



Post-quantum Cryptography for Connected and Cooperative Automated Mobility: A Comprehensive Overview

Mohamed Saied Mohamed¹(✉), Julie Godard², Victor Jimenez³, Adrien Jousse², Pau Perea Paños³, and Miao Zhang¹

¹ FEV.Io GmbH, Neuenhofstraße 188, 52078 Aachen, Germany
mohamed_m@fev.io

² CEA, LIST, Communicating Systems Laboratory, Gif-sur-Yvette, France

³ Technology Centre of Catalonia, Unit of IT&OT Security, Eurecat, Barcelona, Spain

Abstract. Connected and Cooperative Automated Mobility (CCAM) applications, instrumental in enhancing vehicle communication with infrastructure and the cloud, face cybersecurity vulnerabilities due to their intricate components requiring multifaceted cryptographic validation. With quantum computing advancements, traditional public key cryptography becomes susceptible, emphasizing the need for quantum-resistant algorithms to assure long-term automotive cybersecurity. Although Post-Quantum Cryptography (PQC), which provides solutions to counter this quantum risk is still under research, several algorithms have emerged and are under standardization. This paper provides a comprehensive overview of the status of PQC in automotive applications, including a performance analysis of selected algorithms in this research. Further, it presents some potential use cases of PQC (such as Secure Over-The-Air (SOTA) software update and Vehicle to everything (V2X) communication). By relying on PQC, the automotive industry can stay ahead in securing connected vehicles against emerging quantum computer threats.

Keywords: Connected and Cooperative Automated Mobility (CCAM) · Post-Quantum Cryptography (PQC) · Automotive Cybersecurity · Long-Term Security

1 Introduction

Automotive and CCAM applications promise to revolutionize future transportation, making it safer, eco-friendlier, and more efficient. At its core, CCAM thrives on networks that intertwine vehicles (V2V), infrastructure (V2I), broader networks (V2N), and even pedestrians (V2P). Yet, the weaving of these networks casts shadows of data authenticity and privacy concerns. In the CCAM world, vehicles not only update software and relay information over networks but also utilize cameras for pedestrian detection, vehicle identification, and location broadcasting.

Consider the potential consequences if a malicious actor exploits shared vehicular information to track a target or even manipulate a vehicle's controls. What if compromised location data or corrupted software updates were broadcast? These scenarios are not just theories. To avoid such risks, we need to integrate sophisticated cybersecurity and data protection measures into CCAM designs. While these systems are designed to be secure for a time, they must be prepared for future threats such as the rise of quantum computing. When quantum computers gain enough power, our existing cryptographic solutions, such as RSA [11], will be broken [12]. This is particularly concerning in the context of CCAM, where there is a threat of a 'harvest now and break later' attack, potentially compromising sensitive information and cryptographic methods used in the CCAM ecosystem.

2 Long-Term Security

In the CCAM context, ensuring long-term security is of utmost importance. CCAM represents the integration of multiple advanced transportation systems: connected vehicles, automated vehicles, connected infrastructures and their cooperative operations. Vehicles are designed for 10–15 years, automotive infrastructures even more. Given the nature of these systems and their applications, long-term security is not just a luxury but a necessity. The following Table 1 lists several scenarios and reasons that highlight the need for long-term CCAM security.

Quantum computers present significant challenges to existing cryptographic practices in automotive vehicles. Current vehicles rely on public key cryptography for secure updates, both through cables and wirelessly. While these methods ensure integrity and authenticity, they're at risk from quantum advancements. The RSA encryption, which hinges on the difficulty of factoring large numbers, can be swiftly dealt with by quantum capabilities using Shor's algorithm. Furthermore, symmetric encryption isn't entirely safe, with Grover's search algorithm posing potential threats. Given that vehicles frequently share data with entities like manufacturers and insurance agencies, there's an urgent need to turn to post-quantum cryptography to protect updates and preserve data privacy.

Mosca's theorem helps calculate the quantum threat's arrival, weighing the duration of desired data security against the time required for quantum-safe transition. Given a typical vehicle's 10–15 years lifespan and NIST's aim to standardize post-quantum algorithms by 2024 [10], the race is on. Of all quantum defense strategies, PQC emerges as the frontrunner.

Table 1. Long-term security scenarios for CCAM applications.

Scenario	Description	Cause
Vehicle Lifecycle Duration	Vehicles have a long lifecycle (typically 10–20 years or more)	Cryptographic methods that were considered secure at the time of manufacture may become vulnerable. This disparity between the rapid evolution of cryptographic threats and the long lifespan of vehicles necessitates long-term security measures
Future Interoperability	Vehicles from different manufacturing years will need to interact	Ensuring that older vehicles can securely communicate with newer ones requires forward-compatible security solutions
Over-the-Air (OTA) Updates	Vehicles increasingly rely on OTA updates for software patches	To counter vulnerabilities discovered long after a vehicle’s production, the OTA update mechanism itself must be secured for the long term
Vehicle-to-Everything (V2X) Interactions	Vehicles will interact with other vehicles and smart-city infrastructure devices	The diverse and continually evolving landscape of V2X interactions demands that security measures be future proofed to remain effective in the face of unforeseen challenges

3 Post-quantum Cryptography

In March 2022, ENISA proposed a hybrid approach for transitioning from our current cryptographic tools to post-quantum solutions [1]. This method merges the resilience of pre-quantum algorithms against classical attacks with the defenses post-quantum algorithms offer against quantum attacks. For key establishment, a Key Derivation Function (KDF) is used, while signatures utilize concatenation.

The first NIST’s post-quantum competition [10] categorized post-quantum algorithms into five groups:

- Lattice-based Cryptography: Ajtai introduced the SIS (Short Integer Solution) problem in 1996 as part of the first lattice-based cryptographic scheme [2]. Regev formulated the LWE (Learning With Errors) problem in 2005 [2], which was later adapted into the Module-LWE variant [2] for better performance. Separately, the NTRU cryptographic approach, aiming for more compact key sizes, was introduced in 1996 [2].

- Cryptography based on hash functions: The first person to use hash functions to sign documents was Merkle [2]. Later, Lamport [2] and Winternitz [2] showed how to convert Merkle's single signature scheme into a multiple signature scheme. Merkle also introduced a new scheme combining the Winternitz approach with binary trees called Merkle tree.
- Code-based cryptography: The McEliece encryption scheme [2] is first asymmetric method in this field. Its security relies on the difficulty of code-theoretic problems, such as the Syndrome Decoding (SD) problem. Subsequently, Niederreiter [2] proposed a digital signature scheme based on error-correcting codes. A significant drawback of many code-based cryptographic primitives is their large key size. That is why structured variants are developed to reduce key size.
- Multivariate cryptography: Multivariate cryptography is based on the difficulty of solving a system of nonlinear, usually quadratic, equations over a finite field [2]. Most signature schemes in this category are based on the complexity of the MQ problem, finding solutions to a system of multivariate quadratic equations.
- Cryptography based on isogenies of supersingular elliptic curves: This form of cryptography is based on the challenge of identifying isogenies between supersingular elliptic curves [2]. It's used to facilitate a Diffie-Hellman-type key exchange.

4 PQC in Automotive: State-of-the-Art and Applications

As vehicles become interconnected platforms, there is an urgent need for stronger cryptographic systems, especially considering quantum computing threats. As a result, the focus is turning towards PQC.

- Hermelink's et al. Introduced a PQC protocol designed for vehicle component communication. This protocol becomes the foundation for **V2X Communication**, ensuring quantum-secure exchanges with infrastructure [3].
- Lattice-based PQC has benefits, especially for **High-Performance Systems**. This approach ensures swift and secure communications, crucial during high-speed driving scenarios [4].
- Wang and Stöttinger emphasized the importance of **HSMs in Vehicles**. They proposed quantum-secure Hardware Secure Modules (HSM) to protect key vehicle functions, such as starting the ignition [5].
- For **OTA Software Updates**, Bos's et al. Suggested using CRYSTALS-Dilithium. This ensures updates remain quantum-secure, reducing the need for future recalls [7].
- Making vehicle **Boot Processes** quantum-safe is another priority. Using PQC, we can ensure the vehicle's software remains untampered each time it starts [8].
- Gonzalez et al. Highlighted **Signature Verification** methods. Their PQC techniques allow for fast validation, especially useful for devices like traffic cameras [9].
- **Vehicle-to-Vehicle Communication** is another focus. Research underscores the need for these communications to be both private and quantum-secure [6].

There's a noticeable increase in research on PQC for the automotive world, highlighting how crucial it is for the future of transportation. The industry is clearly preparing to tackle quantum challenges.

5 Performance of PQC in Automotive Systems

Kyber, Dilithium, and Falcon are lattice-based cryptographic methods rooted in 512–1024 dimensional mathematical problems, compete for NIST’s PQC standardization [10], with Kyber as a KEM and Dilithium and Falcon as digital signature algorithms. To compare these unique algorithms, NIST uses metrics like Key Length and Algorithm Strength, detailed in Table 2.

Table 2. Key Metrics for NIST’s PQC selected Algorithms [10].

Algorithm	NIST Level	Key & Signature/Ciphertext sizes (bytes)
Dilithium2	2	Secret: 2528, Public: 1312, Signature: 2420
Dilithium3	3	Secret: 4000, Public: 1952, Signature: 3293
Dilithium5	5	Secret: 4864, Public: 2592, Signature: 4595
Falcon-512	1	Secret: 1281, Public: 897, Signature: 666
Falcon-1024	5	Secret: 2305, Public: 1793, Signature: 1280

NIST Levels (1–5): Level 1 is the most vulnerable, easily broken in 8 h with a small investment, while Level 5 is the most secure, ensuring ciphertext doesn’t reveal plaintext.

In our evaluation of open Quantum Safe (OQS) metrics for connected vehicles, we simulated a road-element-to-vehicle interaction using a client/server model. Due to hardware constraints of the OQS library, two Raspberry Pi 4 with 4 CPU cores and 8 GB of RAM were utilized. The server, operating on port 4433, sent packets of varying sizes- 1 KB, 1 MB, and 30 MB- to reflect common communication sizes. We adopted the Kyber KEM for encapsulation and the Dilithium and Falcon algorithms for signatures, aligning with the latest NIST standards (Table 3).

Table 3. Latency from Client Request Launch to Packet Receipt (Seconds)

Packet weight: 1 KB		NIST Security Level		
		2	3	5
Dilithium	Kyber512	0.072	0.072	0.073
Falcon		0.092	N/A	0.095
Dilithium	Kyber1024	0.072	0.075	0.077
Falcon-		0.097	N/A	0.100

Using OQS’s OpenSSL 3.2-dev with TLS1.3, the Kyber KEM keys are dynamically generated for each communication and stored temporarily. We employed the Python tool psutil to gauge CPU and RAM performance, capturing data at **10-ms** intervals across 100 iterations for different algorithm/packet combinations. The results, presented in Table 4, provide an averaged view of CPU and RAM (MB) utilization over the process’s duration.

Table 4. Average CPU and RAM Utilization During Request Lifecycle (packet weight 1KB)

Algorithm	Kyber512				Kyber1024			
	Dilithium2	Dilithium2	falcon512	falcon1024	Dilithium2	Dilithium2	falcon512	falcon1024
CPU (%)	3.949	3.897	3.594	2.897	3.726	4.137	3.361	3.447
RAM	1.059	1.467	1.230	1.477	1.304	1.586	1.354	1.515

6 Conclusion and Recommendations

In the face of advancing quantum computing capabilities, current cryptographic practices within the automotive sector, especially in CCAM, stand vulnerable. Vehicles, now more interconnected than ever, demand the robust protection offered by PQC. Our investigation has shed light on the industry’s noticeable shift towards PQC strategies, which rely on a variety of mathematical foundations and algorithms. Particularly for processes like Vehicle-to-Vehicle Communication and OTA Software Updates, PQC offers enhanced defense against quantum threats. Practical tests, notably on Raspberry Pi 4, have showcased the effectiveness of specific post-quantum methods. Embracing PQC in CCAM not only bolsters security but also positions the transport sector for a quantum-resistant future, ensuring sustained safety and optimal functionality.

To ensure the seamless integration of PQC solutions into real CCAM and other critical automotive applications, it is important to develop lighter and faster PQC techniques. On the other hand, more suitable hardware tailored for post-quantum secure implementations should be developed, thus bridging the gap between theoretical ability and practical feasibility.

Acknowledgment. The research leading to these results has received funding from the European Union’s Horizon Europe programme under grant agreement No 101069748- SELFY project.

References

1. Bernstein, D.J., Hülsing, A., Lange, T.: Post-quantum cryptography, integration study. ENISA (2022)
2. Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.): Post Quantum Cryptography. Springer, Heidelberg (2009)
3. Hermelink, J., Pöppelmann, T., Stöttinger, M., Wang, Y., Wan, Y.: Quantum safe authenticated key exchange protocol for automotive application. In: ESCAR-18 (2020)
4. Winkler, D., Sepúlveda, D., Cupelli, M., Olexa, R., Sepúlveda, J.: Quantum secure high performance automotive systems. In: ESCAR-19 (2021)
5. Wang, W., Stöttinger, M.: Post-quantum secure architectures for automotive hardware secure modules. In: Trends in Data Protection and Encryption Technologies, pp. 83–87 (2023)
6. Fritzmann, T., Vith, J., Flórez, D., Sepúlveda, J.: Strengthening post-quantum security for automotive systems. Microprocess. Microsyst. **87** (2021)
7. Bos, J.W., Dima, A., Kiening, A., Renes, J.: Post-quantum secure over-the-air update of automotive systems. In: EPRINT (2023)

8. Bos, J.W., Carlson, B., Renes, J., Rotaru, M., Sprenkels, D., Waters, G.P.: Post-quantum secure boot on vehicle network processors. In: EPRINT (2022)
9. Gonzalez, R., et al.: Verifying post-quantum signatures in 8 kB of RAM. In: PQCrypto (2021)
10. PQC Standardization. <https://nist.gov/pqcrypto>. Updated 11 Sept 2023
11. Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signature and public-key cryptosystems. *Commun. ACM* **21**(2), 120–126 (1978)
12. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**(5), 1484–1509 (1997)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

