Chaire ICMS PhD topic proposal

'**For a smooth transition to Quantum-Safe vehicles**'

Amira Barki (Ampère), Sébastien Canard (Télécom Paris)

1. The Quantum Threat and its impact on the Automotive domain

Vehicles are becoming increasingly connected (*e.g.* 5G, Wifi, Bluetooth, C-V2X, DSRC) to improve vehicle user experience (*e.g.* Virtual Key feature enabling to unlock the vehicle using user's smartphone, Firmware Over The Air (FOTA) updates providing the capability to remotely add new features for instance) and road users' safety (*e.g.* V2X connected services enabling to warn nearby drivers of potential hazards before they come into view).

Several security controls (*e.g.* TLS protocol and JWS tokens) put in place to ensure the security of these services and features rely on asymmetric cryptographic algorithms such as RSA, ECDSA and ECDH. These algorithms are threatened by the emerging Cryptographically Relevant Quantum Computers (CRQCs). Indeed, these computers would be able to leverage Shor's algorithm to efficiently solve hard problems upon which these algorithms rely on such as integer factorization and the discrete logarithm problems.

To cope with this emerging quantum threat, the NIST launched around a decade ago a first competition to select new cryptographic algorithms known as Post-Quantum Cryptographic (PQC) algorithms that remain secure against attacks by both classical and quantum computers. This competition has already enabled the standardization of 3 PQC algorithms, namely a post-quantum key establishment scheme ML-KEM [3] and two post-quantum digital signature schemes ML-DSA [4] and SLH-DSA [5]. Other algorithms have also been selected for standardization by either the NIST or the ISO, such as FrodoKEM, FALCON and HQC, whose standards are still under development.

Given the long lifecycle of vehicles (which is around 20 years) and NIST recommendations to disallow standard cryptographic algorithms by 2035 [1], there is an urgent need to start preparing the transition to quantum-safe algorithms while considering hybridation and crypto-agility aspects.

2. PhD Objectives

The purpose of this PhD is to address the issues related to the transition to quantum-safe connected vehicles by defining building blocks and solutions enabling a smooth transition for Automotive use cases.

One of the research topics to investigate includes the study of the different PKI architecture possibilities such as Mixed/Heterogeneous PKIs [6], Parallel PKIs, Hybrid PKIs using different certificate formats such as Catalyst extension, etc. and the proposal of a PKI architecture that is suitable for the automotive domain. A set of challenges needs to be considered when addressing this topic, namely ECUs diversity with ECUs having limited computational and storage resources.

Another topic of interest consists in designing a protocol enabling a smooth transition during vehicle serial life from classical cryptographic algorithms to the use of hybrid cryptography for the selected automotive use cases. When doing so, there is a need to identify the different steps that should be successfully performed before actual transition, and the appropriate sequencing to avoid any outage, without losing sight of the need for a good tradeoff between cybersecurity and potential performance and resources constraints. For instance, if we consider the TLS and FOTA use cases, one should at least take into account the need to (1) generate a new TLS key pair for the onboard Electronic Control Unit (ECU) and the Offboard platforms, and retrieve associated certificate, (2) replace ECU's Root CA by the new Root CA, (3) update/reconfigure the ECU/Offboard components to rely on hybrid cryptography for mutual TLS establishment and SW update image verification, etc.

PhD candidate may also investigate proposals to ensure quantum-resilience for use cases involving ECU(s) that cannot handle hybrid cryptography due to either resources constraints or specific constraints related to legacy vehicle architectures.

The proposed protocol and solutions must be implemented on a test bench that is quite representative of the components involved in the selected automotive use case(s) for validation and performance impacts.

3. Working plan

The PhD candidate will start by studying relevant state of the art literature covering Post-Quantum Cryptographic algorithms, PKI architectures, etc. A study of the impacts of the transition to PQC on the automotive domain and the identification of the pre-requisite to ensure actual crypto-agility shall also be done.

Then, the candidate will begin investigating solutions for the considered research topics while continuing the techno watch on new research results that might be of interest for the targeted objectives.

4. References

[1] Moody, D., Perlner, R., Regenscheid, A., Robinson, A., Cooper, D., NIST Internal Report 8547 ipd, Transition to Post-Quantum Cryptography Standards, Initial Public Draft, November 2024, https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

[2] NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Part 1, V1.1, EU PQC Workstream, June 2025, Roadmap_on_postquantum_cryptography_PzBJxNUYyeuEdVUacWL696DofZQ_117507.pdf

[3] NIST, FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism Standard, August 2024, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[4] NIST, FIPS 204 – Module-Lattice-Based Digital Signature Standard, August 2024, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[5] NIST, FIPS 205 – Stateless Hash-Based Digital Signature Standard, August 2024, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf

[6] Paul, Sebastian and Kuzovkova, Yulia and Lahr, Norman and Niederhagen, Ruben, Mixed Certificate Chains for the Transition to Post-Quantum Authentication in TLS 1.3, ASIA CCS'22, https://dl.acm.org/doi/10.1145/3488932.3497755

[7] Alessandro Amadori, Thomas Attema, Maxime Bombar, João Diogo Duarte, Vincent Dunning, Simona Etinski, Daniël van Gent, Matthieu Lequesne, Ward van der Schoot, Marc Stevens and AIVD Cryptologists and Advisors, The PQC Migration Handbook, Guidelines for migrating to Post-Quantum Cryptography, 2nd edition, December 2024, TNO-2024-pqc-en.pdf

[8] Daniel J. Bernstein, Tanja Lange, Jonathan Levin and Bo-Yin Yang, PQConnect: Automated Post-Quantum End-to-End Tunnels, NDSS 2025, PQConnect: Automated Post-Quantum End-to-End Tunnels - NDSS Symposium