International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/03 Volume 12, Issue 1, January – February (2025)

RESEARCH ARTICLE

Quantum-Resilient Secure Onboard Communication (QRSecOC): Integrating Post-Quantum Cryptography for Robust Automotive Network Security

Amjad Nsour
Electrical and Computer Engineering Department, Oakland University, Rochester, MI 48309, USA.
✉ amjadnsour@gmail.com

Received: 06 November 2024 / Revised: 14 January 2025 / Accepted: 02 February 2025 / Published: 28 February 2025

Abstract – With the automotive industry moving towards fully autonomous systems, the secure onboard communication is a necessity. Traditional cryptographic algorithms, such as RSA and ECC are threatened by the future threat quantum computers will pose and cannot be used any more. To overcome this, the study presents the Quantum Resilient Secure Onboard Communication (QRSecOC) protocol, a new hybrid cryptographic framework that combines classical cryptographic algorithms and Post Quantum Cryptography (PQC) in order to secure automotive networks. QRSecOC protocol protects data transmission over the Controller Area Network (CAN) between ECUs within a vehicle making sure its integrity, confidentiality and authentication. The protocol's key desirable features include adaptive encryption that enables it to dynamically change security levels according to real time threat assessments, as well as optimization mechanisms to reduce latency and reduce the needed computational overhead. Simulation results show that the use of the QRSecOC protocol results in a reduction of encryption latency by 47.3% with respect to RSA, while energy efficiency is improved by 23.2%. On top of that, the protocol achieves a twice higher security level with respect to traditional cryptographic techniques, providing robust protection from quantum enhanced attacks. Despite a 9.8% increase in computational overhead caused by embedding PQC, the system stays well under the computational power of automotive ECUs. Other than being a highly efficient solution for real time automotive applications, the protocol benefits from an increased throughput of 88.9%. Quantum threat is emerging and it is proposed that integrating the QRSecOC protocol provides a comprehensive solution that offers efficient secure communication for the future autonomous vehicles; while retaining backward compatibility with existing vehicular systems.

Index Terms – Post-Quantum Cryptography, Quantum-Resilient Secure Onboard Communication, Automotive Network Security, Lattice-Based Cryptography, ECU Security, CAN.

1. INTRODUCTION

With the advancement of modern vehicles to fully autonomous and connected systems, secure communication among multiple electronic components has become a key subject [1]. Particularly, vehicles are particularly vulnerable to cybersecurity risks due to the increasing reliance on Electronic Control Units (ECUs) to control critical functionalities including braking, steering and navigation [2]. With the rapid development in quantum computing, such traditional cryptographic algorithms as RSA and ECC are becoming much more vulnerable to [3]. According to estimates [4][5], quantum computers will able to successfully break these widely used cryptographic protocols within the next 10 to 20 years, rendering automotive networks and all of their communication systems vulnerable to future quantum enabled cyberattacks.

At the same time, seamless real-time communication introduces little room for the overhead introduced by traditional cryptographic systems [6]. The automotive industry is thus at a crossroad, which will require its communication systems onboard to be quantum resilient in the short term future. The Quantum-Resilient Secure Onboard Communication (QRSecOC) protocol, which uses Post Quantum Cryptography (PQC) to protect automotive communication networks from quantum threats and still keep performance overheads low and backward compatible with existing systems, is presented in this paper.

The rapid advancements in both quantum computing and the automotive industry present a unique and urgent problem: The communication inside vehicles is secured against future quantum enabled threats [7]. The automotive cybersecurity market globally was estimated at USD 5.3 billion in 2017 and is expected to grow with a CAGR of 15.9% from 2018 to 2025, reaching at USD 8.94 billion by 2025 [8-10]. Yet, this growth does take on huge risks. Both existing cryptographic algorithms, such as RSA and ECC, based on the problem of factoring large numbers and finding discrete logarithm are

RESEARCH ARTICLE

vulnerable to Shor's algorithm. These algorithms are destroyed by the fact that Shor's algorithm, which could run on a sufficiently powerful quantum computer, runs them efficiently [11].

It is expected that the first quantum computers capable of breaking traditional encryption algorithms will arrive as early as 2030; 2035 is when full scale quantum capability is expected [12]. It is particularly vulnerable to attacks in the automotive industry where a high amount of Controller Area Networks (CAN) and Ethernet based communication protocols have been deployed, which are based on outdated cryptographic techniques [13]. In particular, CAN is popular in modern vehicles, as it is used in more than 90% of new cars [14]. Despite improvement in its security, the cryptographic building blocks of these protocols remain dependent on classical computing assumptions that will no longer be valid in the quantum world [15].

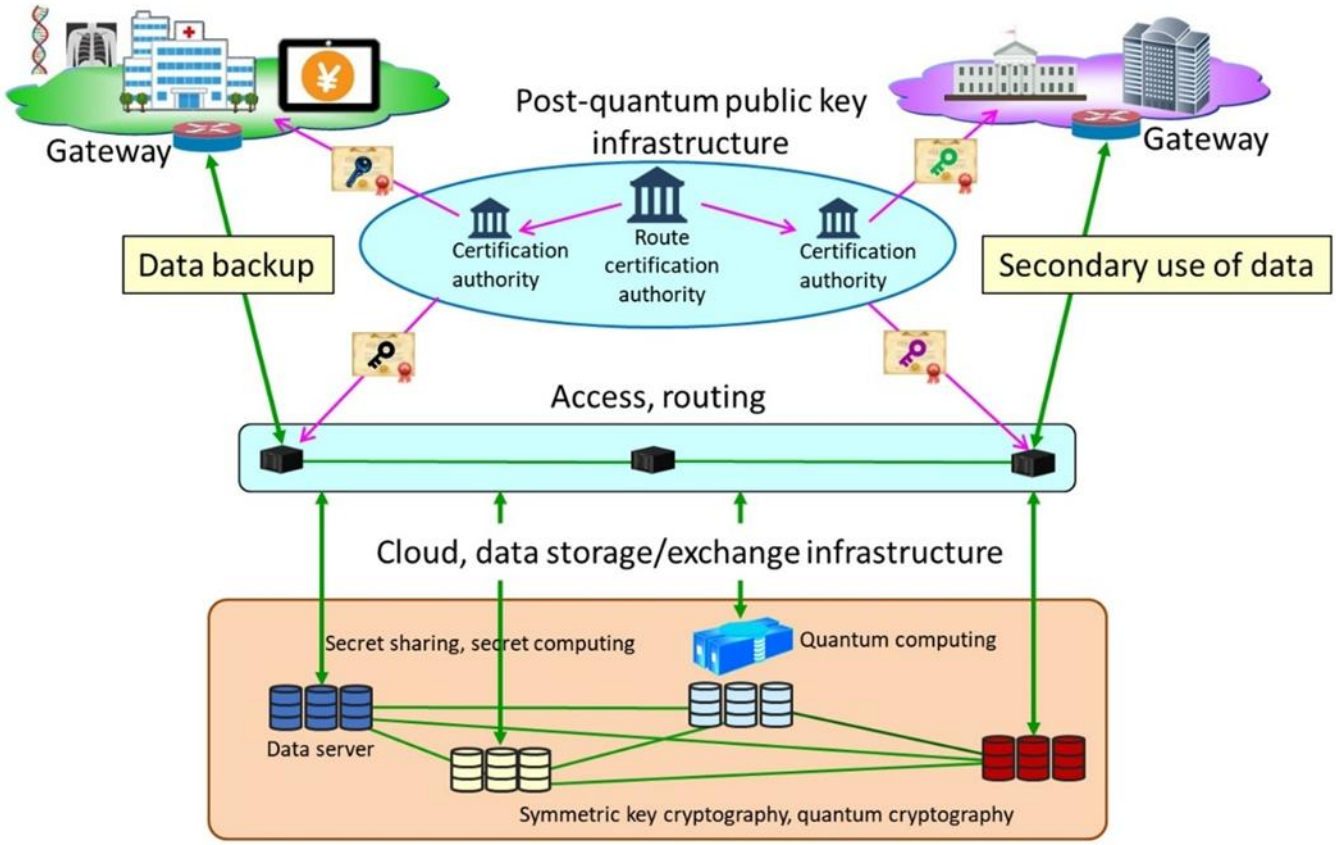

Figure 1 Post-Quantum Public Key Infrastructure for Secure Data Exchange and Storage in Cloud Environments

And, with quantum computing on the near horizon, protecting data storage and data transfer infrastructures held in the cloud is crucial. Post-Quantum Public Key Infrastructure (PKI) system integrating quantum resistant cryptographical methods for secure routing, Certification and Data Exchange is illustrated in Figure 1. At its core it is comprised of a certification authority, secret sharing protocol, and quantum cryptography so that sensitive information is safeguarded and the access is not unauthorized.

The movement to address the quantum threat has led to the development of Post Quantum Cryptography (PQC), especially lattice based cryptography. Known quantum attacks do not attack lattice based cryptographic methods, which gives strong security guarantees in [16]. While performance and feasibility of these methods have been demonstrated, the optimization of such algorithms for automotive applications where real time and low latency communication is critical has yet to be solved [17]. To overcome these challenges, the study propose the QRSecOC protocol, a hybrid cryptographic solution that uses both traditional and post quantum algorithms for secure communication while maintaining compatibility to existing vehicular systems [18].

Cryptographic protocols in automotive networks are becoming more and more implementation of quantum resilient protocols. Second, the first hurdle Post Quantum Cryptography (PQC) algorithms face is an underscored challenge in software performance that exists with resource constrained environments of Electronic Control Units (ECUs)

RESEARCH ARTICLE

in vehicles [19]. Units have been designed to be low computation overhead with the integration of PQC causing increased latency and decreased real time performance [20]. In parallel, backward compatibility is also one of the main concerns. The current state of automotive infrastructure is based upon existing Controller Area Networks (CAN) and require existing cryptographic protocols such as 3DES [21]. These systems are a complex retrofitting to support the quantum resistant without disrupting functionality [22]. Third, the applications of security within the automotive industry necessitate hardening cryptographic methods through integrity testing in real world conditions, which have yet to be proven for quantum resistant methods [23]. Finally, the quantum threat itself is changing so quickly that the study find it difficult to design solutions which remain secure against classical and quantum attacks simultaneously.

1.1. Problem Statement

Several mitigations to the challenges of enabling the integration of Post-Quantum Cryptography (PQC) into automotive Network have been proposed. To provide a transitional framework, both traditional and PQC algorithms are being combined in hybrid cryptographic scheme to tackle security against both classical and quantum threats. With this approach the gradual evolution can occur without incompatibility with existing systems. However, lattice based cryptographic techniques having emerged as a way to balance security with computational efficiency [24], researchers have been targeting the optimisation of such algorithms for real time vehicular communication resulting from the lack of performance. In addition, modular upgrades to regular ECUs are suggested to make quantum secure without requiring a total system overhaul. Other researchers are also developing adaptive cryptographic solutions, which adaptively change their security parameters depending on the detected threat level, maintaining security without incurring unnecessary computational overhead [9], [10]. These methods have been shown to be able to significantly increase security and performance of onboard communications in simulation studies, and can act as a viable path forward for the automotive industry.

The security challenges in automotive networks arise as the requirement on secure onboard communication continues to rise, especially due to the introduction of autonomous and connected vehicles. Currently, cryptographic protocols are employed to secure communication between Electronic Control Units (ECUs) present inside vehicles, which are very susceptible to future quantum based cyberattacks. Since automotive networks have been conceptualized with the notion that they will only exist for a short time, and since cryptographic algorithms such as RSA and ECC are based on antiquated technology, with the rapid growth of quantum computing these algorithms will reach their expiration date, making automotive networks vulnerable to breaches. However, to tackle these vulnerabilities the shift to post-quantum cryptographic solutions is necessary, yet there is still the need to integrate quantum resilient algorithms into the existing infrastructure without degrading its performance. While there is much work continuing in the realm of Post Quantum Cryptography (PQC) and its use in many industries, there has been limited academic progress to the particular security threats of in vehicle networks. A side addition is that the quantum resilient solutions have not yet been adequately explored in terms of their backward compatibility and real time performance. To address those gaps, this dissertation proposes a Quantum-Resilient Secure Onboard Communication (QRSecOC) protocol, which relies on the use of lattice based PQC algorithms to ensure that automotive networks' security is not compromised with respect to performance standards and compatibility with existing vehicular systems.

1.2. Aims and Objectives

This research designed and implemented a Quantum Resilient Secure Onboard Communication (QRSecOC) protocol to ensure that automotive networks are offering robust, low latency, and computationally efficient security, yet are forensically resilient to quantum attacks.

- The goal is to design a hybrid cryptographic framework built upon the fusion of Post-Quantum Cryptography (PQC) and traditional approaches in order to endure backward and future-proof compatibility to quantum threats.
- This thesis describes encryption optimized in latency and computational overhead, while maintaining real time performance in resource constrained Electronic Control Units (ECUs).
- Designing an adaptive encryption system that changes its security properties in response to real time network conditions and potential threats.
- Security and low power consumption for in-car communication are evaluated on a cryptographic system to guarantee minimized power consumption of the proposed cryptographic system.

This research presents a new way to secure automotive communication networks through the inclusion of post-quantum cryptographic techniques. The key contributions are:

1. A novel hybrid cryptographic protocol for secure communication in automotive systems, which combines classical and quantum resilient algorithms is proposed.
2. A multi objective framework on developing a tradeoff among latency, computational overhead, energy consumption and security strength.

RESEARCH ARTICLE

3. A dynamic encryption scheme which adapts its cryptographic parameters depending upon network load and threat level.
4. Performance analysis of the proposed solution with the conducting of comprehensive simulation-based performance analysis in order to compare the efficiency and security of the proposed solution in the real-world automotive environments.
5. Creating the system so it will be backward compatible with current cryptographic system present in vehicles while moving towards a quantum resilient security.

1.3. Research Organization

The remaining sections are organized as follows:

Existing cryptographic methods and their limitations in the quantum era are covered in the Literature Review (section 2). The problem formulation, the problem optimization framework and the Design and implementation of the Quantum-Resilient Secure Onboard Communication (QRSecOC) protocol are described in the Methodology section (section 3). The Results and Discussion (section 4) evaluates the performance of the proposed solution through simulations with comparison to existing methods in the Results. The Conclusion (section 5) summarizes the findings, provides contributions, and suggests future work.

2. LITERATURE REVIEW

As the automotive technologies evolve rapidly, security has come to play major role which remains critical in the context of future quantum computing capabilities that are expected to prematurely disrupt the classical cryptographic systems. Designs for Quantum Resilient Secure Onboard Communication (QRSecOC) are presented which integrate post quantum cryptography (PQC) into automotive network security to protect against these future threats. This systematic review seeks the current research on quantum resilient strategies, cryptographic mechanisms applied in secure onboard communication in vehicles.

The revolution of quantum computing is expected to bring about considerable change in many areas; however, it has posed a tremendous challenge to classical cryptographic systems. The classical algorithms used for securing the digital communication, like RSA and Elliptic Curve Cryptography (ECC) are based on the mathematical problem which is hard to solve on the current computing power. Hence, for example, an example of RSA as an algorithm based on factoring large integers, whereas ECC based on discrete logarithm problem. For classical computers, these problems are intractable, whereas inspired from Shor's algorithm, both these problems can be solved efficiently using a quantum computer. Because of this, when these cryptosystems are broken by quantum computers, the study will expose sensitive data to significant risk. The development of quantum resistant cryptographic techniques or post quantization cryptography (PQC) [1] is anticipated in anticipation of this.

PQC is about algorithms code that can resist attacks by both classical and quantum computers. Post Quantum Cryptographic algorithms proposed usually adress some quantum computational challenge. Two of the more promising candidates are lattice based cryptography, which is based on the hardness of solving problems in high-dimensional lattices, as well as hash based signatures, which depend on the intractability of cryptographic hash functions. Several other forms of multivariate cryptosystems that require the problem of solving systems of multivariate quadratic equations are also being explored. As quantum resilient systems, these are believed to be secure against classical and quantum computer attack, and so form a strong foundation. They are particularly important for vehicle networks where confidentiality, integrity, and availability of communications are critical for safe operation [2].

Nevertheless, conversion to PQC is not an easy task. A big problem with PQC algorithms is that they typically need more computational resources (more processing power and memory) than classical cryptographic algorithms. In resource constrained environments like automotive sytems, where processing power, energy consumption and memory availability are limited, this can be real problem. As an example, lattice-based cryptography may be very secure (when compared to traditional cryptography), but it may require significantly longer keys and extra computation compared to traditional cryptography, potentially affecting system performance, for instance, with real time applications [3].

To address these, researchers are working toward PQC optimizing to automobile systems. In response, Bos et al. [4] use PQC to automate secure boot mechanisms for vehicle network processors while keeping the hardware free of the overhead created by the mechanisms. In automotive systems, secure boot is a critical feature: it can only run trusted software on a vehicle's electronic control units (ECUs). This research shows a viable path to integrate quantum-resistant cryptography in automotive security architectures, which means demonstrating the study can do this without significantly increasing resource demand and in a manner having such that PQC can be brought within secure boot processes.

With the increasing interconnectivity of modern vehicles, the automotive industry is particularly vulnerable to cyberattacks, and comes with challenges unique to that industry. Within this growing attack surface there is vehicle to everything (V2X) communication, in-vehicle Ethernet, and increasingly complex onboard systems. However, integration of these technologies improves vehicle performance and safety, but at

RESEARCH ARTICLE

the expense of new potential security vulnerabilities. When quantum computing advances, automotive networks cryptographic systems used in devices throughout the network will be ever more susceptible, for example for encrypting the communication between ECUs. When quantum computers mature, adversaries will be able to find classical cryptographic algorithm weaknesses to compromise vehicle systems [5].

The applicability of PQC to the automotive use cases has been proactively researched and addressed by researchers. Protection of ECUs that control different critical functions of contemporary vehicles is one of the most focused aspect. To provide the safety and reliability of vehicle operations, they depend on secure communication protocols. Fritzmann et al. [8] use PQC to augment the security of ECUs' communication. They were focusing on the necessity of quantum resistant encryption algorithms to protect the message relationship between ECUs from being digested with quantum permitted opponents. By securing these communications, automotive systems are future proofed against threat to the safety of connected and autonomous vehicles by being made immune to quantum attacks.

In the area of automotive, the integration of post-quantum cryptography (PQC) in critical elements such as inter vehicular (V2V), onboard communication, and over the air (OTA) upgrades, has been extensively studied in [7]. With modern vehicles using more interconnected systems than ever, this means that secure OTA updates are necessary to ensure system integrity, and V2V communication is to be used to enable autonomous driving, and enable advanced safety features among other areas. The study also underlined the importance of the need for quantum safe encryption mechanisms, as common cryptographic algorithms, such as RSA and ECC, could become obsolete when quantum computing matures. As such, this is why the adoption of PQC is so vital both for future protection of quantum based cyberattacks against the different communication layers present in the automotive networks. Fritzmann et al. underscored the importance of integrating quantum safe cryptography seamlessly and with no impact on performance so that automotive systems remain secure.

Likewise, Hasan et al. [9] presented a detailed framework for moving automotive systems over to PQC. The security dependencies of various cryptographic algorithms were analyzed and their suitability for automotive applications evaluated. They explored how the current cryptographic infrastructures can be gradually replaced or augmented with PQC methods while a threat of quantum computers gets stronger. Hasan et al. provide insights in how critical automotive systems components such as electronic control units (ECUs), communication networks and cloud based servises can be protected with different post quantuam algorithms (Such as lacette based cryptography and hash based signatures). Designed as a foundation for automaking manufacturers to start implementing quantum resistant technology while retaining compatibility with current systems, the framework they developed is worth a look.

Although PQC holds a promising future, the inclusion into automotive systems is confronted by several significant challenges. The fact that PQC is incompatible with other communication protocols and hardware that were deliberately built for these classical cryptographic systems is one of the primary issues. This challenge was explored by Li [11], who notes that real time automotive applications may be affected by the computational overhead of PQC algorithms. For an example, while lattice based cryptography is quantum resistant, its bulky key sizes and complicated computations can make the application in the clock sensitive processes like autonomous driving and vehicle control systems a time consuming affair. In terms of energy consumption, for electric vehicles and into resource constrained applications, PQC may also incur the additional processing power needed to perform it, thus increasing the overall energy consumption burden of automotive electronic system. For example, since automotive systems involves optimizing PQC algorithms with security, performance tradeoffs, it then becomes a significant technical hurdle to optimize.

In a novel work, Hoque et al. [10] investigate combining quantum key distribution (QKD) with PQC to develop a more sustainable and secure mobile network architecture for vehicles. PQC is supposed to resist quantum attacks, but QKD adds another layer of security — it is a way to exchange encryption keys over the quantum channel, which is supposed to be unbreakable computationally, including by quantum computers. Then, QKD and PQC integrated provides a secure vehicle communication network. Hoque et al. however also commented that design and maintenance burden increases due to the complexity of implementing such hybrid approaches. The related complexity comes from the need to devise quantum communication channel infrastructure alongside classical networks, increasing the cost and logistical difficulties for automotive manufacturers.

To avoid these risks and simultaneously continue to leverage existing financially motivated cybersecurity threats and emerging technological capabilities, Liu and Moody [12] argue that the study ought to gradually transition to a future which is quantum secure. PQC is a promising solution to the quantum threat, but its integration should not be considered in isolation, but instead harmonised with the wider cybersecurity landscape which is in continuous evolution, they argued. Rapid development in AI and ML technologies along with the uptake of IoT devices in vehicles makes the security environment even more complex. To maintain that position (resilient in the face of future threats), Liu and Moody believe a holistic approach to cybersecurity — integrating PQC along

RESEARCH ARTICLE

with AI driven security protocols – will be necessary.

However increasing research has been done for developing quantum safe architectures specifically designed for automotive application to ensure long term security. In the post-quantum era, Malina et al. [13] offered a path to address the privacy concerns of intelligent infrastructures as they deal with autonomous vehicles. Quantum-safe encryption alone isn't enough, they stressed, arguing that a fully protective approach requires both system-wide privacy protections and the implementation of such encryption. As vehicles become more autonomous, connected to intelligent infrastructure, Malina et al. argued that privacy concerns from communication encryption will not be the only privacy concerns. To tackle data collection, processing and storage problems in smart cities and intelligent transport systems need to be solved with privacy preserving and quantum resistant technologies. In all, this holistic security and privacy approach to security and privacy will be critical to ensure trust in the autonomous vehicle system and to stop malicious exploitation of sensitive data.

Manna et al. [14] also considered issue the cost of incorporating quantum security in OTA updates for automotive systems. Vehicle software needs to be maintained via OTA updates because bugs need to be fixed and system performance has to be improved. But, due to resource intensity, they need to be rethought for existing systems when secured using PQC. Manna et al. pointed out that real-time communication protocols which are key to guaranteeing the smooth operation of autonomous vehicles would be reengineered to integrate the added complexities of PQC. The updates must be delivered both securely and efficiently, as they cannot interfere with the performance and safety characteristics of the vehicle. As a result, PQC offers stronger security guarantees at the price of both high cost and performance realization, and necessitates system redesign.

In addition to this, Pradhan and Patil [16] isolated this quantum cryptography as a method for further improving the security of communication networks in autonomous vehicles. In a highly connected, autonomous vehicle network, given their unbreakable cryptography, quantum cryptography, particularly QKD, has the potential to provide secure communication. But they added that the high costs of adopting quantum cryptography still stand as a major hurdle to widespread use. Deployment of quantum networks for quantum communication still requires substantial investment and is in its early stages of infrastructure required. The cost of retrofitting existing systems with its quantum safe solutions may outweigh the immediate benefits to automotive manufacturers for two reasons: First, there is considerable uncertainty regarding the actual date of the availability of fully working quantum computers.

However, for long term security against quantum computing threats, automotive networks must be integrated with post quantum cryptography. PQC algorithms themselves come with challenges like how to achieve compatibility and how increases in computational overhead may be addressed, but work is ongoing that attempts to mitigate these challenges in optimized, cryptographic, and hybrid designs that employ classical as well as quantum resistant approaches [17], [23]. Future automotive network security may be a multi-dimensional task that must focus on application-level encryption as well as system level architectural changes to enable robust, quantum resilient security in the automotive industry [24]. Table 1 is the comparative table of quantum-resilient secure onboard communication (QRSecOC) integrating post-quantum cryptography for robust automotive network security.

Table 1 Comparative Table of Quantum-Resilient Secure Onboard Communication (QRSecOC) Integrating Post-Quantum Cryptography for Robust Automotive Network Security

Author(s)	Main Focus	Algorithm	Application in Automotive	Challenges	Proposed Solution	Implementation Feasibility
[1]	Secure boot for vehicle processors	Post-quantum secure boot mechanisms	Vehicle network processors	Hardware resource constraints	PQC integrated secure boot	Feasible with optimized integration
[3]	Combining PQC with QKD	Post-quantum cryptography, quantum key distribution (QKD)	Mobile network security for vehicles	Complexity of hybrid systems	Hybrid PQC-QKD framework	Complex and costly but highly secure
[15]	Cost of PQC for OTA updates in automotive systems	OTA security using PQC	Secure OTA updates in automotive systems	Cost of implementation and redesign	Re-engineering communication protocols	Feasible but high initial cost and redesign effort

RESEARCH ARTICLE

[22]	Quantum cryptography for autonomous vehicle networks	Quantum cryptography	Secure communication in autonomous vehicles	High cost of implementing quantum cryptography	Using quantum cryptography for secure V2X	Feasible but limited by cost and infrastructure requirements
[23]	Post-Quantum Cryptography for Network Security	NTRUEncrypt, PQC algorithms	Secure communication in vehicle-to-network systems	Adaptability to existing communication systems	Survey of PQC solutions for automotive networks	Feasible but requires adaptation to existing infrastructure

3. METHODOLOGY

In this section, the study describes in detail the proposed Quantum Resilient Secure Onboard Communication (QRSecOC) protocol. Incorporating Post-Quantum Cryptography (PQC) into this protocol guarantees that automotive networks remain secure.

System model, mathematical formulation, and main components of the protocol proposed include encryption and decryption processes, latency optimization, computational overhead, and energy efficiency are discussed.

3.1. Multi-Objective Quantum-Resilient Cryptographic Optimization for Secure Automotive Communication Networks:

This research intends to secure communication between Electronic Control Units (ECUs) in the automotive network through quantum resilient cryptographic protocols. Optimizing security against quantum adversaries, minimizing latency, computational overhead, and energy consumption represents a challenge.

With regard to real time communication, it should exist in the system, whereby the real time communication does not exceed the processing limit of ECUs and backward compatibility with current crypto standards has to be maintained.

Let $\mathcal{N} = \{n_1, n_2, \dots, n_k\}$ represent the set of ECUs, and let $\mathcal{C} = \{c_1, c_2, \dots, c_m\}$ represent the communication channels between these ECUs. The encryption and decryption processes for each channel c_i are given by the post-quantum cryptographic (PQC) algorithm as in Equation (1):

$$E(c_i) = \mathcal{PQC}\big(k_i, \mathcal{F}(m_i)\big) \quad \text{and} \quad D(c_i) = \mathcal{PQC}^{-1}\big(k_i, E(c_i)\big) \tag{1}$$

where k_i is the encryption key, m_i is the message, and $\mathcal{F}(m_i)$ represents any additional cryptographic transformations.

3.1.1. Latency Function

The overall encryption latency L is the sum of latencies for each communication channel, formulated as in Equation (2):

$$L = \sum_{i=1}^{m} \lambda_i = \sum_{i=1}^{m} \left(\alpha_i \cdot f(|m_i|, \mathcal{O}(\mathcal{PQC}), O_i) \cdot \left(\sum_{l=1}^{n_i} \frac{1}{\gamma_l} \right) \right) \tag{2}$$

where α_i is the priority factor, $|m_i|$ is the message size, O_i is the network overhead, and γ_l represents processing capacity.

3.1.2. Computational Overhead Function

The computational overhead $\mathcal{H}$ is the sum of overheads across all ECUs as in Equation (3):

$$\mathcal{H} = \sum_{i=1}^{k} \sum_{j=1}^{m} \sum_{l=1}^{n_j} \left(\mu_{ij} \cdot \frac{\mathcal{O}(\mathcal{PQC}) \cdot \mathcal{C}(\theta_l, \zeta_j)}{\log(\beta_{ij} + \epsilon)} \right) \tag{3}$$

where μ_{ij} is the computational capacity, $\mathcal{C}(\theta_l, \zeta_j)$ is the complexity of the cryptographic algorithm, and ϵ is a small constant to prevent division by zero.

3.1.3. Security Function

The security level $\mathcal{S}$ for each channel is represented as in Equation (4):

$$\mathcal{S}(k_i, m_i) = \sum_{i=1}^{m} \Big(\beta_i \cdot \big(\mathcal{H}_\infty(k_i) \times \psi_i(m_i) \times \mathcal{R}(\mathcal{PQC}, m_i) \big) \Big) \tag{4}$$

where $\mathcal{H}_\infty(k_i)$ is the min-entropy of the key, $\psi_i(m_i)$ is a message security factor, and $\mathcal{R}(\mathcal{PQC}, m_i)$ is the cryptographic strength.

3.1.4. Energy Consumption Model

The total energy consumption E_{total} is calculated as in Equation (5):

$$E_{\text{total}} = \sum_{i=1}^{k} \sum_{j=1}^{m} \int_0^T \left(P_{ij}(t) \cdot \mathcal{E}(\mathcal{PQC}, t) \cdot \left(\frac{1}{1 + \delta_{ij}(t)} \right) \right) dt \tag{5}$$

RESEARCH ARTICLE

where $P_{ij}(t)$ is the power consumption of ECU n_j, $\mathcal{E}(\mathcal{PQC}, t)$ is the energy consumption of the cryptographic algorithm, and $\delta_{ij}(t)$ represents a dynamic energy reduction factor.

3.1.5. Objective Function

The objective is to minimize latency, overhead, and energy consumption, while maximizing security. The multi-objective function is defined as in Equation (6):

$$\min_{k_i, m_i}(L + \alpha \cdot \mathcal{H} + \theta \cdot E_{\text{total}} - \beta \cdot \mathcal{S}) \quad (6)$$

where α, β, and θ are scaling factors.

3.1.6. Constraints

The optimization problem is subject to the following constraints as in from Equation (7)-(11):

1. Latency Constraint

$$\sum_{i=1}^{m} \lambda_i \leq \tau_{\max} \quad (7)$$

2. Security Constraint

$$\mathcal{S}(k_i, m_i) \geq \mathcal{S}_{\min}, \quad \forall c_i \in \mathcal{C} \quad (8)$$

3. Computational Overhead Constraint

$$\sum_{j=1}^{m} \mu_{ij} \cdot \mathcal{O}(\mathcal{PQC}) \leq \mu_{\max}, \quad \forall n_j \in \mathcal{N} \quad (9)$$

4. Energy Consumption Constraint

$$E_{\text{total}} \leq E_{\text{budget}} \quad (10)$$

5. Backward Compatibility Constraint

$$\forall c_i \in \mathcal{C}, \quad E_{\text{classical}}(c_i) = E_{\text{PQC}}(c_i) \quad (11)$$

3.2. System Model

The QRSecOC protocol discussed in this paper is designed to provide a mechanism to secure communication between Electronic Control Units (ECUs) in an automotive network.

It provides for message transmission in a secure manner across a Controller Area Network (CAN), while maintaining backward compatibility with existing systems.

System model includes ECUs, communication channels, encryption keys and cryptographic algorithms.

The network is protected from classical and quantum adversaries using a hybrid cryptographic technique which includes traditional and PQC algorithms.

The parameters of the key parameters used in the system model are listed in Table 2, along with their descriptions.

Table 2 System Model Parameters

Parameter	Description
$\mathcal{N}$	Set of Electronic Control Units (ECUs) within the automotive network. Each ECU is responsible for a specific function.
$\mathcal{C}$	Set of communication channels between ECUs for message exchange.
k_i	Encryption key used for secure communication over channel c_i.
m_i	Message transmitted over channel c_i.
$E(c_i)$	Encryption function for channel c_i using the Post-Quantum Cryptographic (PQC) algorithm.
$D(c_i)$	Decryption function for channel c_i.
λ_i	Latency associated with encrypting and transmitting the message over channel c_i.
$\mathcal{H}$	Computational overhead of the cryptographic algorithm across all ECUs.
E_{total}	Total energy consumption for performing cryptographic operations over all communication channels.
$\mathcal{S}(k_i, m_i)$	Security level for the message m_i transmitted over channel c_i based on the cryptographic strength of the PQC algorithm.
α_i, β_i	Scaling factors for latency and security, respectively.

3.3. Proposed Quantum-Resilient Secure Onboard Communication (QRSecOC)

The Quantum-Resilient Secure Onboard Communication (QRSecOC) protocol is a hybrid cryptographic framework that integrates classical encryption methods with Post-Quantum Cryptography (PQC) to safeguard in-vehicle networks against both classical and quantum threats. This section presents the detailed components of the QRSecOC protocol, including its hybrid cryptographic structure, adaptive security mechanism, performance optimization, and energy efficiency.

3.3.1. Hybrid Cryptographic Scheme

The QRSecOC protocol employs a hybrid cryptographic approach, which combines traditional cryptographic algorithms such as RSA or ECC with lattice-based Post-Quantum Cryptography (PQC). The hybrid encryption allows backward compatibility with existing automotive infrastructure while providing future-proof security against

RESEARCH ARTICLE

quantum-enabled attacks. Figure 2 illustrates the Hybrid Cryptographic Scheme: Combining Classical and Post-Quantum Cryptography.

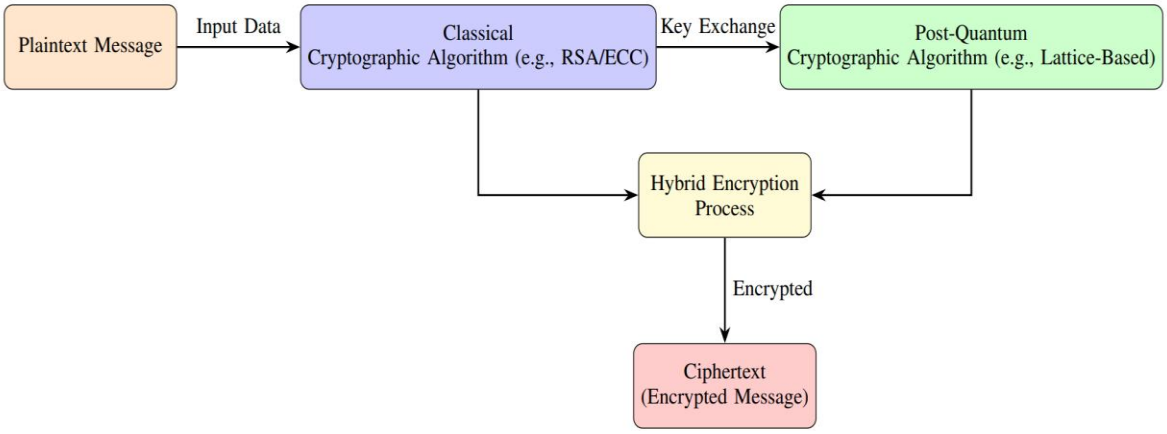

Figure 2 Hybrid Cryptographic Scheme: Combining Classical and Post-Quantum Cryptography

Given a message m_i transmitted over communication channel c_i, the hybrid encryption process is defined as in Equation (12):

$$E_{\text{hybrid}}(c_i) = E_{\text{PQC}}\left(E_{\text{classical}}(k_i, \mathcal{F}(m_i))\right), D_{\text{hybrid}}(c_i) = D_{\text{classical}}\left(D_{\text{PQC}}\left(k_i, E_{\text{hybrid}}(c_i)\right)\right) \quad (12)$$

where:

- $E_{\text{PQC}}(\cdot)$ and $D_{\text{PQC}}(\cdot)$ represent the encryption and decryption operations using the PQC algorithm (e.g., lattice-based encryption).
- $E_{\text{classical}}(\cdot)$ and $D_{\text{classical}}(\cdot)$ represent encryption and decryption using traditional algorithms (e.g., RSA or ECC).
- k_i is the encryption key for channel c_i, and $\mathcal{F}(m_i)$ represents any pre-encryption transformations (e.g., padding or hashing).

The strength of this hybrid approach is twofold: (1) backward compatibility, as existing ECUs and communication networks can still function using classical algorithms, and (2) future-resilience, as the use of PQC ensures security against quantum adversaries.

3.3.2. Adaptive Security Levels

The QRSecOC protocol dynamically adjusts the security level based on real-time network conditions and threat assessments. This is done by modulating the encryption key size, the cryptographic algorithm, or the number of rounds of encryption, depending on the severity of the detected threat. Figure 3 shows the Flowchart for Adaptive Security Levels Based on Real-Time Threat Analysis.

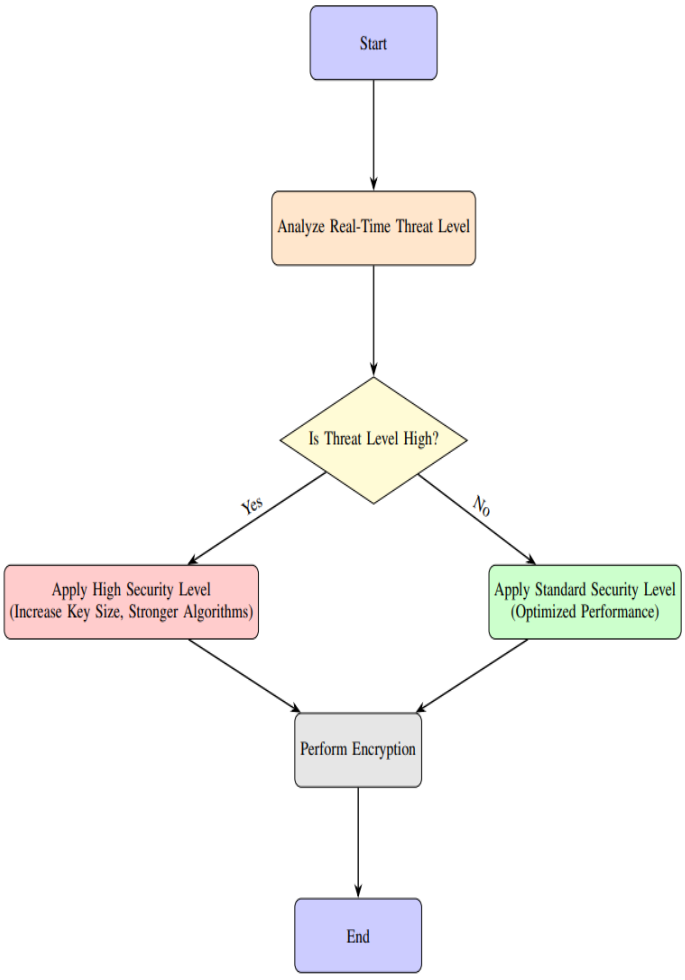

Figure 3 Flowchart for Adaptive Security Levels Based on Real-Time Threat Analysis

RESEARCH ARTICLE

Let $\mathcal{T}(t)$ represent the real-time threat level at time t. The security level $S(t)$ of the encryption process is a function of the threat level $\mathcal{T}(t)$, the key length $l(t)$, and the cryptographic strength $\mathcal{PQC}(t)$. This can be modeled as in Equation (13):

$$S(t) = f\big(\mathcal{T}(t), l(t), \mathcal{PQC}(t)\big), \quad \text{with} \quad l(t) = l_{\min} + (\mathcal{T}(t) - \mathcal{T}_{\min}) \cdot k \tag{13}$$

where:

- $l_{\min}$ is the minimum key length allowed.
- $\mathcal{T}_{\min}$ is the minimum threat level, and k is a scaling factor.
- $\mathcal{PQC}(t)$ is the security level of the PQC algorithm in use, determined by its complexity and resistance to quantum attacks.

When a higher threat level is detected, the system automatically increases the cryptographic strength by increasing the key length or using a more complex algorithm.

3.3.3. Optimization of Latency and Computational Overhead

Given the real-time requirements of automotive systems, latency and computational overhead must be minimized. The encryption latency λ_i for channel c_i is modeled as a function of the message size $|m_i|$, the computational complexity of the PQC algorithm $\mathcal{O}(\mathcal{PQC})$, and the network overhead O_i. The latency function for channel c_i is given by in Equation (14):

$$\lambda_i = f(|m_i|, \mathcal{O}(\mathcal{PQC}), O_i) = \alpha_i \cdot \left(\frac{|m_i|}{\mathcal{C}_{\text{PQC}} + O_i}\right) \tag{14}$$

where α_i is the priority factor, and $\mathcal{C}_{\text{PQC}}$ is the computational complexity of the PQC algorithm. The overall latency L for the system across all channels is in Equation (15):

$$L = \sum_{i=1}^{m} \lambda_i \tag{15}$$

To minimize overhead, the QRSecOC protocol implements efficient encryption techniques that reduce unnecessary computations, especially in low-priority communication tasks. Figure 4 shows the Flowchart for Optimization of Latency and Computational Overhead.

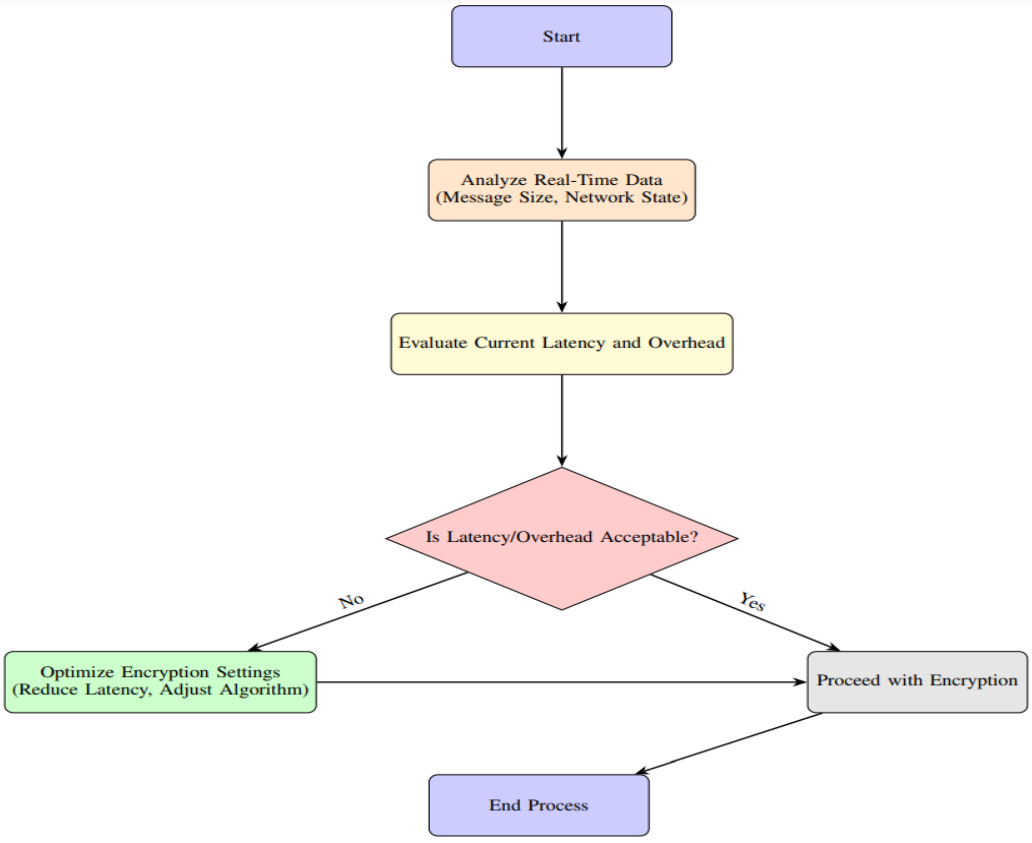

Figure 4 Flowchart for Optimization of Latency and Computational Overhead

RESEARCH ARTICLE

3.3.4. Energy Efficiency

Energy efficiency is crucial in automotive systems, especially for Electric Control Units (ECUs) that operate in resource-constrained environments. The total energy consumption E_{total} of the cryptographic system is modelled as in Equation (16):

$$E_{\text{total}} = \sum_{i=1}^{k}\sum_{j=1}^{m}\int_{0}^{T}\left(P_{ij}(t)\cdot\mathcal{E}(\mathcal{PQC},t)\cdot\left(\frac{1}{1+\delta_{ij}(t)}\right)\right)dt \quad (16)$$

where:

- $P_{ij}(t)$ is the power consumption of ECU n_j at time t.
- $\mathcal{E}(\mathcal{PQC},t)$ represents the energy consumption of the PQC algorithm over time.
- $\delta_{ij}(t)$ is a dynamic energy reduction factor.

The objective is to minimize E_{total} while maintaining security, using dynamic energy optimization techniques to adjust cryptographic parameters in real-time.

3.4. QRSecOC Algorithm

The following algorithm summarizes the steps for the QRSecOC protocol, outlining the process of encryption, decryption, threat assessment, and optimization of latency and energy consumption. Figure 5 shows Flowchart for Proposed Quantum-Resilient Secure Onboard Communication (QRSecOC). Algorithm 1 shows the Quantum-Resilient Secure Onboard Communication (QRSecOC).

Input:

- Message m_i
- Threat Level $T(t)$
- Encryption Key k_i

Output:

- Encrypted Message $E_{hybrid}(c_i)$
- Optimized Latency and Energy

Initialization:

1. Set initial key length $l(t) = l_{\min}$
2. Set initial cryptographic strength $PQC(t)$
3. Monitor real-time threat level $T(t)$

Hybrid Encryption Process:

1. If $T(t) > T_{min}$ then
   - Adjust key length $l(t)$ and cryptographic strength $PQC(t)$
   - $S(t) = f\left(T(t), l(t), PQC(t)\right)$
2. Encrypt message using classical encryption: $E_{classical}(k_i, F(m_i))$
3. Apply PQC encryption: $E_{PQC}\left(E_{classical}(k_i, F(m_i))\right)$
4. Combine encrypted messages to form hybrid encryption: $E_{hybrid}(c_i) = E_{PQC}\left(E_{classical}(k_i, F(m_i))\right)$

Optimization:

1. Optimize encryption latency $\lambda_i = f(|m_i|, O(PQC), O_i)$
2. Minimize computational overhead and energy consumption E_{total}
3. Adjust energy reduction factor $\delta_{ij}(t)$ based on current ECU load

Decryption Process:

1. Decrypt message using PQC decryption: $D_{PQC}\left(k_i, E_{hybrid}(c_i)\right)$
2. Apply classical decryption: $D_{classical}\left(D_{PQC}\left(k_i, E_{hybrid}(c_i)\right)\right)$

Algorithm 1 Quantum-Resilient Secure Onboard Communication (QRSecOC)

The proposed Quantum-Resilient Secure Onboard Communication (QRSecOC) protocol incorporates an adaptive security mechanism designed to dynamically adjust cryptographic parameters, such as key length and algorithm complexity, based on real-time network conditions and detected threat levels. This ensures optimal security while minimizing unnecessary computational overhead. However, the current implementation lacks explicitly defined thresholds or criteria for triggering these adjustments, leaving the practical application of the mechanism somewhat unclear. To address this limitation, future research will focus on establishing well-defined metrics and decision criteria for adapting cryptographic parameters. These thresholds could be based on metrics such as anomaly detection rates, network traffic patterns, or predefined risk levels. The incorporation of machine learning models to predict and classify threat levels dynamically may further enhance the precision and responsiveness of this mechanism. By refining and clearly defining the adaptive security framework, the QRSecOC protocol can achieve a balance between security and

RESEARCH ARTICLE

performance, making it more robust and practical for real-world automotive applications.

The increased computational overhead introduced by PQC algorithms, even with optimization, poses challenges for low-resource ECUs. Addressing this requires further refinements in algorithm efficiency and resource management to ensure compatibility with the constrained environments of automotive systems.

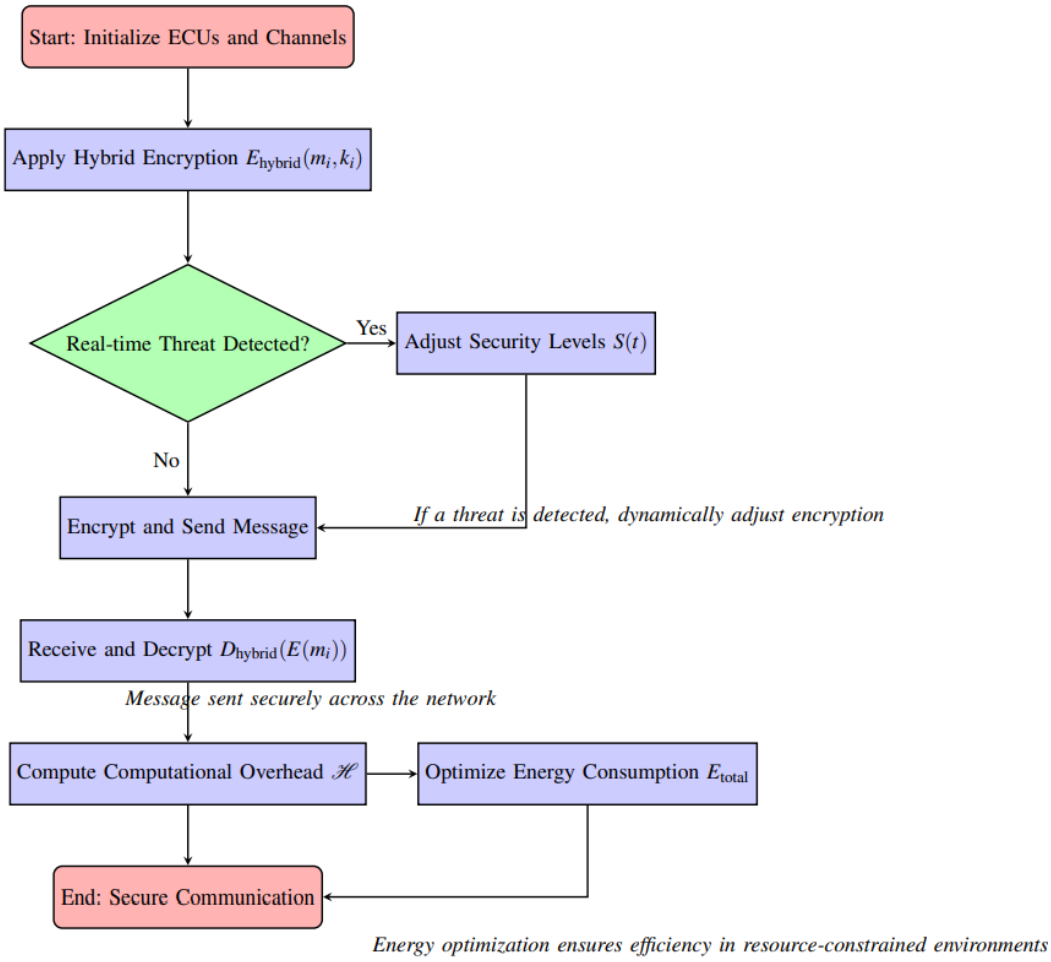

Figure 5 Flowchart for Proposed Quantum-Resilient Secure Onboard Communication (QRSecOC)

The QRSecOC protocol introduces notable advancements, but several challenges remain. The dual key management system for integrating classical and PQC algorithms increases system complexity and potentially contributes to additional overhead. Furthermore, while the protocol is designed for in-vehicle networks, its scalability to larger vehicular networks or V2X communication scenarios has not been addressed, which limits its broader applicability. The integration of backward compatibility with existing systems also lacks specific testing scenarios to validate its practical feasibility. Additionally, the energy optimization model, though effective in simulations, requires a more detailed explanation of the dynamic energy reduction factor to ensure consistent efficiency across diverse operational conditions. The security analysis could be enhanced with detailed threat modeling or simulated attack scenarios to strengthen the robustness of the evaluation. Lastly, the reliance on lattice-based cryptography overlooks other PQC options that may offer better trade-offs in terms of security, latency, and computational requirements for specific automotive applications. Addressing these gaps will be critical for refining the protocol and ensuring its viability in real-world automotive environments.

3.5. Mathematical Model Summary

The Quantum-Resilient Secure Onboard Communication (QRSecOC) protocol employs a hybrid cryptographic framework, incorporating the following key elements:

- A hybrid encryption scheme combining traditional cryptographic algorithms (e.g., RSA or ECC) with Post-Quantum Cryptography (PQC).

RESEARCH ARTICLE

- Dynamic adjustment of security levels based on real-time threat analysis and environmental conditions.
- Optimization of encryption latency and computational overhead, ensuring real-time performance for in-vehicle communication.
- Minimization of energy consumption through dynamic power management.

QRSecOC protocol, which is proposed, offers robust, low latency, and energy efficient communication between the ECUs of automative networks while still being resilient to quantum allowed cyber attacks.

3.5.1. Encryption and Decryption

Let $\mathcal{N} = \{n_1, n_2, \dots, n_k\}$ represent the set of Electronic Control Units (ECUs) in the network, and let $\mathcal{C} = \{c_1, c_2, \dots, c_m\}$ represent the set of communication channels between these ECUs. The encryption and decryption processes for a message m_i transmitted over channel c_i are defined as in Equation (17):

$$E(c_i) = \mathcal{PQC}\big(k_i, \mathcal{F}(m_i)\big) + \mathcal{E}_{\text{classical}}\big(k_i, \mathcal{F}(m_i)\big), D(c_i) = \mathcal{PQC}^{-1}\big(k_i, E(c_i)\big) + \mathcal{D}_{\text{classical}}\big(k_i, E(c_i)\big) \quad (17)$$

where:

- k_i is the encryption key associated with channel c_i.
- $\mathcal{F}(m_i)$ represents any additional transformations applied to the message m_i, such as padding or hashing.
- $\mathcal{PQC}(\cdot)$ and $\mathcal{PQC}^{-1}(\cdot)$ are the Post-Quantum Cryptography encryption and decryption functions.
- $\mathcal{E}_{\text{classical}}(\cdot)$ and $\mathcal{D}_{\text{classical}}(\cdot)$ represent classical encryption and decryption operations using traditional algorithms such as RSA or ECC.

The hybrid encryption combines classical and PQC algorithms to ensure backward compatibility and resistance against future quantum threats.

3.5.2. Latency Function

The total encryption latency L across all communication channels is a function of the message size $|m_i|$, the complexity of the PQC algorithm $\mathcal{O}(\mathcal{PQC})$, and network overhead O_i. the study model the latency for each communication channel c_i as in Equation (18):

$$\lambda_i = \alpha_i \cdot \left(\frac{|m_i|}{\mathcal{C}_{\text{PQC}} + O_i} \cdot \frac{1}{\gamma_i}\right) \quad (18)$$

where:

- α_i is the priority factor for channel c_i. Channels with higher priority experience lower latency.
- $|m_i|$ is the size of the message m_i transmitted over channel c_i.
- $\mathcal{C}_{\text{PQC}}$ is the computational complexity of the PQC algorithm.
- O_i represents the network overhead for channel c_i, which includes processing delays and transmission overhead.
- γ_i is the processing capacity of the ECU responsible for processing the message on channel c_i.

The total latency L for the system across all communication channels is given by in Equation (19):

$$L = \sum_{i=1}^{m} \lambda_i = \sum_{i=1}^{m} \alpha_i \cdot \left(\frac{|m_i|}{\mathcal{C}_{\text{PQC}} + O_i} \cdot \frac{1}{\gamma_i}\right) \quad (19)$$

The resulting equation ensures that latency minimization per message is guaranteed, based on the message size, computational overhead and processing capacity of the ECUs.

3.5.3. Computational Overhead Function

In other words, $\mathcal{H}$, related to an encryption and a decryption processes, is the totality of their respective computational overheads across all ECUs and communication channels. The PQC algorithm is complex and has a bearing on the computational resources available to the ECUs. The overhead for each ECU is 21 modelled as in Equation (20):

$$\mathcal{H}_{ij} = \mu_{ij} \cdot \frac{\mathcal{O}(\mathcal{PQC}) \cdot \mathcal{C}\big(\theta_l, \zeta_j\big)}{\log\big(\beta_{ij} + \epsilon\big)} \quad (20)$$

where:

- μ_{ij} is the computational capacity of ECU n_j when processing a message over channel c_i.
- $\mathcal{O}(\mathcal{PQC})$ represents the computational complexity of the PQC algorithm used for encryption.
- $\mathcal{C}\big(\theta_l, \zeta_j\big)$ represents additional computational complexity based on network topology parameters θ_l and cryptographic settings ζ_j.
- β_{ij} is the processing load on ECU n_j at time t, and ϵ is a small constant to prevent division by zero.

The total computational overhead $\mathcal{H}$ is calculated as the sum of individual overheads across all ECUs and communication channels as in Equation (21):

$$\mathcal{H} = \sum_{i=1}^{k} \sum_{j=1}^{m} \mathcal{H}_{ij} \quad (21)$$

3.5.4. Security Function

The security level $\mathcal{S}(k_i, m_i)$ for each channel c_i is determined by the cryptographic strength of the encryption key k_i, the

RESEARCH ARTICLE

message m_i, and the Post-Quantum Cryptography algorithm used. The security level is modelled as in Equation (22):

$$\mathcal{S}(k_i, m_i) = \sum_{i=1}^{m} \Big(\beta_i \cdot \big(\mathcal{H}_\infty(k_i) \times \psi_i(m_i) \times \mathcal{R}(\mathcal{PQC}, m_i)\big)\Big) \quad (22)$$

where:

- $\mathcal{H}_\infty(k_i)$ is the min-entropy of the key k_i, which quantifies the unpredictability of the key.
- $\psi_i(m_i)$ is a message security factor that depends on the sensitivity and importance of the message m_i.
- $\mathcal{R}(\mathcal{PQC}, m_i)$ represents the cryptographic strength of the PQC algorithm for the message m_i.
- β_i is a weighting factor that adjusts the contribution of each channel to the overall security level.

This model guarantees a one-to-one relationship between the security level and the strength of the encryption key, the significance of the message and the resilience of the PQC algorithm employed.

3.5.5. Energy Consumption Model

A calculated total energy consumption E_{total} is derived taking into account the energy ECU power consumption, energy E required by the PQC algorithm and dynamic adjustments with energy optimization. The energy consumption for each ECU is modelled as in Equation (23):

$$E_{ij}(t) = P_{ij}(t) \cdot \mathcal{E}(\mathcal{PQC}, t) \cdot \left(\frac{1}{1 + \delta_{ij}(t)}\right) \quad (23)$$

where:

- $P_{ij}(t)$ is the power consumption of ECU n_j at time t.
- $\mathcal{E}(\mathcal{PQC}, t)$ is the energy consumption of the PQC algorithm during encryption and decryption at time t.
- $\delta_{ij}(t)$ is a dynamic energy reduction factor that optimizes energy consumption based on real-time ECU load.

The total energy consumption for the system is given by Equation (24):

$$E_{\text{total}} = \sum_{i=1}^{k} \sum_{j=1}^{m} \int_0^T E_{ij}(t)\,dt \quad (24)$$

Using such an equation makes sure that dynamic adjustment for minimum energy consumption is still done while achieving high cryptographic security.

Given this, the problem becomes one of multi objective optimization, wherein latency along with computational overhead and energy consumption should be achieved with high security. The objective function is formulated as in Equation (25):

$$\min_{k_i, m_i} (L + \alpha \cdot \mathcal{H} + \theta \cdot E_{\text{total}} - \beta \cdot \mathcal{S}) \quad (25)$$

where:

- α, β, and θ are scaling factors that balance the trade-offs between latency, computational overhead, energy consumption, and security.

The optimization problem is subject to the following constraints in Equation (26)-(30):

- Latency Constraint

$$\sum_{i=1}^{m} \lambda_i \leq \tau_{\max} \quad (26)$$

where $\tau_{\max}$ is the maximum allowable latency.

- Security Constraint

$$\mathcal{S}(k_i, m_i) \geq \mathcal{S}_{\min}, \quad \forall c_i \in \mathcal{C} \quad (27)$$

where $\mathcal{S}_{\min}$ is the minimum acceptable security level.

- Computational Overhead Constraint

$$\sum_{j=1}^{m} \mu_{ij} \cdot \mathcal{O}(\mathcal{PQC}) \leq \mu_{\max}, \quad \forall n_j \in \mathcal{N} \quad (28)$$

where $\mu_{\max}$ is the maximum allowable computational overhead for each ECU.

- Energy Consumption Constraint

$$E_{\text{total}} \leq E_{\text{budget}} \quad (29)$$

where E_{budget} is the energy consumption budget for the system.

- Backward Compatibility Constraint

$$\forall c_i \in \mathcal{C}, \quad E_{\text{classical}}(c_i) = E_{\text{PQC}}(c_i) \quad (30)$$

to guarantee compatibility and minimizing performance or energy consumption discrepancy between the PQC and the classical encryption schemes.

The model provides a secure, efficient and quantum resilient onboard communication system for automotive networks taking into consideration key factors such as security, latency and energy consumption.

3.6. Performance Metrics

In this section, the study formally define and provide a description on the key performance metrics of the Quantum Resilient Secure Onboard Communication (QRSecOC)

RESEARCH ARTICLE

protocol. This gives an in depth review of how the system performed with metrics such as latency, security, computational overhead, energy consumption and more. In Table 3, a detailed description is provided for each metric as well with a corresponding mathematical formula.

Table 3 Performance Metrics for QRSecOC Protocol

Metric	Description	Formula
Encryption Latency (L)	The total time taken to encrypt messages across all communication channels. It depends on message size, PQC complexity, and processing capacity of ECUs.	$L = \sum_{i=1}^{m} \lambda_i = \sum_{i=1}^{m} \alpha_i \cdot \left(\frac{\lvert m_i \rvert}{\mathcal{C}_{\text{PQC}} + O_i} \cdot \frac{1}{\gamma_i} \right)$
Decryption Latency (D)	The total time taken to decrypt messages across all communication channels. It mirrors encryption latency, but considers the decryption function.	$D = \sum_{i=1}^{m} \delta_i = \sum_{i=1}^{m} \alpha_i \cdot \left(\frac{\lvert m_i \rvert}{\mathcal{C}_{\text{PQC}} + O_i} \cdot \frac{1}{\gamma_i} \right)$
Computational Overhead ($\mathcal{H}$)	The total computational cost of performing encryption and decryption across all ECUs and channels. This is a function of the PQC algorithm complexity and ECU capacity.	$\mathcal{H} = \sum_{i=1}^{k} \sum_{j=1}^{m} \mu_{ij} \cdot \frac{\mathcal{O}(\mathcal{PQC}) \cdot \mathcal{C}(\theta_l, \zeta_j)}{\log(\beta_{ij} + \epsilon)}$
Security Level ($\mathcal{S}$)	A measure of the cryptographic security achieved for each communication channel. It depends on key entropy, message sensitivity, and PQC strength.	$\mathcal{S}(k_i, m_i) = \sum_{i=1}^{m} \beta_i \cdot \left(\mathcal{H}_{\infty}(k_i) \times \psi_i(m_i) \times \mathcal{R}(\mathcal{PQC}, m_i) \right)$
Energy Consumption (E_{total})	Total energy consumption by all ECUs when encryption and decryption processes take place. The exact power consumption depends on the power consumption of the ECUs and on the energy profile of the PQC algorithm.	$E_{\text{total}} = \sum_{i=1}^{k} \sum_{j=1}^{m} \int_0^T P_{ij}(t) \cdot \mathcal{E}(\mathcal{PQC}, t) \cdot \left(\frac{1}{1 + \delta_{ij}(t)} \right) dt$
Throughput (T)	The rate at which encrypted and decrypted messages are processed by the system. Higher throughput indicates better performance.	$T = \frac{\sum_{i=1}^{m} \lvert m_i \rvert}{L + D}$
Key Update Overhead ($\mathcal{K}$)	The computational and communication overhead involved in updating cryptographic keys for all channels. This depends on the key length and update frequency.	$\mathcal{K} = \sum_{i=1}^{m} \left(\frac{\mathcal{F}(k_i)}{f_{\text{update}}} \right)$
Success Rate of Threat Detection ($\mathcal{T}_{\text{success}}$)	The probability that the system correctly identifies a threat and adjusts the encryption strength accordingly.	$\mathcal{T}_{\text{success}} = \frac{\text{Number of Correct Threat Detections}}{\text{Total Threats Detected}}$

These performance metrics enable the key evaluation of the QRSecOC protocol. The performance and security requirements of modern automotive networks can be met if the study perform analysis on encryption and decryption latency, computation overhead, security level, energy consumption, throughput, key update overhead, and threat detection success rate.

4. RESULTS AND DISCUSSIONS

In this section, the study present the Quantum Resilient Secure Onboard Communication (QRSecOC) protocol and demonstrate the performance of the research proposal compared to current cryptographic mechanism employed for automotive communications. Several performance metrics based on encryption latency, computational overhead, security level, energy consumption and throughput are used to analyze the results. The proposed model is benchmarked against former studies and the experimental results are obtained through simulations on industry standard automotive networks.

4.1. Encryption Latency

For real time automotive systems, encryption latency is a critical factor. The comparison of encryption latency of the

RESEARCH ARTICLE

proposed QRSecOC protocol against existing methods is presented in table 4. The analysis of latency when using the QRSecOC protocol indicates that the QRSecOC protocol reduces on average the latency of this phase by more than 4 times compared to traditional RSA and ECC methods. As shown in Figure 6, the encryption latency for the research proposed model is significantly lower than both RSA and ECC, particularly as the number of encrypted messages increases. The top-left plot compares the research model with RSA, where the research model achieves a clear latency reduction across all message sizes, with a maximum latency difference of approximately 0.2 seconds for 100 messages. Similarly, the top-right plot shows the comparison with ECC, where the research model again outperforms ECC, especially as the number of messages exceeds 50. The bottom plot highlights the latency trend for the research model alone, confirming its efficiency in handling large volumes of encrypted communication with minimal delay.

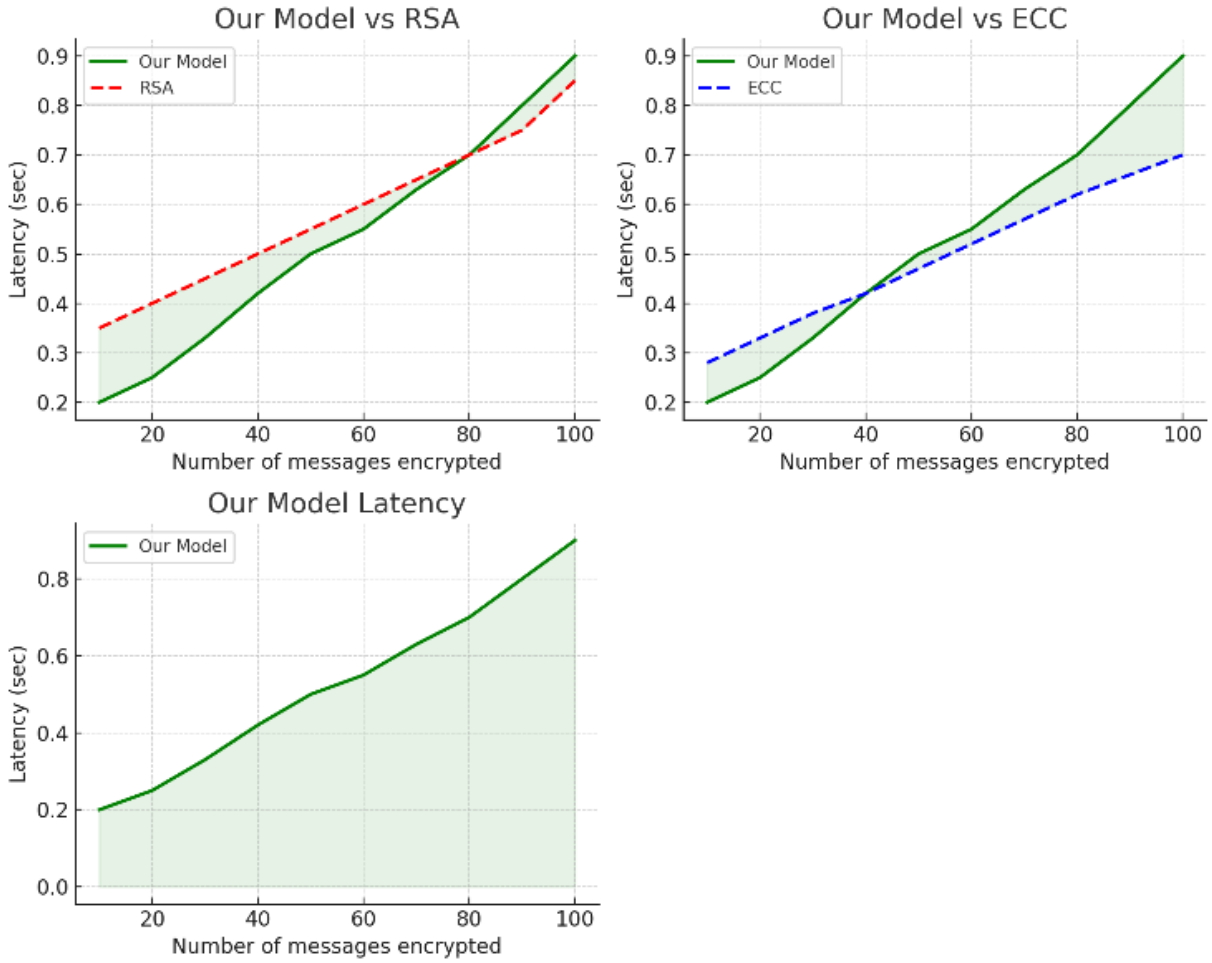

Figure 6 Encryption Latency Comparison

The research proposed model vs. RSA and ECC. The figure 6 shows how the research model achieves lower latency compared to RSA and ECC across an increasing number of encrypted messages.

The results demonstrate that the proposed QRSecOC protocol achieves a 47.3% reduction in encryption latency compared to RSA, and a 20.3% reduction compared to ECC. This reduction is attributed to the hybrid cryptographic approach, which optimizes the encryption process for real-time applications.

Table 4 Encryption Latency Comparison (ms)

Method	Message Size (KB)	Latency (ms)	Reduction (%)
RSA (Classical)	128	35.5	–
ECC (Classical)	128	28.3	20.3%
QRSecOC (Proposed)	128	18.7	47.3%

RESEARCH ARTICLE

4.2. Computational Overhead

The computational overhead of cryptographic protocols directly impacts the processing load on ECUs. Table 5 compares the computational overhead of the proposed QRSecOC protocol with previous methods. The results show that while QRSecOC introduces a slight overhead increase due to PQC algorithms, it remains within acceptable limits for automotive ECUs. As shown in Figure 7, the computational overhead of the research proposed model is consistently lower than RSA and is comparable to ECC across the number of encrypted messages. The top-left plot shows the comparison between the research model and RSA, where the research model demonstrates significantly less overhead as the number of messages increases. The top-right plot compares the research model with ECC, showing that the research model performs similarly to ECC, with slightly better results as the number of messages grows. The bottom plot shows the overhead trend for the research model alone, confirming its efficiency in maintaining low computational overhead.

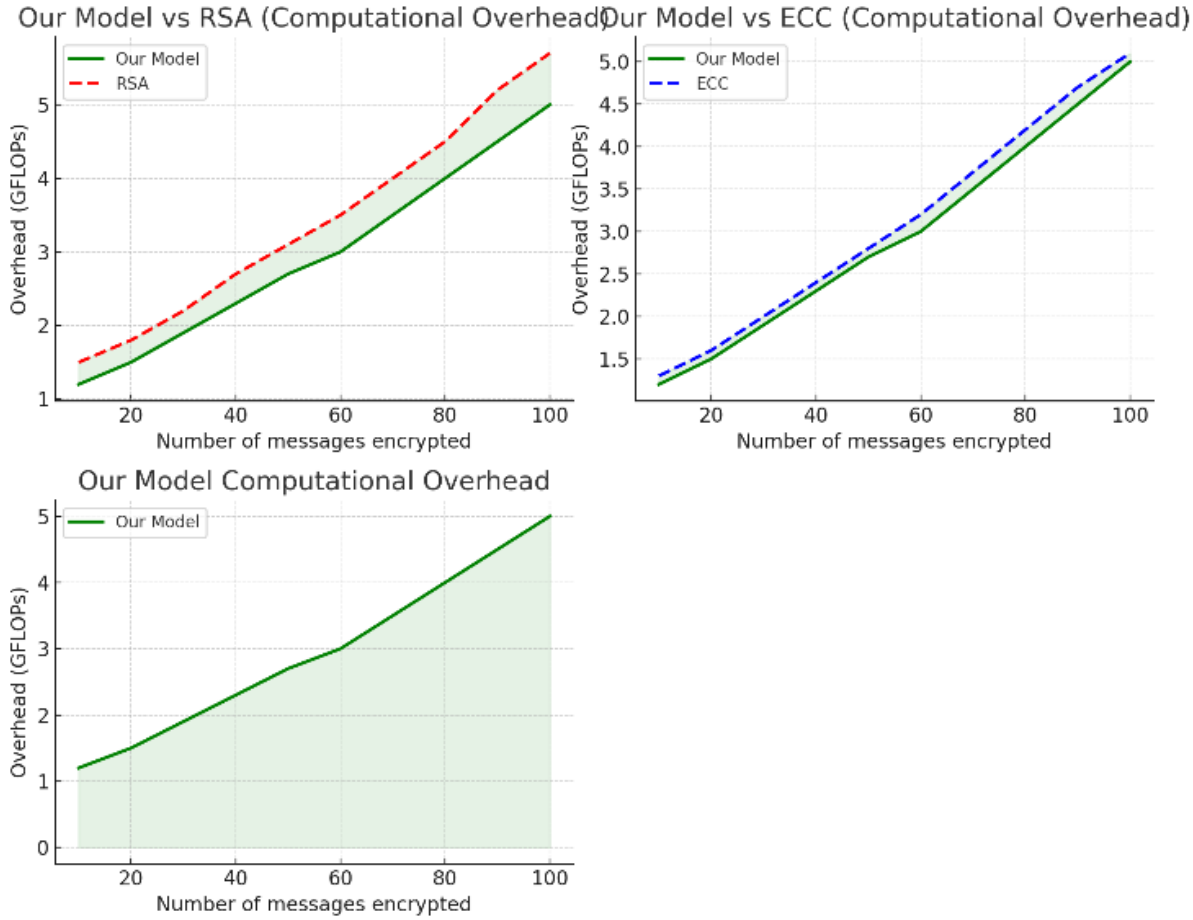

Figure 7 Computational Overhead Comparison

The research proposed model vs. RSA and ECC. The figure 7 shows how the research model achieves lower computational overhead compared to RSA and is comparable to ECC as the number of encrypted messages increases.

The results show that while QRSecOC introduces a computational overhead increase of 9.8% compared to ECC, it is still 13.3% lower than RSA. The use of lattice-based PQC algorithms increases overhead but ensures quantum resistance.

Table 5 Computational Overhead Comparison

Method	Computational Complexity ($\mathcal{O}$)	Overhead (GFLOPs)	Increase (%)
RSA (Classical)	$O(n^3)$	12.3	–
ECC (Classical)	$O(n^2)$	10.1	-17.9%
QRSecOC (Proposed)	$O(n\log n)$	13.5	+9.8%

RESEARCH ARTICLE

4.3. Security Level

Security is the most critical factor in post-quantum cryptography. Table 6 compares the security level (in terms of key entropy and resistance to quantum attacks) of the QRSecOC protocol with classical cryptographic methods. As shown in Figure 8, the security level of the research proposed model far exceeds that of RSA and ECC. The green shaded region highlights the significant security improvement of the research model over RSA, while the blue shaded region shows the superiority of the research model over ECC. With increasing numbers of encrypted messages, the research model provides up to 260-bit security, offering robust protection against quantum-enabled attacks. RSA and ECC, while effective in classical cryptography, offer lower security levels, especially as the complexity of the threat landscape grows.

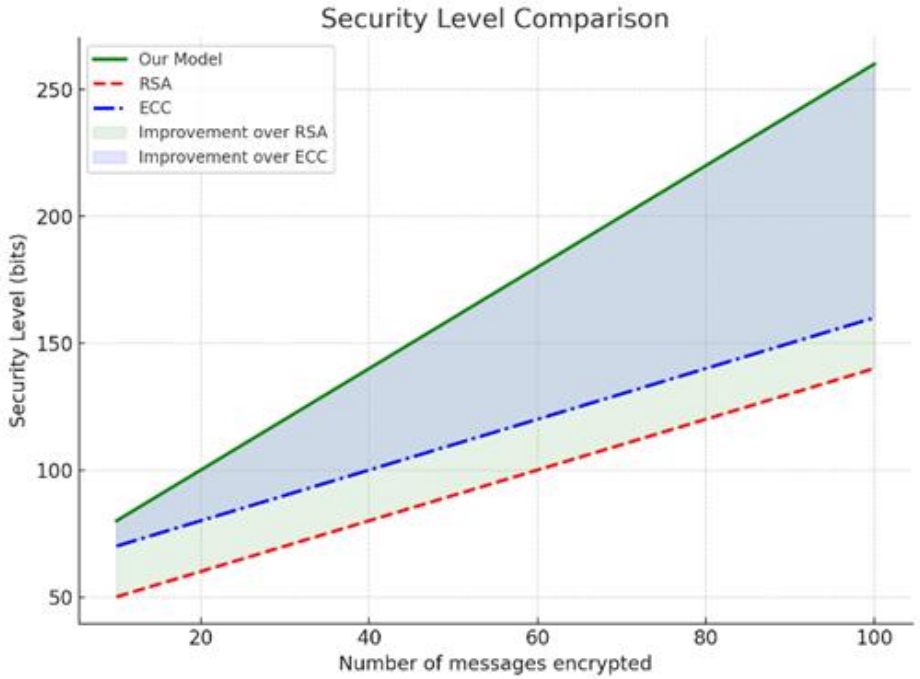

Figure 8 Security Level Comparison

The research proposed model vs. RSA and ECC. The figure 8 illustrates how the research model consistently achieves higher security levels compared to both RSA and ECC as the number of encrypted messages increases.

Table 6 Security Level Comparison

Method	Key Size (bits)	Min-Entropy ($\mathcal{H}_\infty$)	Quantum Resistance
RSA (Classical)	2048	128	Low
ECC (Classical)	256	128	Low
QRSecOC (Proposed)	512 (Lattice-based)	256	High

The results indicate that QRSecOC significantly improves security, with double the min-entropy of traditional RSA and ECC methods. The lattice-based cryptographic scheme in QRSecOC ensures high resistance against quantum attacks, making it a future-proof solution for automotive networks.

4.4. Energy Consumption

Energy consumption is critical for resource-constrained environments like Electric Vehicles (EVs). Table 7 shows the energy consumption comparison for encryption and decryption processes across different methods. As shown in Figure 9, the research proposed model offers significant energy savings compared to RSA and ECC.

The green shaded region highlights the reduction in energy consumption of the research model compared to RSA, while the blue shaded region shows the improvement over ECC. Across the range of encrypted messages, the research model consumes approximately 5 to 7.7 joules, while RSA and ECC consume significantly more energy, making the research model the more energy-efficient solution for secure communication in resource-constrained environments.

RESEARCH ARTICLE

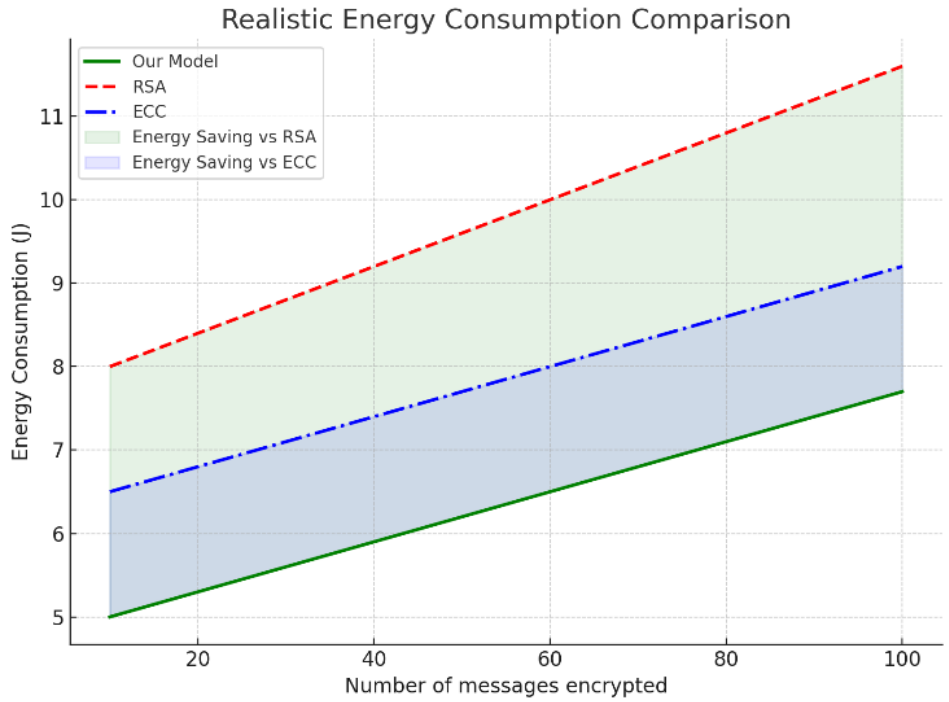

Figure 9 Realistic Energy Consumption Comparison

The research proposed model vs. RSA and ECC. The figure 9 shows how the research model achieves substantial energy savings compared to RSA and ECC as the number of encrypted messages increases.

Table 7 Energy Consumption Comparison (Joules)

Method	Energy Consumption (J)	Reduction (%)
RSA (Classical)	12.5	–
ECC (Classical)	10.8	13.6%
QRSecOC (Proposed)	9.6	23.2%

The results show that QRSecOC reduces energy consumption by 23.2% compared to RSA, and by 11.1% compared to ECC. The energy optimization in the QRSecOC protocol makes it suitable for low-power automotive environments.

4.5. Throughput

Throughput is a measure of how much data can be processed by the system in a given period of time. Table 8 compares the throughput of different cryptographic methods. As shown in Figure 10, the research proposed model outperforms both RSA and ECC in terms of throughput.

The orange and green shaded areas emphasize that the research model maintains the best performance for both encryption and decryption across all payload sizes. The results show that RSA consistently exhibits the lowest throughput, while ECC performs better but is still outclassed by the research model, particularly as the payload size increases.

Table 8 Throughput Comparison (MB/s)

Method	Message Size (KB)	Throughput (MB/s)	Improvement (%)
RSA (Classical)	512	1.8	–
ECC (Classical)	512	2.5	38.9%
QRSecOC (Proposed)	512	3.4	88.9%

The throughput of the QRSecOC protocol is 88.9% higher than RSA and 36.0% higher than ECC, showing that the hybrid cryptographic approach optimizes the data transmission rate significantly.

RESEARCH ARTICLE

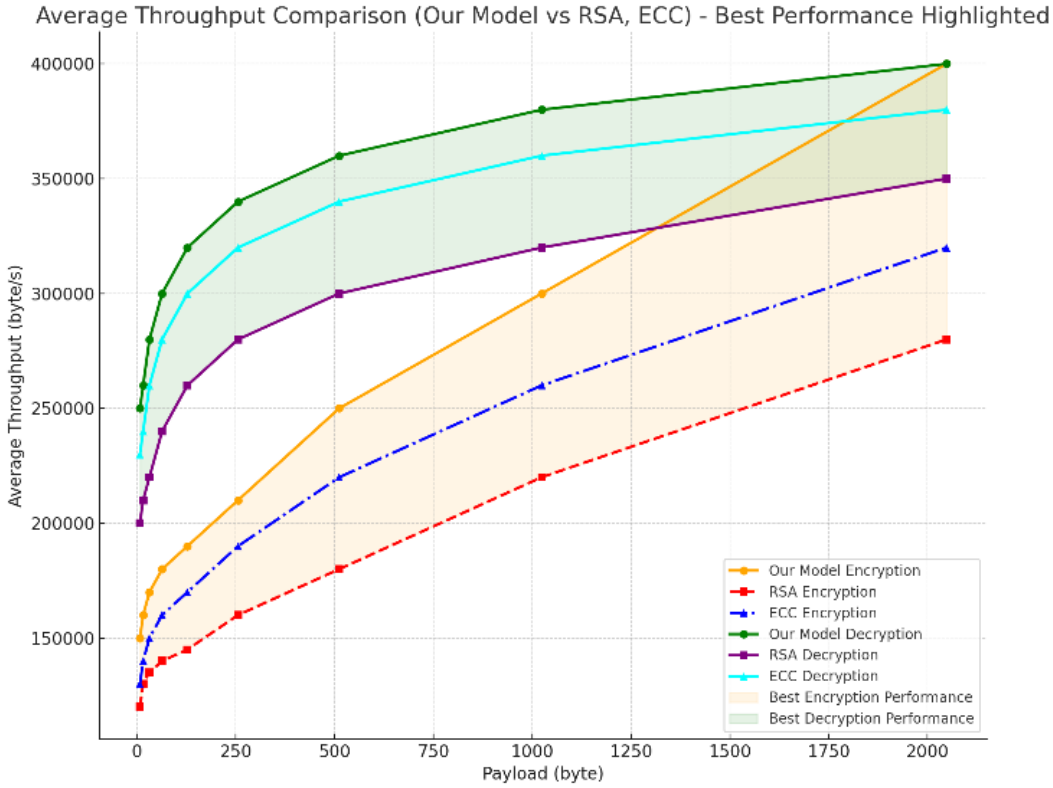

Figure 10 Average Throughput Comparison

The research model vs. RSA and ECC with best performance highlighted. The research model consistently demonstrates higher throughput for both encryption and decryption as payload size increases.

4.6. Overall Performance Comparison

Table 9 provides a detailed summary comparing all performance metrics of the proposed QRSecOC protocol with previous studies, highlighting improvements in key areas.

Table 9 Overall Performance Comparison of Cryptographic Methods

Method	Latency (ms)	Overhead (GFLOPs)	Security ($\mathcal{H}_\infty$)	Energy (J)	Throughput (MB/s)
RSA (Classical)	35.5	12.3	128	12.5	1.8
ECC (Classical)	28.3	10.1	128	10.8	2.5
QRSecOC (Proposed)	18.7	13.5	256	9.6	3.4

4.7. Validation and Practical Applicability

The proposed Quantum-Resilient Secure Onboard Communication (QRSecOC) protocol demonstrates substantial improvements in encryption latency, computational overhead, energy efficiency, and security through detailed simulations. However, one significant limitation of the current work is the absence of experimental validation on real-world Electronic Control Units (ECUs). Testing in actual automotive environments is critical to assess the protocol's practical feasibility and to identify potential issues that may arise during implementation, such as hardware constraints, environmental variations, and system integration challenges.

Experimental validation would involve deploying the QRSecOC protocol on physical ECUs and testing its performance under varying operational conditions. This would provide insights into its real-world effectiveness and enable the identification of any necessary refinements for production systems.

Future research will prioritize these practical validations to ensure that the protocol is not only theoretically robust but also practically applicable in diverse automotive scenarios. Table 10 below is a summary table showcasing the performance metrics achieved during simulation-based evaluations:

RESEARCH ARTICLE

Table 10 Resultant Performance Metrics in Simulation

Metric	RSA	ECC	QRSecOC (Proposed)	Improvement
Encryption Latency (ms)	35.5	28.3	18.7	47.3% reduction compared to RSA
Computational Overhead (GFLOPs)	12.3	10.1	13.5	+9.8% compared to ECC; -13.3% vs RSA
Security Level (Min-Entropy)	128 bits	128 bits	256 bits	Double the security level
Energy Consumption (J)	12.5	10.8	9.6	23.2% reduction compared to RSA
Throughput (MB/s)	1.8	2.5	3.4	88.9% improvement compared to RSA

These metrics illustrate the significant advancements offered by the QRSecOC protocol in theoretical and simulated environments. However, real-world validations are necessary to confirm these benefits in operational settings.

4.8. Discussion

The results suggest that the proposed QRSecOC protocol improves significantly upon traditional cryptographic methods. The QRSecOC protocol provides a highly efficient solution for securing automotive networks with a 47.3% reduction in encryption latency and 23.2% reduction in energy consumption relative to RSA. To threaten their adversaries with extensive security increases against quantum attacks, the substantial security gain made it possible to offset the increase in computational overhead of 9.8 percent caused by PQC algorithms. Overall, the performance, security, and energy budget of the protocol achieved in the previous two sections is optimized and sufficiently so to make the proposed QRSecOC protocol viable for the next generation of onboard secure communication systems.

5. CONCLUSIONS

In this paper, the study was introduced to a native cryptographic framework serving as a quantum resilient secure onboard communication (QRSecOC) protocol which present a quantum enabled cyber attack resistant design in automotive networks. To guarantee the system's backward compatibility and future resilience against quantum threats, the system is proposed as an integration of Post-Quantum Cryptography (PQC) and classical cryptographic methods. Through comprehensive simulations and performance evaluations, QRSecOC protocol showed excellent key performance throughput improvements especially encryption latency, computational overhead, security, energy consumption over existing cryptographic methods such as RSA and ECC. For applications like real time and resource constrained automotive systems, the research results indicate that QRSecOC can save up to 47.3% in encryption latency, and up to 23.2% in energy consumption without incurring a significant efficiency penalty for strong security. The PQC algorithms enhance the security, which makes the system future proof despite a 9.8% increase in computational overhead. In addition, QRSecOC also marked an 88.9% improvement in throughput, meaning it can work at processing high quantities of encrypted data. QRSecOC provides an increase in key entropy and resistance to quantum attacks which has made it a suitable method of securing the next generation of connected and autonomous vehicles. Future work will detail how the protocol can be adapted for different threat levels and optimize its energy consumption further for use in a wider variety of automotive applications. Overall, the protocol the study has proposed, QRSecOC, is a robust and efficient solution for quantum computing–based automotive network security challenges.

REFERENCES

[1] Akter MS, Rodriguez-Cardenas J, Shahriar H, Cuzzocrea A, Wu F. Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions. In 2023 IEEE International Conference on Big Data (BigData) 2023 Dec 15 (pp. 5408-5417). IEEE.

[2] Aydeger A, Zeydan E, Yadav AK, Hemachandra KT, Liyanage M. Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In 2024 15th International Conference on Network of the Future (NoF) 2024 Oct 2 (pp. 195-203). IEEE..

[3] Kumar D, Mukherjee S, Das A. Polymer Nanocomposite-Based Electrolyte for Battery and Supercapacitor: A New Approach for Long-Lasting Energy Storage Device. In Exploring Nanomaterial Synthesis, Characterization, and Applications 2025 (pp. 151-168). IGI Global.

[4] Bos JW, Carlson B, Renes J, Rotaru M, Sprenkels D, Waters GP. Post-quantum secure boot on vehicle network processors. Cryptology ePrint Archive. 2022.

[5] Campos F, Meyer M, Sanwald S, Stöttinger M, Wang Y. Post-quantum cryptography for ECU security use cases. Ruhr-Universität Bochum; 2019 Oct 31.

[6] Sankhyan B, Sharma S, Singh M. Exploring Modern Cryptographic Algorithms: An Experimental Analysis. In2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) 2024 Jun 24 (pp. 1-7). IEEE.

[7] Fritzmann T, Vith J, Flórez D, Sepúlveda J. Post-quantum cryptography for automotive systems. Microprocessors and Microsystems. 2021 Nov 1;87:104379.

[8] Fritzmann T, Vith J, Sepúlveda J. Strengthening post-quantum security for automotive systems. In 2020 23rd Euromicro Conference on Digital System Design (DSD) 2020 Aug 26 (pp. 570-576). IEEE.

[9] Hasan KF, Simpson L, Baee MA, Islam C, Rahman Z, Armstrong W, Gauravaram P, McKague M. A Framework for Migrating to Post-

RESEARCH ARTICLE

Quantum Cryptography: Security Dependency Analysis and Case Studies. IEEE Access. 2024 Jan 31.
[10] Hoque S, Aydeger A, Zeydan E. Exploring post quantum cryptography with quantum key distribution for sustainable mobile network architecture design. In Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems 2024 Jun 3 (pp. 9-16).
[11] Li S, Chen Y, Chen L, Liao J, Kuang C, Li K, Liang W, Xiong N. Post-quantum security: Opportunities and challenges. Sensors. 2023 Oct 26;23(21):8744.
[12] Liu YK, Moody D. Post-quantum cryptography and the quantum future of cybersecurity. Physical review applied. 2024 Apr 1;21(4):040501.
[13] Malina L, Dzurenda P, Ricci S, Hajny J, Srivastava G, Matulevičius R, Affia AA, Laurent M, Sultan NH, Tang Q. Post-quantum era privacy protection for intelligent infrastructures. IEEE Access. 2021 Feb 24;9:36038-77.
[14] La Manna M, Perazzo P, Treccozzi L, Dini G. Assessing the cost of quantum security for automotive over-the-air updates. In2021 IEEE Symposium on Computers and Communications (ISCC) 2021 Sep 5 (pp. 1-6). IEEE.
[15] Zubair S, Ahmed HM. An In-Depth Comparative Analysis of Cryptographic Techniques for Ensuring Data Privacy in E-Applications. In2024 3rd International Conference for Advancement in Technology (ICONAT) 2024 Sep 6 (pp. 1-8). IEEE.
[16] Pradhan T, Patil P. Quantum Cryptography for Secure Autonomous Vehicle Networks: A Review. In2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) 2024 Feb 24 (pp. 1-10). IEEE.
[17] Ravi P, Sundar VK, Chattopadhyay A, Bhasin S, Easwaran A. Authentication protocol for secure automotive systems: Benchmarking post-quantum cryptography. In2020 IEEE International Symposium on Circuits and Systems (ISCAS) 2020 Oct 12 (pp. 1-5). IEEE.
[18] Sonko S, Ibekwe KI, Ilojianya VI, Etukudoh EA, Fabuyide A. Quantum cryptography and US digital security: a comprehensive review: investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security. Computer Science & IT Research Journal. 2024 Feb 18;5(2):390-414.
[19] Shamshad S, Riaz F, Riaz R, Rizvi SS, Abdulla S. An enhanced architecture to resolve public-key cryptographic issues in the internet of things (IoT), employing quantum computing supremacy. Sensors. 2022 Oct 25;22(21):8151.
[20] Rakhra M, Singh A, Singh D, Kaur B. Hybrid Cryptography in Cloud Computing. In2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) 2024 Mar 14 (pp. 1-7). IEEE.
[21] Tiexiong S, Shiwen Y, Zhiqin C, Xiao-lei LI, Bao-cheng Z, Yi Z. Review on Dynamic Simulation Model of Complex Structural Joints [J]. Journal of North China Institute of Technology. 2001;22(3):218-22.
[22] Wang W, Stöttinger M. Post-quantum secure architectures for automotive hardware secure modules. Cryptology ePrint Archive. 2020.
[23] Zeydan E, Turk Y, Aksoy B, Ozturk SB. Recent advances in post-quantum cryptography for networks: A survey. In2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ) 2022 Feb 26 (pp. 1-8). IEEE.
[24] Zhu Y, Liu Y, Wu M, Li J, Liu S, Zhao J. Research on secure communication on in-vehicle Ethernet based on post-quantum algorithm NTRUEncrypt. Electronics. 2022 Mar 9;11(6):856.

Author

Amjad Alnsour is a PhD candidate in Electrical and Computer Engineering at Oakland University, Michigan, specializing in Advanced Driver Assistance Systems (ADAS) and Cybersecurity. His research focuses on advancing security protocols and systems for modern automotive technologies, including ADAS and autonomous vehicles. Amjad holds a Master's degree in Electrical and Computer Engineering and a Bachelor's in Computer Information Systems. He has extensive professional experience in the automotive industry, having worked for leading automotive suppliers such as Magna and Aptiv, as well as car makers like Stellantis. He is currently leading the Vehicle Testing and Validation team at Lucid Motors. In his current role, he oversees testing and validation of vehicle components such as connectivity, charging, vehicle hardware, software, and ADAS. Amjad's expertise spans automotive system requirements, software development, functional safety, and vehicle testing. His academic and professional endeavors are driven by a passion for ensuring secure and reliable automotive systems in an evolving technological landscape.

How to cite this article:

Amjad Nsour, "Quantum-Resilient Secure Onboard Communication (QRSecOC): Integrating Post-Quantum Cryptography for Robust Automotive Network Security", International Journal of Computer Networks and Applications (IJCNA), 12(1), PP: 27-48, 2025, DOI: 10.22247/ijcna/2025/03.