Universidade Federal de Campina Grande
Electrical Engineering Department

Session 5: Breakthrough Technologies Enabling 6G including Useable Security and Privacy

Post-Quantum Criptography

Edmar Candeia Gurjão

ecg@dee.ufcg.edu.br

Motivation for Post-Quantum Cryptography

- Shor's Algorithm (1994): Polynomial-time factorization and discrete logarithms – breaks RSA, DSA, ECC.
- Grover's Algorithm: Quadratic speed-up in brute-force search – weakens symmetric-key systems and hash functions.

- **Implication**: TLS, VPNs, Blockchain, and digital signatures are at risk once scalable quantum computers become practical.

Why We Need Post-Quantum Cryptography

- Long-term confidentiality: sensitive data (medical, financial, governmental) must remain secure for decades.
- Harvest-now, decrypt-later attacks: adversaries store encrypted traffic now and decrypt it once quantum computers exist.
- Telecommunication systems, including 5G/6G authentication, IoT device identity, and secure key exchange, must adapt.
- Regulatory push: NIST PQC standardization (Kyber, Dilithium, Falcon).

Families of Post-Quantum Schemes

- Lattice-based: CRYSTALS-Kyber (KEM), Dilithium (Signature).
- Code-based: Classic McEliece (KEM).
- Hash-based: SPHINCS+ (Signature).
- Multivariate-quadratic: Rainbow (deprecated).
- Isogeny-based: SIKE (broken 2022, but research continues).

Applications in Telecommunications

- 5G Authentication and Key Agreement (AKA): Replace ECC with lattice-based KEMs.
- IoT devices: lightweight PQC algorithms for constrained environments.
- VPN & TLS for telecom backbones: transition from RSA/ECC to NIST PQC schemes.
- Satellite communication: secure command/control links with PQC-resistant signatures.

Recent NIST PQC Updates

UFCG

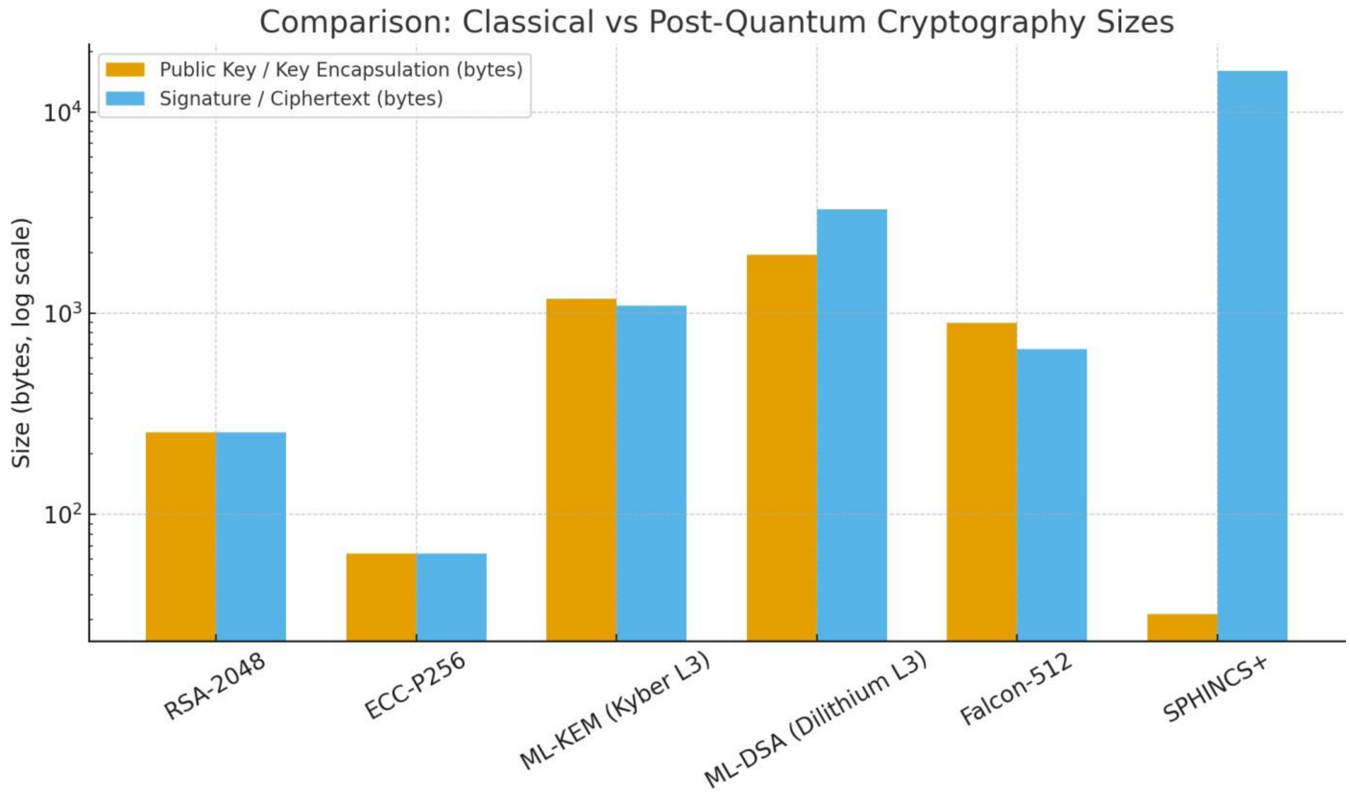
SUPRA OMNES LUX LUCIS

- FIPS 203: ML-KEM (Kyber) – Key Encapsulation Mechanism.
- FIPS 204: ML-DSA (Dilithium) – Digital Signature Algorithm.
- FIPS 205: SLH-DSA (SPHINCS+) – Hash-based Signature (backup scheme).
- Falcon: compact signatures – candidate for future standardization.
- HQC: code-based KEM selected as backup (2025).

Performance Trade-offs

- ML-KEM (Kyber): Public keys ~800–1568 bytes, ciphertext ~768–1568 bytes.
- ML-DSA (Dilithium): Signatures ~2.4–4.6 KB, public keys ~1.3–2.6 KB.
- Falcon: More compact signatures (~666–1280 bytes).
- SLH-DSA (SPHINCS+): Very large signatures (7–49 KB).
- Implications: bandwidth, latency, storage impact in telecom infrastructure.

Classical vs Post-Quantum Key and Signature Sizes



How to implement in the actual systems?

Thank you!

Edmar Candeia Gurjão
ecg@dee.ufcg.edu.br
ecandeia.dee.ufcg.edu.br
+55 83 98894 1403

Laboratório de Processamento de Sinais e Informação

LabMet