Post-Quantum Cryptography (PQC) for Cooperative ITS: ready for transition?

Brigitte Lonc

Boosting Digital Transformation

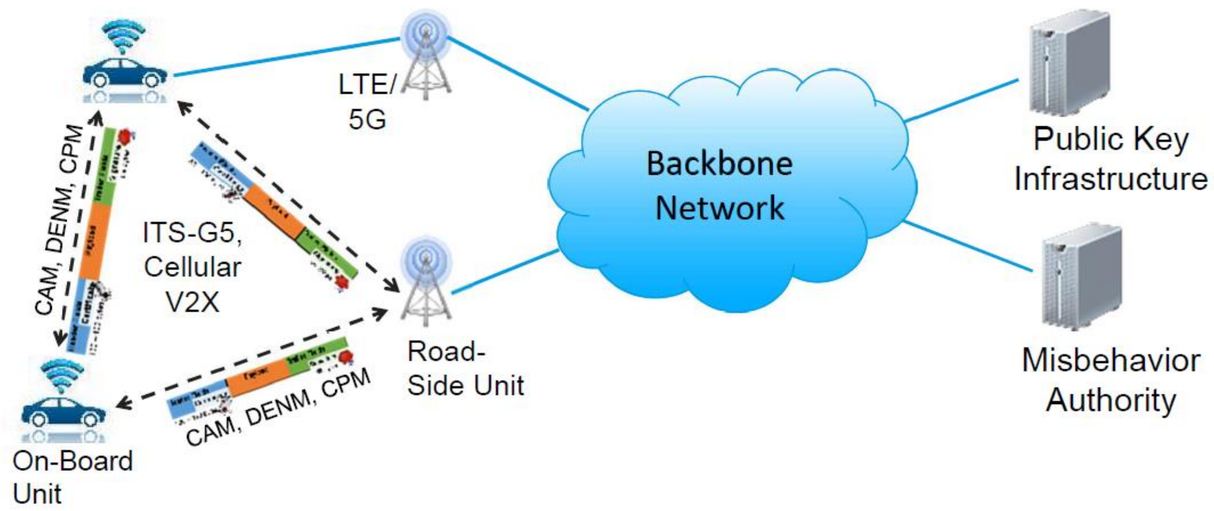
ETSI Security Conference, 16-19 October 2023

Post-Quantum Cryptography (PQC) for Cooperative ITS: ready for transition?

Quantum Computing threats to C-ITS

When a cryptographically-relevant Quantum Computer becomes available, classical asymmetric crypto standards might be broken:

- Used crypto not quantum-safe.
- No more trust in PKI



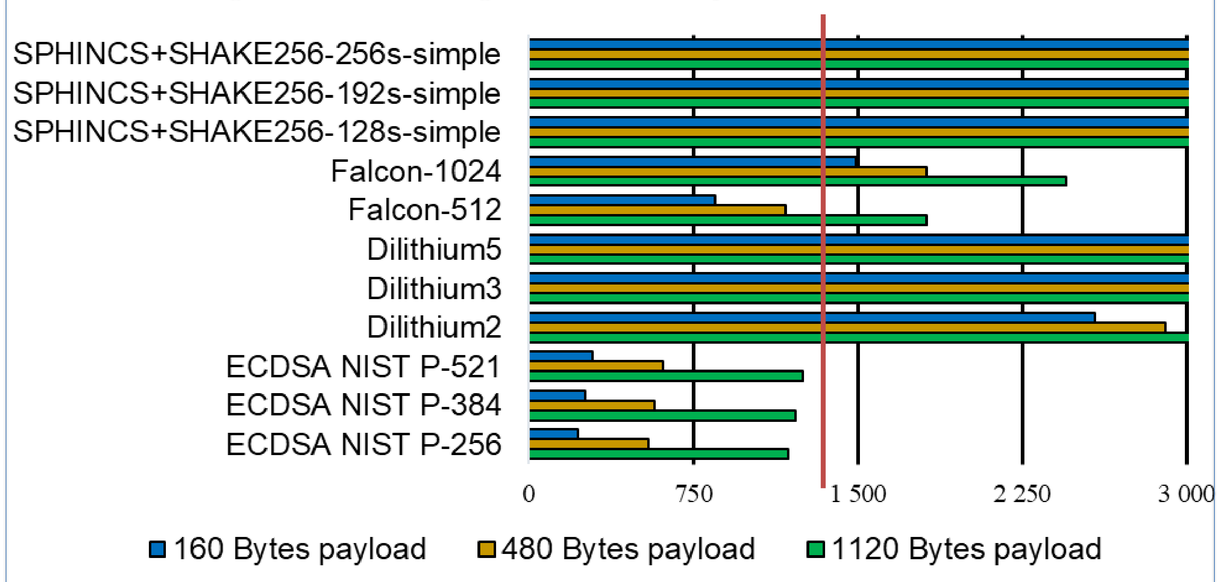
PQC Benchmark goal

Assess whether PQC algorithms can be used on common hardware without impacting C-ITS standards

Benchmark set-up and results

4 platforms representing low end/high end OBU, RSU, PKI server + Supercop (version 2022-05-06 round3)

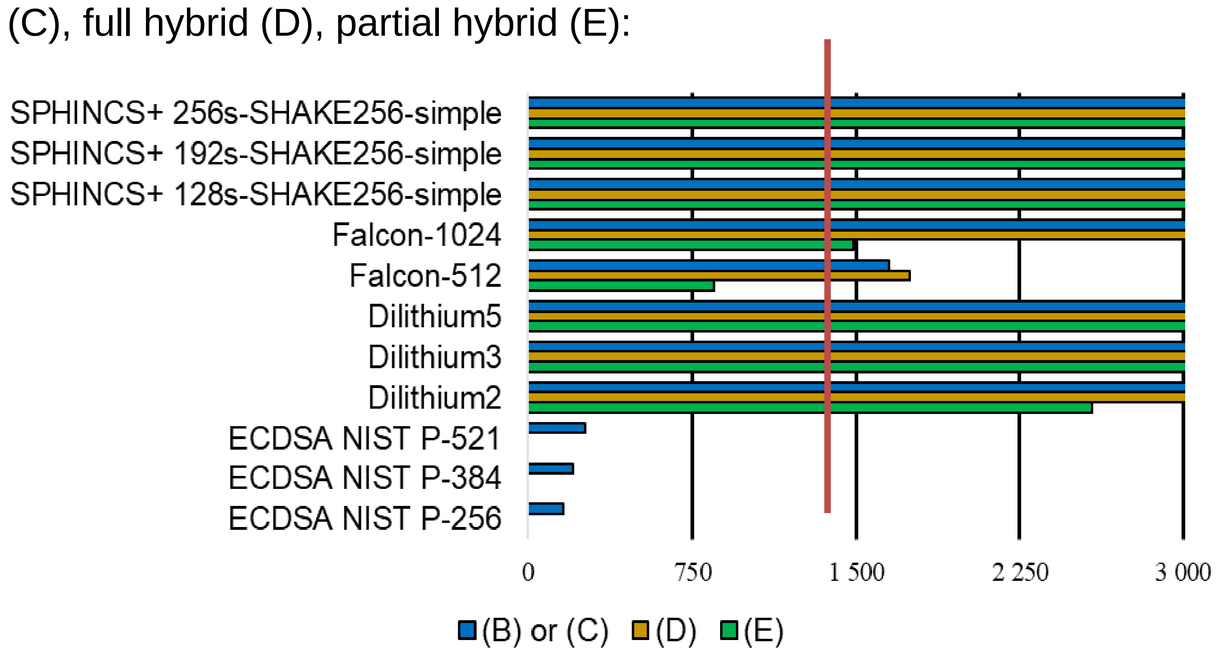
1. Signed message size in Bytes



Must fit the size limit for messages (1400 Bytes), no fragmentation

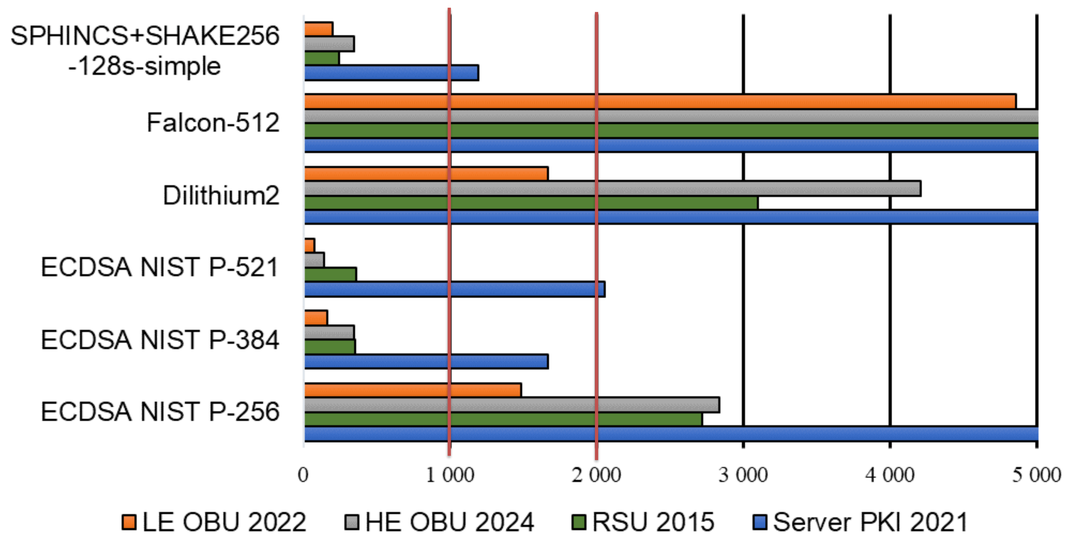
2. AT certificate size in Bytes

comparison of different certificate formats: classical (B), PQC (C), full hybrid (D), partial hybrid (E):



Authorization Ticket (pseudonymous certificate) must be transmitted in a basic CAM every second

3. Verification operations per second (1109 Bytes)



Must reach NIST Security level 1. At least 1000 verifications per second,

Signature time shall be less than 5ms

Conclusion/ perspectives

- ECDSA/Falcon selected for hybrid signatures (backward compatible + best tradeoff bandwidth, performance & security)
- KYBER meets our requirements for encrypted data
- 40 new candidates were submitted to NIST call for additional signature schemes. Some have smaller signature and public key size but verification performance seems to low in C-ITS context

Trusted Autonomous Mobility (TAM) project

This work has been supported by the French government under the "France 2030" program, as part of the SystemX Technological Research Institute within the TAM project

Partners: SystemX, Eviden, Oppida, Renault Group, Stellantis, Trialog, YoGoKo, Institut Mines-Télécom

Contact: Brigitte Lonc, brigitte.lonc@ext.irt-systemx.fr