APEX STANDARDS

Quantum-Resilient Telecommunications: The Shift to PQC and 6G Standards

Quantum computing is revolutionizing telecommunications, leading to a necessary shift towards Post-Quantum Cryptography (PQC) for the security of 6G Radio Access Network (RAN) and User Equipment (UE). In this transition, key standardization bodies such as 3GPP, ITU-T, GSMA, and ETSI are leading the efforts, each contributing to the development of a quantum-resilient future.

Quantum computers threaten to undermine existing asymmetric cryptographic standards, posing a significant risk to the emerging 6G network's security infrastructure. Traditional encryption methods, like RSA and ECC, rely on the computational difficulty of problems such as integer factorization or elliptic curve logarithms, which are currently secure against classical computing attacks. However, quantum computers, with their ability to process information in a fundamentally different way, can solve these problems much faster. For instance, Shor's algorithm, a quantum algorithm, can factorize large numbers exponentially faster than the best-known classical algorithms, rendering current public-key cryptography vulnerable. This vulnerability is particularly concerning for 5G and 6G networks, which are the backbone of critical infrastructure and a myriad of IoT devices. These networks rely heavily on encryption for secure communication, meaning that a quantum breakthrough could compromise everything from individual privacy to national security.

This risk necessitates the transition to PQC to maintain the integrity and confidentiality of communications across the network. In response, the U.S.' National Institute of Standards and Technology (NIST) has been proactive in developing Federal Information Processing Standards—FIPS 203, 204, and 205—to focus on quantum-resistant key establishment and digital signature schemes. These efforts are complemented by 3GPP and ITU-T SG11, which are instrumental in setting standards and recommendations to ensure the resilience against quantum threats.

The GSMA's Post Quantum Telco Network (PQTN) Task Force is assessing the impact of PQC on the telecommunications industry and outlining strategies for a transition to quantum-resistant practices. Similarly, ETSI Cyber and the U.K,'s National Cyber Security Centre (NCSC) are revising security standards and guidelines to adapt to the demands of the quantum computing era. The industry is therefore poised to adopt PQC algorithms, a transition that necessitates joint efforts from standardization bodies, governments, and the telecommunications sector. This includes collaborative R&D initiatives, an emphasis on both education and training, and strategic planning to address challenges such as overhauling existing Public Key Infrastructure (PKI) architectures and managing legacy systems.

In the U.S., NIST has launched a detailed PQC roadmap to guide this transition, calling on organizations to methodically catalog their cryptographic systems and report their findings annually to the Office of the National Cyber Director (ONCD) and the Cybersecurity and Infrastructure Security Agency (CISA) until the year 2035. The PQC standardization efforts orchestrated by NIST, which began with a competitive selection process initiated in 2016, are key to the selection of consensus-based PQC algorithms. These efforts are expected to culminate in the publication of the first PQC standards in 2024, setting a precedent for a secure shift to quantum-resistant cryptographic methods. To assist organizations in this transition, NIST also publishes whitepapers, playbooks, and demonstrable implementations, in addition to encouraging public testing of the pre-standardized PQC algorithms.

The Security Algorithms Group of Experts (SAGE), under the ETSI Special Committee (SC), chaired by Patrik Ekdahl from Ericsson, is tasked with specifying cryptographic algorithms essential for telecommunications standards. The group's primary focus has been on developing 256-bit algorithms for 5G, aimed to counter potential quantum computing threats. These algorithms are designed for both user plane and control plane traffic for 3GPP SA3's review. SAGE also proposes new authentication and key agreement (AKA) algorithms based on 256-bit primary secrets.

Before the industry moves forward to PQC, an intermediate step is the development of quantum-safe standards and the deployment of "hybrid" cryptographic schemes. These schemes are multi-algorithmic in nature, encompassing a mix of traditional and post-quantum algorithms to fulfill the same cryptographic purpose. Examples include Hybrid Key Encapsulation Mechanisms (KEM) and Hybrid Public Key Encryption (PKE) schemes, where each combines at least one post-quantum and one traditional algorithm. This approach offers a pragmatic and balanced path to enhance security, while maintaining compatibility with existing systems. Such hybrid strategies provide cryptographic agility, enabling organizations to adapt to evolving threats and manage the complexities of the changing cryptographic landscape. This dual-algorithm approach effectively mitigates risks associated with quantum computing and ensures ongoing security and interoperability in digital communications.

Collaboration in standardizing quantum-safe schemes is crucial for their global adoption and the establishment of consistent security protocols. Exploring these schemes in real-world scenarios will deepen our understanding of their practical capabilities and limitations. At present, there is no immediate requirement to alter symmetric cryptographic structures since quantum attacks are still largely theoretical and of academic interest. SAGE deems the existing 128-bit security robust against quantum threats, yet it recognizes that advancements in classical computing might eventually require upgrading to 256-bit algorithms. Keeping abreast of emerging technologies will be essential for future readiness. The prevailing wisdom advocates for maintaining effective security while minimizing disruptions to current systems, recommending a balanced approach in adapting to the evolving quantum computing technologies.

Preparing the telecom industry for a quantum-resistant future involves a comprehensive reevaluation and redesign of security systems, including the transition to 6G. This effort balances factors such as cost and complexity to ensure the industry will withstand the challenges posed by quantum computing.

Configuration	DNsF signing algorithm	gNB signing algorithm	Features		
			Quantum resistant	Message size to distribute the short-term certificate	Do short-term certificate and/or signature fit in a single SIB?
#1	ECDSA	ECDSA	No	Short: ECDSA signature using DSnF's ECDSA private key on a short-term gNB ECDSA public-key	Yes
#2	ECDSA	Hash Chain-based	No	Short: ECDSA signature using DSnF's ECDSA private key on the new gNB's hash chain anchor.	Yes
#3	Rainbow	Rainbow	Yes	Long: Rainbow signature using DSnF's rainbow private key on a short-term gNB's rainbow public-key (long)	No: 1) the signature fits; 2) the short-term certificate does not fit in a single SIB.
#4	Rainbow	Hash Chain-based	Yes	Short: Rainbow signature using DSnF's Rainbow private key on the new gNB's hash chain anchor.	Yes
#5	Falcon	Falcon	Yes	Medium: Falcon signature using DSnF's Falcon private key on a short-term gNB Falcon public-key	No: 1) a signature generated by the gNB does not fit in a SIB; 2) the short-term certificate does not fit in a single SIB.
#6	Falcon	Hash Chain-based	Yes	Medium-short: Falcon signature using DSnF's Falcon private key on the new gNB's hash chain anchor.	No: 1) only the signature fits; 2) the short-term certificate does not fit in a single SIB.

Table 6.20.3.14-1, derived from TDoc S3-234163, details a Change Request (CR) for updating "TR 33.809: Study on 5G security enhancements against False Base Stations (FBS)." This CR, initially reviewed and agreed upon at the S3-112 working group meeting in Gothenburg in August 2023, received approval during the SP-101 Plenary meeting, as documented in TDoc SP-230890 in Bangalore, India, the following month. The table presents various digital signing algorithm configurations in telecommunications, focusing on the challenge of achieving quantum resistance without sacrificing performance. Traditional algorithms, such as ECDSA in configurations #1 and #2, are currently efficient in terms of message size, accommodating short-term certificates in a single System Information Block (SIB). However, their lack of quantum resistance poses a security risk with the advancement of quantum computing. The move towards quantum-resistant algorithms like Rainbow and Falcon, in configurations #3 to #6, counters quantum threats but introduces performance challenges, notably the increased message size that surpasses a single SIB's capacity. This could necessitate the use of additional SIBs or a redesign of system information messaging, potentially affecting network throughput and latency. In particular, the Rainbow algorithm, with its extended signature sizes, and the Falcon algorithm, featuring medium-length signatures, struggle to fit both the signature and short-term certificate within the confines of existing network protocols. These security and performance trade-offs highlight the need for further research and development in post-quantum cryptography. This is essential to ensure that future network generations can sustain current performance levels while providing strong security against quantum computing threats. These factors gain increased significance, demanding a delicate balance between implementing advanced security measures and maintaining the efficiency of high-speed telecommunication networks.