Session #4: Security & Privacy

17 July 2024

Post Quantum Cryptography (PQC), a must for 6G Networks

by

Prashant Chugh, C-DOT

An Overview of PQC and Standardization

- PQC refers to a new type of Cryptographic algorithms that are being designed to withstand potential security threat to conventional cryptography from advancement in Quantum Computers
- NIST started a PQC standardization process in 2016 through an open "Call for Proposals" and subsequent to three rounds of rigorous public evaluation has released 3 Draft PQC standards in Aug 2023. **Final PQC standards are expected from NIST any time now.**

Summary of Draft NIST PQC Standards			
Standard Number	**Standard Name**	**Based-on 3rd Round Short-listing**	**Usage**
FIPS 203	Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)	CRYSTALS-KYBER	Key-Exchange
FIPS 204	Module-Lattice-Based Digital Signature Standard (ML-DSA)	CRYSTALS-DILITHIUM	Digital Signatures
FIPS 205	Stateless Hash-Based Digital Signature Standard (SLH-DSA)	SPHINCS	Digital Signatures

National & Global Efforts towards PQC Migration

- United States has come out with a National Security Memorandum to prioritize transition to PQC and migrate by 2035
- Many countries such as UK, Germany, Australia have come up with guidance for PQC Migration
- Most countries plan to follow NIST final PQC standards
- ETSI has released recommendations for migration to PQC. It advocates hybrid classical/PQC key-exchange and certificates.
- IETF has come out up with draft RFCs of TLS as well as IPSec with hybrid Classical/PQC approach
- In India, TEC has constituted a WG for Preparation of guidelines/ report on Migration to PQC and the subject has been discussed by various speakers in the previous two Annual Quantum Conclave co-organized by C-DOT, TEC and TSDSI

Are Mobile Telephony Systems used today Quantum-safe?

All **public** Telephony systems, including all public Cellular/ Mobile Telephony Systems, being used today anywhere in the world, including 4G, 5G and 5G-Advanced systems are Quantum vulnerable

- 3GPP released TR 33.841 in March 2019 on “Study on the support of 256-bit algorithms for 5G” in which it analyzed Threats of Quantum Computing to 5G. It decided to study this subject further after release of NIST PQC standards
- TSDSI released a TR on “Study of PQC for Future 5G Networks and Application Verticals” in March 2023. This report analyzed the Quantum Threat to various Security Algorithms used in 5G Architecture
- A number of Quantum vulnerabilities in the algorithms used for Confidentiality, Integrity & Authentication in 5G Architecture have been brought out in both the above TR. The cryptographic algorithms underlying IPSec & TLS used extensively in 5G architecture are Quantum vulnerable.

GSMA Task Force on PQC

- GSMA formed a Post Quantum Telco Network (PQTN) Task Force in Sep 2022 with the objective to support roadmap for PQC and its adoption across global telecommunications supply chain
- It has released Whitepaper on "PQC Guidelines for Telecom Use-cases" in Feb 2024 which *identifies initial set of telco use-cases impacted by PQC*

Summary of telco use cases impacted by PQC as per GSMA Whitepaper
• IP Traffic between RAN and Core Network in 4G/5G Networks
• Authentication of all VNFs (such as Mobile core, IMS, SD-WAN) on cloud or NFV infrastructure
• Signing algorithms used in all firmware updates
• VPNs used for managing all telecom devices or updating firmware
• Transfer of Data (Root key) between Mobile Network Operator & SIM vendor as part of physical SIM configuration
• Remote e-SIM provisioning for all IoT/M2M, Consumer Electronics & Mobile Phones

Why PQC is a must for 6G Networks

- As per 3GPP and ITU roadmap on 6G standards, first commercial 6G deployments are expected to start in Year 2030. Hence, Cryptographically Relevant Quantum Computers (CRQCs) shall for sure be a reality in lifetime of 6G Systems.
- Advancements in 6G will lead to proliferation of many additional use-cases that mandate PQC, such as:
  - *Real-time High-precision Surgery as a result of Hyper Reliable & Low Latency Communication (HRLLC) being conceived in 6G*
  - *Autonomous vehicles and V2X Communication*
  - *Massive Machine Type Critical industrial use-case scenarios*
- 6G's focus on Integrated AI & Communication and Integrated Sensing & Communication is expected to lead to 6G carrying a lot of Private Data related to Health & Finance,
- Privacy regulations such as GDPR (Europe), DPDP (India), HIPPA(Health Sector, USA), PCI-DSS (Payment card industry) already have provision for huge fines in case of leakage of Private Data. Such regulations are expected to increase worldwide in many other countries by 2030

Conclusion:

- **PQC is a must for 6G Networks**
- **6G Security & Privacy Design needs to include PQC from the beginning**

Thank You

Prashant Chugh, C-DOT, New Delhi

Email: prashant@cdot.in