Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

Future generation Security for smart and connected Cars - FuSeCar

Deliverable D3.2: Post-quantum safety for current vehicular communication protocols and architectures

WP3: Post-quantum safety for current vehicular communication protocols and architectures

Authors:

Gianluca Dini[1]

gianluca.dini@unipi.it
[1]Dept. of Information Engineering
University of Pisa

Current revision: R2.0
Delivery date: 30th, August 2025

Revision history

Authors	Changes	Date	Revision
Gianluca Dini	Due version according to time plan	November 30th, 2024	R1.0
Gianluca Dini	Improved version encompassing publications 1	August 31th, 2025	R2.0

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

Contents

1 Introduction

The rapid evolution of connected and software-defined vehicles is reshaping the automotive domain into a highly dynamic, networked, and mobile cyber–physical system. Vehicles increasingly rely on continuous connectivity to edge, cloud, and backend infrastructures to enable advanced functionalities, lifecycle-long software maintenance, and rapid deployment of security patches. In this context, mobility is not limited to the physical movement of vehicles, but extends to the migration of services, data, and trust relationships across heterogeneous and distributed environments. Ensuring secure, seamless, and scalable operation under such conditions has become a central challenge for automotive systems engineering.

At the same time, the long operational lifetime of vehicles exposes automotive security mechanisms to the disruptive impact of quantum computing. Cryptographic primitives that are currently deployed to protect communication channels, software updates, and access control are expected to become vulnerable within the lifespan of vehicles produced today. This creates a pressing need to transition toward post-quantum cryptography while preserving performance, scalability, and deployability on resource-constrained embedded platforms. The automotive domain therefore represents a particularly demanding reference case for evaluating the practicality of post-quantum solutions in real-world, mobility-driven scenarios.

The three works considered in this context address complementary aspects of this problem space. Together, they investigate how post-quantum cryptography can be integrated across different layers of the automotive ecosystem, ranging from secure service continuity in mobile edge–cloud environments [1], to the protection of over-the-air software updates in terms of both authenticity and confidentiality [2, 3]. By focusing on concrete automotive use cases—such as edge proxy handovers, firmware distribution, and fine-grained access control—the studies collectively demonstrate that post-quantum security can be achieved without undermining the stringent performance and availability requirements imposed by vehicular mobility. Taken as a whole, they outline a coherent framework in which mobility-aware architectures and post-quantum cryptographic primitives jointly contribute to the long-term security and resilience of future automotive systems.

1.1 Fast and Secure Service Continuity in the Edge-Cloud Continuum: A Study of TLS 1.3 Resumption and Post-Quantum Key Exchange

This work investigates how strong, future-proof security mechanisms can be integrated into edge–cloud platforms without compromising service continuity and performance, a requirement that is increasingly critical in dynamic environments such as smart cities, smart transportation systems, smart and connected vehicles, logistics, and mobile IoT ecosystems. Building on a previously proposed proxy-based architecture for seamless service continuity, the authors extend the platform by incorporating advanced features of TLS 1.3 that address both emerging security threats and the stringent latency constraints inherent to mobility-driven edge computing scenarios.

The main contribution lies in the combined adoption of hybrid post-quantum key exchange and stateless TLS 1.3 session resumption within a distributed set of edge proxies. Hybrid key exchange based on X25519 and ML-KEM-768 is introduced to mitigate the Store Now Decrypt Later threat posed by future quantum adversaries, while maintaining backward compatibility and robustness against potential weaknesses in novel post-quantum schemes. In parallel, stateless session resumption using pre-shared keys is leveraged to significantly reduce the cost of repeated TLS handshakes during client mobility or load-driven proxy reassignment, which are common in edge–cloud continuums.

The work presents an open-source implementation relying on Envoy proxies and the BoringSSL library, enhanced to support post-quantum cryptographic primitives and cross-proxy session resumption through shared session ticket encryption keys. A comprehensive experimental evaluation is conducted on an emulated testbed under multiple network conditions representative of wired, cellular, and bandwidth-constrained environments.

The analysis considers cryptographic overhead, handshake message size, and end-to-end handshake duration, providing a detailed view of the trade-offs introduced by stronger security mechanisms.

The results demonstrate that hybrid post-quantum TLS introduces a noticeable but manageable increase in computational and data overhead, while offering substantially improved long-term security guarantees. More importantly, TLS 1.3 session resumption yields significant performance gains, reducing connection establishment costs by up to 73 percent and largely offsetting the overhead of post-quantum cryptography, especially in scenarios where network latency dominates. Overall, the study shows that it is feasible to deploy quantum-resilient cryptography in edge–cloud systems without undermining responsiveness or transparency at the application level.

The work concludes that the proposed enhancements make the service-continuity platform well suited for secure, mobility-driven edge computing deployments. It positions the work as a practical step toward quantum-ready edge infrastructures and outlines future directions, including the exploration of TLS 1.3 0-RTT and QUIC, as well as post-quantum authentication mechanisms, to further reduce latency and strengthen security in highly demanding smart-city environments.

The full paper is reported in Appendix A

1.2 On hardware acceleration of quantum-resistant FOTA systems in automotive

This work examines the impact of post-quantum cryptography on automotive Firmware Over-The-Air (FOTA) systems, with a specific focus on performance, scalability, and long-term security requirements in vehicles whose operational lifetime may extend for decades. Motivated by the growing threat posed by future large-scale quantum computers to classical digital signature schemes such as RSA and ECDSA, the study investigates how quantum-resistant signature algorithms can be realistically deployed in production-grade automotive environments while complying with emerging regulatory frameworks on cybersecurity and software updates.

The work concentrates on two lattice-based digital signature schemes standardized by NIST, namely CRYSTALS-Dilithium and Falcon, which are widely regarded as the most viable candidates for post-quantum authentication in embedded systems. Using an Uptane-compliant reference FOTA architecture, the authors perform an extensive experimental evaluation of signature generation, signature verification, and hashing operations on representative automotive hardware platforms, including microprocessor-based and microcontroller-based Electronic Control Units. The analysis highlights that, in realistic FOTA workflows, vehicles predominantly verify signatures rather than generate them, making verification performance more critical than signing performance from a system-level perspective.

A key finding of the study is that the choice between Dilithium and Falcon has only a limited effect on the overall execution time of FOTA procedures. Although Falcon generally offers faster signature verification and smaller signatures, the dominant performance bottleneck is shown to be the computation of cryptographic hashes over large firmware images, which may reach hundreds of megabytes or even gigabytes in modern vehicles. This observation holds across different security levels and hardware architectures and becomes particularly evident in complete update scenarios involving a large number of ECUs.

Based on this insight, the work argues that accelerating digital signature primitives alone is insufficient to achieve meaningful performance gains in automotive FOTA systems. Instead, the authors propose and design a dedicated hardware accelerator for the SHAKE hash function, which is a core component of both Dilithium and Falcon as well as the SHA-3 family standardized by NIST. The accelerator is implemented on FPGA and integrated into multiple ECU-class architectures. Experimental results demonstrate that hardware acceleration of SHAKE yields substantial speedups in hash computation, reaching up to two orders of magnitude on resource-constrained microcontrollers, and significantly reduces the overall duration of FOTA procedures in worst-case update scenarios.

The work concludes that hardware-assisted hashing is a crucial enabler for the practical adoption of post-

quantum cryptography in automotive software update mechanisms. By shifting the performance focus from signature algorithms to hash computation, the proposed approach makes quantum-resistant FOTA feasible without degrading user experience or operational availability. The results provide concrete guidance for automotive system designers and standardization bodies, and they position SHAKE hardware acceleration as a strategic building block for future quantum-resilient vehicular security architectures.

The full paper is reported in Appendix B

1.3 On Post-Quantum Attribute-Based Encryption for Automotive Over-the-Air Soft-ware Updates

This work investigates the feasibility of using post-quantum Attribute-Based Encryption (ABE) to protect the confidentiality of automotive over-the-air (OTA) software updates in the presence of future quantum adversaries. While existing OTA security solutions primarily emphasize authenticity and integrity, confidentiality is often treated as secondary and typically enforced through traditional asymmetric encryption or secure transport protocols. These approaches either scale poorly or leave software updates exposed when stored on semi-trusted infrastructure, such as cloud servers or in-vehicle gateways. The authors argue that this exposure is particularly problematic for protecting manufacturers' intellectual property and motivates the adoption of more flexible cryptographic mechanisms.

The work focuses on Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which enables fine-grained access control by embedding access policies directly into ciphertexts. In contrast to conventional public-key encryption, CP-ABE allows a single encrypted update to be selectively decryptable only by vehicles whose attributes satisfy a specified policy, thereby eliminating the need to encrypt updates individually for each vehicle. However, most CP-ABE schemes rely on pairing-based cryptography, which is vulnerable to quantum attacks. To address this limitation, the work evaluates a CP-ABE scheme based on the Ring Learning with Errors (RLWE) problem, a lattice-based primitive widely regarded as quantum-resistant.

The authors implement the RLWE-based CP-ABE scheme proposed by Gür et al. and integrate it into an automotive OTA update scenario that includes an OEM, a cloud repository, and in-vehicle components such as a gateway and a dedicated Update and Configuration Manager (UCM). The system and adversary model assumes that cloud servers and gateways are honest-but-curious, making confidentiality at rest and in transit a primary concern. To efficiently handle large software updates, the solution adopts a digital envelope approach in which CP-ABE is used to encrypt a symmetric key, while the bulk update payload is encrypted with symmetric cryptography.

An experimental evaluation is conducted on an embedded platform representative of automotive environments, focusing on decryption time and memory requirements on the vehicle side. Results show that CP-ABE decryption introduces a fixed and moderate overhead that is independent of the update size, while symmetric decryption dominates for larger payloads. Memory consumption for secret keys and ciphertexts, although non-negligible, remains within the capabilities of realistic in-vehicle hardware. Importantly, the relative overhead of the CP-ABE component rapidly decreases as update sizes grow, making it negligible for typical automotive updates in the order of tens or hundreds of megabytes.

The work concludes that post-quantum CP-ABE based on RLWE is a practical and effective solution for ensuring the confidentiality of automotive OTA updates. The proposed approach provides strong quantum-resistant security guarantees, scalable access control, and acceptable computational and storage overhead on embedded automotive platforms. These results support the viability of integrating post-quantum ABE into future OTA frameworks as a complement to existing mechanisms for authenticity and integrity, contributing to a comprehensive and long-term secure software update ecosystem for connected vehicles.

The full paper is reported in Appendix C

A Fast and Secure Service Continuity in the Edge-Cloud Continuum: A Study of TLS 1.3 Resumption and Post-Quantum Key Exchange

B On hardware acceleration of quantum-resistant FOTA systems in automotive

C On Post-Quantum Attribute-Based Encryption for Automotive Over-the-Air Software Updates

References

[1] Lorenzo Catoni, Carlo Puliafito, and Gianluca Dini. Fast and secure service continuity in the edge-cloud continuum: A study of tls 1.3 resumption and post-quantum key exchange. In *2025 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 396–401. IEEE, 2025.

[2] Gianluca Dini, Salvatore Lombardi, and Tommaso Antonini. On Post-Quantum Attribute-Based Encryption for Automotive Over-the-Air Software Updates. In *2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design (IOLTS)*, pages 1–4. IEEE, 2025.

[3] Pericle Perazzo, Stefano Di Matteo, Gianluca Dini, and Sergio Saponara. On hardware acceleration of quantum-resistant FOTA systems in automotive. *Computers and Electrical Engineering*, 118:109327, 2024.