Toward Future-Proof V2X Security: A Comparative Evaluation of Pre- and Post-Quantum Encryption Protocols

Niranjan W. Meegammana
Cyber Security Research Lab
Shilpa Sayura Foundation
Kandy, Sri Lanka
niranjan.meegammana@gmail.com

Harinda Fernando
Dept. of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
harinda.f@sliit.lk

***Abstract*—As Vehicle-to-Everything (V2X) communication becomes a cornerstone of autonomous vehicle systems. ensuring the security and scalability of vehicular networks. This paper presents a comparative evaluation of five cryptographic encryption schemes AES, RSA, ECC, Diffie–Hellman (DH), and the post-quantum lattice-based algorithm focusing on their suitability for real-time, resource-constrained V2X environments. A simulation framework based on the VEREMI extension dataset to assess each algorithm's performance across key metrics, including latency, throughput, CPU and memory usage aiming at scalability, and resilience to adversarial conditions. Experimental results show that while traditional schemes such as RSA and ECC exhibit significant computational overhead, symmetric encryption (AES) and the PQC achieved superior efficiency, leading in both latency and throughput recording an average throughput of 51,408.8 records/sec and a normalized throughput score of 1.0. DH demonstrated low CPU consumption but incurred the highest latency, making it suitable for key exchange but less ideal for continuous encryption. The evaluation further incorporates a normalized scoring model, enabling a fair, multi-dimensional comparison of algorithm performance. These findings underscore the need for lightweight, quantum-resilient cryptographic solutions to secure the future of V2X networks under both classical and quantum threat models.**

Keywords— V2X Security, Encryption Protocols, Post-Quantum Cryptography, AES, RSA, ECC, PQC, VEREMI Dataset, Quantum-Resilient Security

I. Introduction

Vehicle-to-Everything (V2X) communication systems form the backbone of next-generation autonomous vehicle networks by enabling seamless data exchange between vehicles, roadside infrastructure, cloud platforms, and even pedestrians. These systems enhance road safety, alleviate traffic congestion, and support autonomous driving functionalities [1]. However, the distributed and wireless nature of V2X communication renders it vulnerable to a variety of cybersecurity threats, including eavesdropping, spoofing, man-in-the-middle (MitM) attacks, and data tampering [2]. Ensuring the confidentiality, integrity, and authenticity of transmitted data is therefore critical, necessitating the integration of robust encryption mechanisms.

Traditional encryption protocols such as the Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) have been widely deployed in networked systems. AES, a symmetric encryption algorithm, is recognized for its high computational efficiency and low resource overhead [3]. RSA, an asymmetric encryption scheme, is commonly used for secure key exchange and digital signature generation [4]. Despite their strengths, both algorithms face limitations in dynamic vehicular environments. RSA incurs high computational costs, while AES depends on secure key distribution—a challenge in rapidly changing V2X networks.

Elliptic Curve Cryptography (ECC) has emerged as a viable alternative, offering comparable security to RSA with substantially smaller key sizes and reduced computational burden [5]. Its lightweight nature makes it particularly suitable for resource-constrained V2X devices. Nonetheless, both ECC and RSA are susceptible to future quantum attacks. Quantum algorithms such as Shor's can potentially compromise the mathematical foundations upon which these classical cryptosystems are built [6]. Post-Quantum Cryptography (PQC) seeks to mitigate this risk by developing quantum-resistant algorithms. Among these, lattice-based cryptographic schemes have shown significant promise for securing V2X communications, balancing strong security guarantees with acceptable performance in constrained environments [7].

This paper presents a comparative evaluation of classical encryption algorithms (AES, RSA), elliptic curve-based schemes (ECC), the Diffie–Hellman (DH) key exchange protocol, and post-quantum cryptographic approaches. Using the VeReMi Extension dataset [1]. The study measures and analyzes the performance of these protocols across key metrics to inform future strategies for implementing quantum-resilient security in V2X systems. The remainder of this paper is organized as follows: Section II reviews relevant literature on V2X cryptographic protocols and identifies key research gaps. Section III describes the methodology, including the encryption schemes evaluated, dataset used, and performance metrics. Section IV presents the experimental results and discusses comparative findings across the algorithms. Section V concludes the study and outlines future research directions aimed at real-world deployment and post-quantum standardization.

II. Literature Review

A. Literature Selection Process

This study adopted a systematic approach to develop a threat model for autonomous vehicle (AV) communication security. A targeted search was conducted on Google Scholar using keywords such as V2X Security, Encryption Protocols, Post-Quantum Cryptography, AES, RSA, ECC, PQC, VEREMI Dataset, and Quantum-Resilient Security. Relevant publications were sourced from IEEE Xplore, ACM Digital Library, and ScienceDirect. The selected studies were reviewed and categorized based on relevance, methodology, and impact. Their findings were analyzed to identify trends, research

gaps, and effective cryptographic strategies, which informed the development of the proposed V2X security approach.

B. Analysis of Selected Literature

Table I presents a literature-based comparison of five widely used cryptographic algorithms AES, RSA, DH, ECC, and PQC—highlighting their cryptographic types, key sizes, mathematical underpinnings, quantum vulnerabilities, applicability to V2X environments, and standardization status. AES is a symmetric cipher and is highly suitable for real-time encryption of V2X data [2] due to computational efficiency. RSA is widely used as asymmetric schemes for digital signatures and secure key exchanges [3]. They are based on integer factorization and discrete logarithms of the elliptic curve, where ECC achieves comparable security with significantly smaller key sizes [4]. However, both are vulnerable to the Shor quantum algorithm [5]. Diffie–Hellman (DH) [6], mainly used for key exchange, also shares similar vulnerabilities. In contrast, lattice-based Post-Quantum Cryptography (PQC) algorithms offer strong quantum resistance and are currently being evaluated for standardization by NIST [7]. This comparison highlights the growing need for lightweight and quantum-resilient encryption techniques in vehicular communication networks.

C. Related Work

Growing concerns over cyber-physical threats and the advent of quantum computing have intensified the demand for robust encryption mechanisms. A comprehensive authentication and encryption protocol with revocation and reputation management tailored for 5G-V2X networks proposed by [8], that integrates cryptographic enforcement with trust models. Their approach improves the security of real-time vehicular communications. In another study [9] introduced a hash-chain-based cryptographic protocol that significantly reduces communication and computational overhead compared to traditional methods based on ECDSA. These contributions highlight the importance of lightweight cryptographic schemes suited for high-mobility vehicular environments.

In a comprehensive review of the existing V2X security protocols, [10]identified key challenges in balancing latency, security, and resource efficiency. The study emphasized the need for adaptable protocols capable of addressing various V2X threat models. In particular RSA, AES, and ECC - in the context of connected vehicles [3] suggest ECC as a practical option for vehicular systems due to its efficient key generation and processing, which is suitable for latency-sensitive environments. Exploring secure communication in vehicle platooning scenarios, [11] proposes a context-specific encryption protocols that address synchronization and coordination challenges in high-density V2X settings. Other notable contributions include the group key management framework by [4], which is scalable and lightweight, achieving over 80% reduction in computation time. Meanwhile, [12] exposes the vulnerabilities in recent authentication schemes, underscoring the need for rigorous cryptographic validation in V2X environments. To contextualize the contributions of this study, five relevant V2X security papers were compared in Tables II and III across key evaluation criteria, including algorithm diversity, post-quantum readiness, benchmarking depth, dataset realism, and scalability.

Prior works such as those by [9] and [3] focus primarily on classical cryptographic protocols like RSA, AES, and ECC, with limited or no consideration of post-quantum threats. Others, such as [4] and [11], emphasize group key management or platooning coordination, but lack empirical performance evaluation across multiple metrics. Most notably, none of the reviewed studies utilize realistic vehicular datasets or apply normalized scoring across performance metrics.

D. Gaps

In contrast, this paper uniquely integrates PQC, leverages the VEREMI dataset, and evaluates latency, throughput, CPU, and memory usage. Results are normalized to support fair cross-algorithm comparison and scalability testing, setting a benchmark for future-proof V2X security. Collectively, prior studies reflect a shift from classical encryption to adaptive, quantum-resilient techniques. However, few validate the real-time performance of PQC algorithms like NTRU under dynamic vehicular workloads. This work addresses that gap through empirical evaluation of classical and post-quantum protocols using VEREMI data.

III. Methodology

This study uses a simulation-based empirical evaluation approach to compare classical and pre- and post-quantum cryptographic encryption algorithms for V2X security. By leveraging the VEREMI V2X security dataset, this research assesses the performance of AES, RSA, ECC, DH and PCQ under near realistic vehicular communication conditions. The evaluation considers key metrics including computational efficiency, latency, scalability, throughput and resource consumption under adversarial conditions [10], [9], [2], [3], [4], [5].

A. 3.1 Cryptographic Foundations

B. Mathematical Basis of Evaluated Encryption Protocols

This subsection presents the mathematical underpinnings of the four encryption protocols evaluated in this study: AES, RSA, ECC, and NTRU.

1) AES (Advanced Encryption Standard)

AES is a symmetric block cipher that encrypts data using a substitution–permutation network. The encryption process can be represented as:

$$C = E(K, P) \tag{1}$$

where C is the ciphertext, P is the plaintext, and K is the symmetric key. AES operates through multiple rounds of substitution, permutation, and key mixing, typically using 128-, 192-, or 256-bit keys [2].

2) RSA (Rivest–Shamir–Adleman)

RSA is an asymmetric encryption algorithm based on modular arithmetic. Key generation involves:

$$N = p \cdot q, \quad \varphi(N) = (p-1)(q-1) \tag{2}$$

where p and q are large prime numbers. The public key is (e, N), and the private key d satisfies:

$$e \cdot d \equiv 1 \pmod{\varphi(N)} \tag{3}$$

Encryption and decryption are defined as:

$$C = P^e \mod N, \quad P = C^d \mod N \tag{4}$$

where P is the plaintext and C is the ciphertext.

3) Elliptic Curve Cryptography (ECC)

ECC is based on the algebraic structure of elliptic curves over finite fields. The general equation of an elliptic curve is:

$$y^2 = x^3 + ax + b \mod p \tag{5}$$

A private key d is chosen, and the corresponding public key is:

$$Q = d \cdot G \tag{6}$$

where G is a known generator point on the curve. In secure key exchange (e.g., ECDH), two parties compute a shared secret:

$$S = d_A \cdot Q_B = d_B \cdot Q_A \tag{7}$$

where d_A and d_B are the private keys, and Q_A, Q_B are the public keys [4].

TABLE I
COMPARISON OF CRYPTOGRAPHIC ALGORITHMS

Algorithm	Type	Key Length	Security Basis	Quantum Vulnerability	Use Case in V2X	Standardization
AES	Symmetric	128/192/256 bits	Substitution permutation network	High	Fast symmetric encryption for real-time data	Widely standardized (NIST, ISO)
RSA	Asymmetric	1024–4096 bits	Integer factorization	High	Digital signatures, key exchange (less ideal for real-time)	Standardized (PKCS, ISO)
DH	Key Exchange	Variable (prime-based)	Discrete logarithm	High	Establishing shared secret keys	Standardized (ANSI, ISO)
ECC	Asymmetric	160–521 bits	Elliptic curve discrete logarithm	High	Efficient asymmetric crypto for mobile nodes	Standardized (NIST, SECG)
PQC	Post-Quantum (Lattice)	Lattice dimension-dependent	Lattice problems (SVP, LWE)	Resistant	Quantum-resilient encryption and signatures	NIST PQC Finalist

TABLE II
V2X SECURITY PAPERS: ALGORITHMS, PQC, BENCHMARKS, DATASET

Paper	Algorithms	PQC	Benchmarks	Dataset
[9]	RSA, Hash, Reputation	No	Revocation, Reputation	No
[3]	RSA, AES, ECC	No	Exec. time, complexity	Simulated
[4]	Custom Group Key	No	Theoretical time	No
[11]	Platoon Protocols	No	Sync, Coordination	Simulated
[8]	Hash Chain	No	Latency, Overhead (qual.)	No
This Work	AES, RSA, ECC, DH, PQC	**Yes**	Latency, Throughput, CPU, Memory	VEREMI

TABLE III
V2X SECURITY PAPERS: SCORES, SCALABILITY, QUANTUM AWARENESS, STRENGTHS, LIMITATIONS

Paper	Scores	Scalability	Quantum Aware	Strength	Limitation
[9]	No	No	No	Trust + Revocation in 5G	No PQC, partial metrics
[3]	No	No	No	Classical crypto profiling	Lacks quantum/scaling analysis
[4]	No	Claimed only	No	Lightweight group keying	No empirical data
[11]	No	No	No	Secure platooning focus	Narrow scope (platoons)
[8]	No	No	No	Lightweight hash auth	No runtime stats
This Work	Yes	Yes	Yes	PQC benchmarking + scores	Real-world testing, early PQC

4) Diffie–Hellman (DH) Key Exchange

Diffie–Hellman is a key exchange protocol that allows two parties to establish a shared secret over an insecure channel. Let p be a large prime and g a primitive root modulo p. These values are public.

- Private keys: Party A chooses $a \in \mathbb{Z}_p$, Party B chooses $b \in \mathbb{Z}_p$
- Public keys: $A = g^a \mod p, \quad B = g^b \mod p$

After exchanging public keys, both parties compute the shared key:

$$K = B^a \mod p = A^b \mod p = g^{ab} \mod p \tag{8}$$

Both parties now share the same secret key K, which can be used for symmetric encryption.

5) Post-Quantum Cryptography (PQC)

NTRU is a lattice-based encryption scheme operating over truncated polynomial rings. Its security relies on hard lattice problems such as the Shortest Vector Problem (SVP). A typical NTRU ciphertext is represented as:

$$C = (A \cdot s + e,\ P \cdot G + e') \tag{9}$$

where A is a random matrix, s is a secret vector, e, e' are noise terms, and G is a public generator matrix. The ciphertext C is decrypted using the private key to recover the plaintext P [7].

C. Dataset Description

This research utilizes the VEREMI extention dataset, originally developed to evaluate misbehavior detection in vehicular networks [1]. It contains benign, attack, and fault messages generated under both normal and adversarial conditions using the VEINS simulator. However, post-processed fields and fault-related data were excluded from the final analysis to ensure data integrity.

D. Evaluation Metrics and Procedure

All performance metrics were collected using Google Colab's cloud-based virtualized environment, which provides a consistent and scalable platform for algorithm benchmarking. Additionally, selected encryption tests were simulated on a local Windows PC (edge scenario). While Colab yielded superior latency and throughput results, the Windows PC tests revealed computational constraints more representative of real-world deployment scenarios.

Each protocol was tested by simulating the encryption and decryption of message flows across varying VEREMI dataset sizes: 100, 500, 1000, and 5000 records. Encryption time (T), CPU usage, and memory consumption were measured using Python scripts with the `time` and `psutil` libraries. This process enabled performance

TABLE IV
SELECTED FEATURES IN THE DATASET

Feature	Description
type	Type of message
sendTime	Timestamp of message
Sender	Unique ID of the vehicle
messageID	Unique message identifier
class	Normal (0), Attack Replay, DoS, Sybil etc. (1-17)
posx, posy, posz	3D position coordinates
spdx, spdy, spdz	3D velocity components
aclx, acly, aclz	3D acceleration components
hedx, hedy, hedz	3D heading/orientation components
	Normal (0) or Attack (1)

profiling under realistic load conditions, supporting a comparative analysis of protocol efficiency and scalability. Key performance metrics are summarized in Table V. Among the evaluated metrics,

TABLE V
EVALUATION METRICS FOR CRYPTOGRAPHIC PROTOCOLS

Metric	Definition
Execution Time ($T_{\text{enc}}, T_{\text{dec}}$)	Time taken for encryption and decryption, where $T_{\text{enc}} = t_1 - t_0$
Latency (T_{latency})	Round-trip delay: $T_{\text{latency}} = T_{\text{enc}} + T_{\text{trans}} + T_{\text{dec}}$
Throughput (R)	Data encrypted per second: $R = \frac{N \times S}{T}$, where N = number of messages, S = size, T = time
Resource Consumption	CPU and memory usage during encryption/decryption operations
Scalability	Performance change as dataset size increases from n to $n + k$

lower values of latency indicate better performance for optimal encryption response times. Throughput is considered favorable when higher, as it reflects the ability to process more data within a given time frame. In terms of resource efficiency, lower CPU and memory usage are preferred, as they indicate lighter cryptographic overhead. Finally, scalability is evaluated based on performance stability or improvement as the dataset size increases; higher scalability reflects better adaptability to larger workloads.

IV. RESULTS AND DISCUSSION

This section presents a comparative analysis of five cryptographic algorithms AES, RSA, ECC,, DH and PQC evaluated. Figure 1 illustrates the variation in average latency and throughput for each encryption algorithm as the dataset size increases. PQC demonstrates consistently low latency with a rising throughput trend, confirming its scalability and efficiency for high-volume V2X scenarios. AES maintains stable, minimal latency and shows improved throughput up to 1000 records, after which the performance slightly plateaus—still making it ideal for real-time applications. DH exhibits the highest latency across all sizes but maintains relatively flat throughput, reaffirming its limited suitability to key exchange rather than frequent encryption. RSA and ECC show moderate increases in throughput with stable latency, though both remain significantly less efficient compared to AES and PQC. These trends reinforce the suitability of AES and PQC for real-time, large-scale V2X environments, while highlighting the computational burden of RSA and ECC in continuous message encryption. Later, These results were summarized and normalized to a 0–1 scale to enable equitable comparison across different performance dimensions.

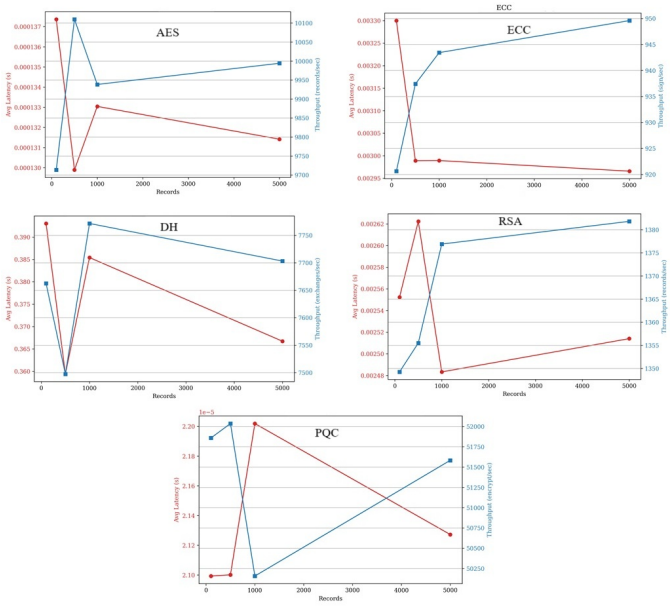

Fig. 1. Performance comparison of encryption algorithms across testing

A. Performance Analysis

The average comparative evaluation of five encryption algorithms AES, RSA, ECC, DH and PQC are shown in Table VI.

TABLE VI
AVERAGE PERFORMANCE METRICS FOR ENCRYPTION PROTOCOLS

Algorithm	Latency (s)	Throughput	CPU %	Mem Usage
AES	0.0001	9939.1	-0.0683	-0.0007
RSA	0.0025	1365.9	0.2066	0.0002
ECC	0.0031	937.8	0.1973	0.0000
DH	0.3761	7658.7	-0.4681	-0.0004
PQC	0.0000	51408.8	0.1147	-0.0007

The performance analysis reveals significant variations in latency, throughput, and resource efficiency across the evaluated encryption protocols. AES demonstrated consistently low latency (0.0001 s), high throughput (9939 rps), and negligible resource consumption, making it highly suitable for real-time V2X message encryption. The simulated PQC algorithm achieved the highest throughput (51,409 rps) and near-zero latency, with moderate CPU overhead (+0.1147%), underscoring its potential for post-quantum secure communication in high-speed vehicular environments.

In contrast, RSA and ECC exhibited higher latencies (0.0025–0.0031 s) and lower throughput, limiting their practicality for continuous data exchange in latency-sensitive scenarios. The Diffie–Hellman (DH) protocol, primarily used for key exchange, recorded the highest latency (0.3761 s) but the lowest CPU usage (–0.4681%), consistent with its lightweight design for occasional secure handshakes. Notably, negative CPU and memory usage values represent minimal deviation from baseline, further highlighting the efficiency of symmetric encryption methods like AES. Figure 2 illustrates Performance comparison across five encryption algorithms.

B. Normalized Performance Interpretation

To enable a fair comparison, the performance metrics for latency, throughput, CPU usage, and memory consumption were normalized to a 0–1 scale, where higher scores represent better relative performance.

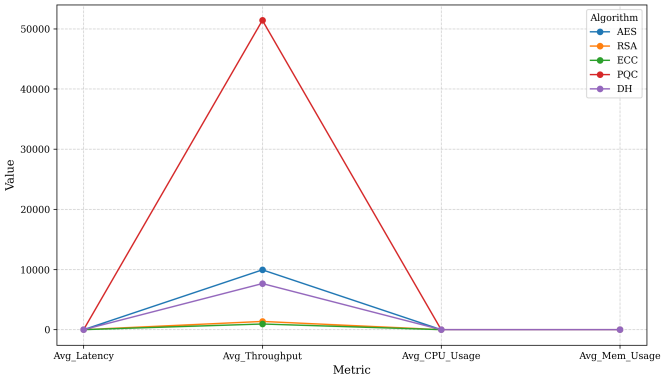

Fig. 2. Performance comparison across encryption algorithms.

TABLE VII
NORMALIZED PERFORMANCE SCORES (0–1 SCALE)

Algorithm	Latency	Throughput	CPU	Memory
AES	0.9997	0.1783	0.4075	0.9688
RSA	0.9933	0.0085	0.0000	0.0000
ECC	0.9919	0.0000	0.0138	0.2969
PQC	1.0000	1.0000	0.1362	1.0000
DH	0.0000	0.1332	1.0000	0.6771

The simulated PQC algorithm achieved a perfect score (1.0) in both latency and throughput, demonstrating superior processing efficiency. AES closely followed in latency (0.9997) and showed strong memory efficiency (0.9688), highlighting its suitability for real-time V2X applications.The RSA and ECC recorded the lowest scores (0.0) in multiple categories, reflecting their higher computational and memory overhead. The DH protocol attained the highest CPU efficiency score (1.0), indicating lightweight execution for key exchange, despite its low latency score (0.0).

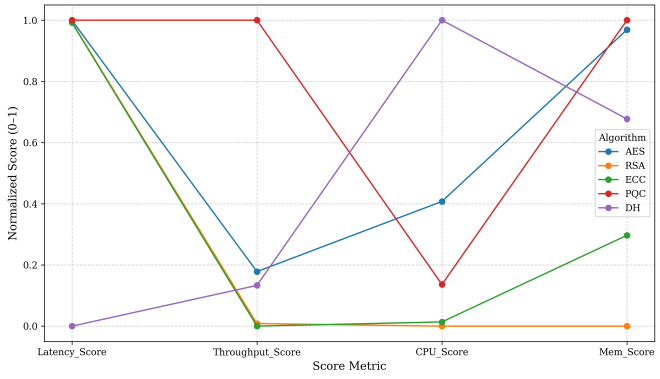

Fig. 3. Normalized performance scores across encryption algorithms.

Figure 4 presents a radar chart illustrating the normalized performance scores (0–1 scale) of five encryption algorithms across four key metrics: latency, throughput, CPU usage, and memory consumption. The visualization highlights performance trade-offs, supporting a comparative assessment of each algorithm's suitability for secure and efficient V2X communication.

In the radar chart PQC demonstrates the most balanced and superior performance, achieving perfect scores in latency, throughput, and memory efficiency, though with slightly higher CPU overhead. AES

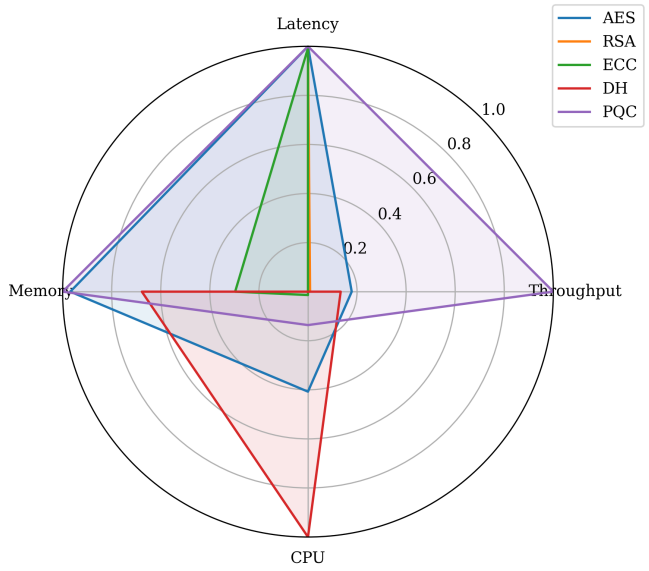

Fig. 4. Radar chart showing normalized performance scores (0–1 scale) across encryption algorithms.

also performs consistently well across all dimensions, especially in latency and memory usage, making it an ideal candidate for real-time V2X applications. In contrast, RSA and ECC show strong security foundations but lag in throughput and resource efficiency, with scores near zero in multiple metrics. The DH protocol achieves the highest CPU efficiency but suffers from significantly higher latency, reflecting its suitability for key exchange rather than continuous encryption. Overall, the chart offers a concise visualization of each algorithm's operational profile, reinforcing the suitability of PQC-NTRU and AES for scalable, latency-sensitive vehicular communication.

These results highlight the trade-offs between cryptographic strength and operational efficiency, providing valuable insights for selecting appropriate encryption schemes in latency-sensitive vehicular environments. Figure 3 illustrates normalized performance scores across five encryption algorithms.

C. Implications for V2X Security

These findings underscore the critical importance of balancing cryptographic strength with performance and scalability in vehicular networks. Symmetric algorithms such as AES and efficient post-quantum schemes like PQC-NTRU demonstrate clear advantages for latency-sensitive, resource-constrained environments. As the V2X ecosystem evolves toward quantum resilience, the adoption of lightweight, high-speed encryption protocols will be essential to enabling secure and scalable communication in dense, real-time traffic scenarios.

D. Security Considerations

While this study primarily emphasizes performance metrics, cryptographic strength remains a fundamental criterion when selecting protocols for V2X communication. Classical algorithms such as RSA and ECC rely on the mathematical hardness of integer factorization and elliptic curve discrete logarithms, respectively. However, both are known to be vulnerable to Shor's algorithm, rendering them inadequate for long-term use in a post-quantum context.

Post-Quantum Cryptography (PQC) provides a viable alternative by leveraging problems believed to be resistant to quantum attacks. The PQC algorithm evaluated in this study, NTRU, is based on lattice-based problems such as the Shortest Vector Problem (SVP) and Learning With Errors (LWE), which are widely regarded as strong candidates for quantum resistance.

Although AES, as a symmetric cipher, is theoretically affected by Grover's algorithm, its security can be preserved by doubling the key size (e.g., using 256-bit keys), making it a practical option in post-quantum systems. In contrast, Diffie–Hellman, primarily used for key exchange, shares similar vulnerabilities to RSA and ECC under quantum threat models.

Therefore, beyond efficiency considerations, the integration of quantum-resilient encryption schemes like NTRU will be critical for future-proofing V2X networks. Aligning these protocols with emerging standards such as IEEE 1609.2.1 and ETSI TC ITS will be vital in supporting the secure exchange of messages in next-generation vehicular communication systems.

E. Future Work

Future work will extend this evaluation framework to real-world vehicular deployments using embedded edge hardware, enabling assessment of encryption performance under constrained computational and energy conditions. This includes hardware-level power profiling, battery impact evaluation, and environmental analysis such as temperature-related performance fluctuations. Additionally, multi-hop V2V/V2I simulations will be conducted to examine protocol resilience under dynamic mobility patterns and network congestion. The study also plans to incorporate standardized post-quantum algorithms finalized by NIST to benchmark their operational readiness in V2X environments.

Furthermore, future efforts will explore adaptive encryption frameworks capable of dynamically selecting cryptographic schemes based on message priority, resource availability, and situational context—optimizing the trade-off between performance and security. While this study focuses primarily on performance metrics, future extensions will more deeply consider cryptographic strength. PQC-NTRU, based on hard lattice problems such as the Shortest Vector Problem (SVP), offers promising resistance to quantum attacks. Conversely, RSA and ECC remain vulnerable to quantum algorithms such as Shor's, rendering them less suitable for long-term deployment in quantum-resilient vehicular systems. This future work also aligns with emerging V2X security standards, including IEEE 1609.2.1 and ETSI TC ITS, which are increasingly incorporating post-quantum and lightweight cryptographic requirements for secure vehicular communication.

V. Conclusion

This study presented a comprehensive comparative analysis of five cryptographic algorithms—AES, RSA, ECC, DH, and PQC—evaluated under simulated V2X message traffic conditions. The evaluation considered latency, throughput, CPU usage, and memory consumption across increasing dataset sizes, with results normalized to enable fair cross-metric comparison.

The findings indicate that symmetric encryption (AES) and the simulated PQC scheme offer superior performance in latency-sensitive, high-throughput environments. PQC achieved the highest overall performance, demonstrating readiness for future-proof, quantum-resilient V2X systems. AES remained a strong baseline due to its well-balanced efficiency and low resource overhead. Conversely, RSA and ECC, while cryptographically secure, exhibited performance limitations that make them less suitable for secure real-time vehicular communication. DH proved efficient for key exchange but lacked the responsiveness required for frequent message-level encryption.

In conclusion, the results support the adoption of lightweight, high-performance cryptographic protocols—particularly quantum-safe PQC—for securing V2X networks. Future work will extend this analysis to real-world deployments, integrating hardware-level power profiling and multi-hop V2V/V2I scenarios to further validate algorithm suitability.

Data Availability

All data, source code, models, configurations, and experimental results used in this study are publicly available at the following GitHub repository: https://github.com/niranjanmeegammana/V2XEncryption

References

[1] J. Kamel, M. Wolf, A. Kaiser, P. Urien, and F. Kargl, "VeReMi Extension: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," in *2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–7.

[2] M. K. Hasan *et al.*, "Lightweight cryptographic algorithms for guessing attack protection in complex internet of things applications," *Complexity*, vol. 2021, pp. 1–13, April 2021.

[3] A. Fazzat, R. Khatoun, H. Labiod, and R. Dubois, "A comparative performance study of cryptographic algorithms for connected vehicles," *IEEE Conference Proceedings*, pp. 1–8, October 2020.

[4] H. Aliev, H. Kim, and S. Choi, "A scalable and secure group key management method for secure v2v communication," *Sensors*, vol. 20, no. 21, p. 6137, October 2020.

[5] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[7] T. Veugen, F. Blom, S. J. A. de Hoogh, and Z. Erkin, "Secure comparison protocols in the semi-honest model," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1217–1228, October 2015.

[8] S. A. A. Hakeem, M. A. A. El-Gawad, and H. Kim, "Comparative experiments of v2x security protocol based on hash chain cryptography," *Sensors*, vol. 20, no. 19, p. 5719, October 2020.

[9] S. A. Hakeem and H. Kim, "Authentication and encryption protocol with revocation and reputation management for enhancing 5g-v2x security," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 7, p. 101638, July 2023.

[10] M. M. A. Muslam, "Enhancing security in vehicle-to-vehicle communication: a comprehensive review of protocols and techniques," *Vehicles*, vol. 6, no. 1, pp. 450–467, March 2024.

[11] M. Sontowski *et al.*, "Towards secure communication for high-density longitudinal platooning," *KIT Institute of Telematics Publication*, 2019, available at: https://ps.tm.kit.edu/downloads/publications/sontowski19towards.pdf.

[12] A. Karati and L.-C. Chang, "Cryptanalysis of a lightweight privacy enhancing authentication scheme for internet of vehicles," *IEEE ISCC 2023*, July 2023.