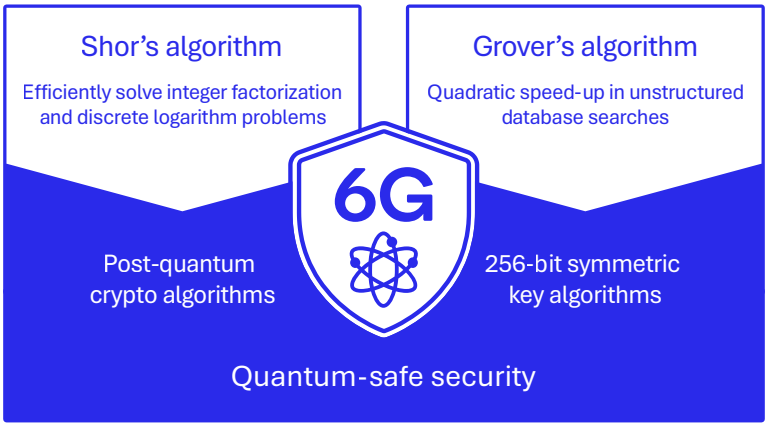

Figure 9. Ensure communication security as quantum technology advances

Quantum-safe security

As quantum technology progresses, traditional public key algorithms relying on the computational hardness of certain algorithms, such as integer factorization and discrete logarithm problems, face increasing threats. In particular, Shor's algorithm, which efficiently solves integer factorization and discrete logarithm problems, necessitates the development of PQC algorithms. NIST is currently standardizing these algorithms, ensuring security readiness for the Quantum era. Additionally, quantum properties enable a quadratic speed-up in unstructured database searches, posing risks to symmetric key algorithms. To counter this threat, 256-bit symmetric key algorithms like AES-256, SNOW5G, and ZUC-256 are essential for 3GPP air interface security, along with Authenticated Encryption with Additional Data (AEAD). As we move toward 6G, resilience against quantum attacks gains importance, requiring the adoption of PQC and 256-bit algorithms to safeguard communication security.

Making connectivity synonymous with security and trust

Advancements in connectivity, compute and AI bring unprecedented opportunities, but they also demand robust security measures to protect our digital future. At Qualcomm Technologies, our vision is to create a secure, adaptable and trustworthy mobile ecosystem that meets today's challenges and is prepared for tomorrow's threats. By addressing opportunities across the 6G radio access stratum and the RAN protocol stack, we are laying the groundwork for a resilient and secure future.

Join us as we help shape the next decade of mobile connectivity with 6G. Stay tuned for more updates from the 6G Foundry.

References:

1. Forward security protects the connection at the handover target RAN node against compromises of keys at the source RAN node.

2 Backward security prevents the target RAN node from accessing the key used at the source RAN node after handover.

Qualcomm

Follow us on:

For more information, visit us at: qualcomm.com

Learn more and get the latest updates:

Read more technology perspectives from the 6G foundry ↗

Sign up for our wireless technology newsletter ↗