Secured Small-Key-Based Post Quantum Cryptographic Scheme for Blockchain-based VANET

Final Report

by

Mizanur Rahman, *The University of Alabama*
Akid Abrar, *The University of Alabama*
Kazi Hassan Shakib, *The University of Alabama*
Mashrur Chowdhury, *Clemson University*
Abdullah Al Mamun, *Clemson University*
M Sabbir Salek, *Clemson University*
Yingjie Lao, *Clemson University*
Zhenkai Zhang, *Clemson University*
Shaozhi Li, *Clemson University*

February 2025

NATIONAL CENTER FOR TRANSPORTATION CYBERSECURITY AND RESILIENCY (TraCR)

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated in the interest of information exchange. The report is funded, partially or entirely, by the National Center for Transportation Cybersecurity and Resiliency (TraCR) under Grant No. 69A3552344812 and 69A3552348317 which is headquartered at Clemson University, South Carolina, USA, from the U.S. Department of Transportation's University Transportation Centers Program. The U.S. Government assumes no liability for the contents or use thereof.

Non-exclusive rights are retained by the U.S. DOT.

CONTACTS

For more information:

Mizanur Rahman
2007 SCIB, 28 Kirkbride Lane,
Tuscaloosa, AL 35487-0288
Phone: (205) 348-1717
Email: mizan.rahman@ua.edu

TraCR
Clemson University
One Research Dr
Greenville, SC 29607
tracr@clemson.edu

ACKNOWLEDGMENT

The study is funded by the National Center for Transportation Cybersecurity and Resiliency (TraCR) under Grant No. 69A3552344812 and 69A3552348317, which is headquartered at Clemson University, South Carolina, USA, from the U.S. Department of Transportation's University Transportation Centers Program. The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. The U.S. Government assumes no liability for the contents or use thereof.

Technical Report Documentation Page

1. Report No. 13	**2. Government Accession No.** N/A	**3. Recipient's Catalog No.** N/A
4. Title and Subtitle Secured Small-Key-Based Post Quantum Cryptographic Scheme for Blockchain-based VANET		**5. Report Date** February 2025 **6. Performing Organization Code** N/A
7. Author(s) Mizanur Rahman, Ph.D.; https://orcid.org/0000-0003-1128-753X Akid Abrar; https://orcid.org/0009-0007-5880-9389 Kazi Hassan Shakib; https://orcid.org/0000-0002-7894-0719 Mashrur Chowdhury, Ph.D.; https://orcid.org/0000-0002-3275-6983 Abdullah Al Mamun, Ph.D.; https://orcid.org/0000-0002-1066-3540 M Sabbir Salek, Ph.D.; https://orcid.org/0000-0001-7326-3694 Yingjie Lao, Ph.D.; https://orcid.org/0000-0002-9413-2455 Zhenkai Zhang, Ph.D.; https://orcid.org/0000-0002-9025-3460 Shaozhi Li, Ph.D.; https://orcid.org/0000-0002-5432-6802		**8. Performing Organization Report No.** 13
9. Performing Organization Name and Address National Center for Transportation Cybersecurity and Resiliency (TraCR), Clemson University, 414 A One Research Dr, Greenville, SC 29607 Department of Civil, Construction & Environmental Engineering, The University of Alabama 2007, Smart Communities and Innovation Building (SCIB) 28 Kirkbride Lane, Tuscaloosa, Box 870288, AL 35487-0288		**10. Work Unit No.** N/A **11. Contract or Grant No.** 69A3552344812 and 69A3552348317
12. Sponsoring Agency Name and Address U.S. Department of Transportation Office of the Assistant Secretary for Research and Technology 1200 New Jersey Avenue, SE, Washington, DC 20590		**13. Type of Report and Period Covered** Final Report, 01/01/2024 - 12/31/2024 **14. Sponsoring Agency Code** OST-R
15. Supplementary Notes Conducted under the U.S. DOT Office of the Assistant Secretary for Research and Technology's (OST-R) University Transportation Centers (UTC) program.		

16. Abstract
The emergence of quantum computing presents significant challenges to traditional cryptographic algorithms used to secure data communication within Transportation Cyber-Physical Systems (TCPS). The vulnerabilities of traditional cryptographic schemes against quantum computing-based cyberattacks, with a particular focus on the data communication aspects of TCPS, are identified in this report. A case study has been conducted to analyze the vulnerabilities of a TCPS application from the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) service package, i.e., Electronic Toll Collection, leveraging the Microsoft Threat Modeling tool. This case study highlights the cryptographic vulnerabilities of a TCPS application. In addition, this report, specifically, investigates the vulnerabilities of secured blockchain-based VANETs and presents an impersonation attack model utilizing Shor's algorithm implemented in a quantum computer to target the trust-based architecture of such networks. The findings reveal that an impersonation attack is feasible on a blockchain-based VANET, effectively compromising its trust chain. Consequently, this research underscores the critical need for a quantum-secured blockchain to enhance the security of VANETs and the urgency of transitioning to post-quantum cryptography (PQC) to mitigate these risks in TCPS. Thus, the National Institute of Standards and Technology (NIST)'s PQC standardization process, security levels, and implementation considerations of various PQC families in TCPS are reviewed. Finally, an experimental evaluation of CRYSTALS-Kyber assessed its performance across diverse TCPS communication scenarios, including both wired and wireless technologies. While CRYSTALS-Kyber proves effective in securing TCPS applications over high-bandwidth, low-latency Ethernet networks, this research highlights challenges in meeting the stringent latency requirements of safety-critical wireless applications within TCPS.

17. Keywords Post-Quantum Cryptography, Quantum Computing, Blockchain, VANET, Cybersecurity, Cyber-attack, Traditional Cryptography, Threat Modeling, and CRYSTALS-Kyber		**18. Distribution Statement** No restrictions.	
19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 56	**22. Price** N/A

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

TABLE OF CONTENTS

DISCLAIMER 2
CONTACTS 2
ACKNOWLEDGMENT 3
EXECUTIVE SUMMARY 9
CHAPTER 1 11
Introduction 11
CHAPTER 2 13
Literature Review 13
2.1. Vulnerabilities of Cryptographic schemes for TCPS Applications 13
2.1.1. Vulnerabilities of Traditional Cryptographic Schemes to Quantum Computing-Based Attack 13
2.1.1.1. Vulnerabilities in Public Key Cryptography and Digital Signatures 13
2.1.1.2. Vulnerabilities in Symmetric Key Cryptography 14
2.1.1.3. Vulnerabilities in Hash Functions 14
2.1.2. Post-Quantum Cryptography 15
2.1.2.1. NIST PQC Standardization Process 15
2.1.2.2. PQC Scheme Overview 16
2.1.2.2.1. Lattice-Based Cryptography 16
2.1.2.2.2. Code-Based Cryptography 16
2.1.2.2.3. Multivariate Polynomial-Based Cryptography 16
2.1.2.2.4. Hash-Based Cryptography 17
2.1.2.2.5. Isogeny-Based Cryptography 17
2.1.2.3. NIST Security Requirements and Evaluation 17
2.1.2.4. NIST Fourth-Round Finalists: A Comparative Overview 18
2.2 Blockchain-based Vehicular Ad-hoc Network 20
CHAPTER 3 23
Methods 23
3.1. PQC for TCPS Applications 23
3.1.1. Case Study on Cryptographic Vulnerabilities in a TCPS Application 23
3.1.2. Experimental evaluation and security Assessment of CRYSTALS-Kyber FOR TCPS 26
3.1.2.1. Security Features of Kyber to Support TCPS 27
3.1.2.1.1. Fundamental Security Features 27
3.1.2.1.2. Core SVP Estimates, Resistance to Primal and Dual Attacks, and Quantum Resource Requirements for Kyber 28

3.1.2.1.3. Resistance to Algebraic and Symmetric Primitive Attacks 29
3.1.2.1.4. Protection against Decryption Failures 29
3.1.3. Simulation Scenarios and Setup 29
3.2. Blockchain-Based VANET and Threat Model 32
3.2.1.Blockchain-based VANET Architecture 32
3.2.2. Threats and Vulnerabilities of a Blockchain-based VANET 33
3.2.3. Impersonation Attack Scheme 34
3.2.4. Experimental Setup and Implementation 36
3.2.4.1. VANET Setup 36
3.2.4.2. Blockchain Setup 38
3.2.4.3. Quantum Computing Environment Setup 39
CHAPTER 4 41
Results 41
4.1 PQC for TCPS Applications – Performance Evaluation 41
4.2. Blockchain-based VANET Architecture – Evaluation Outcomes 43
CHAPTER 5 49
Conclusions 49
REFERENCES 51

List of Tables

Table 1. Impact of Quantum Computing on Traditional Cryptographic Schemes. (Adapted from (Chen *et al.*, 2016)) 15

Table 2. NIST Security Strength Categories and Computational Requirements. (National Institute of Standards and (NIST), 2016) 18

Table 3. Claimed Security Levels and Key Sizes of NIST Fourth-Round Finalists. (Adopted from (Alagic *et al.*, 2022)) 19

Table 4. Summary of Microsoft Threat Modeling Tool Report 25

Table 5. Summary of Microsoft Threat Modeling Tool Report 26

Table 6. Parameter Sets for Kyber.(Avanzi *et al.*, 2021) 28

Table 7. Simulation Environment Setup 30

Table 8. Components and Their Corresponding Functionalities for Blockchain Based VANET 33

Table 9. Key Parameters. 38

Table 10. Execution time for cryptographic operations. 41

Table 11. Communication delay (in μs) for different simulation scenarios 42

List of Figures

Figure 1. An example attack scenario for a Blockchain-based VANET. 12

Figure 2. Architecture and data flow of TM10: Electronic Toll Collection. 24

Figure 3. Data Flow between the Payment Administration Center, ITS Roadway Equipment, and Light Vehicle OBE using Microsoft Threat Modeling Tool. 25

Figure 4. Simulation Scenarios for Evaluating Kyber in Wired and Wireless Communication Networks in TCPS. 31

Figure 5. Impersonation attack scheme using Shor's algorithm implemented in a quantum computer for blockchain-based VANET. 35

Figure 6. Block diagram of system interaction architecture. 36

Figure 7. Implementation of impersonation attack model utilizing Shor's algorithm implemented in a quantum computer. 37

Figure 8. Quantum circuit implementation of modular exponentiation for this study using IBM Qiskit... 39

Figure 9. No of packets vs simulation time over a time span from 0 to 7.003 seconds (a) data transmission, (b) data reception. 45

Figure 10. Variation of accumulated trust value in RSU. 45

Figure 11. Vehicular trust value profiles. 46

Figure 12. Probability distribution of required time (in seconds) for factorization. 47

Figure 13. IBM quantum roadmap for factorizing RSA-2048 bits. 48

EXECUTIVE SUMMARY

The emergence of quantum computing presents significant challenges to traditional cryptographic algorithms used to secure data communication within Transportation Cyber-Physical Systems (TCPS). Prior studies have demonstrated that Shor's algorithm can efficiently break Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC), while Grover's algorithm reduces the security of symmetric key algorithms, such as the Advanced Encryption Standard (AES). The vulnerabilities of traditional cryptographic schemes against quantum computing-based cyberattacks, with a particular focus on the data communication aspects of TCPS, are identified in this report. By examining the strengths and weaknesses of traditional cryptographic schemes, this research seeks to inform the development of robust security strategies for TCPS. To illustrate real-world implications, a case study has been conducted to analyze the vulnerabilities of a TCPS application from the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) service package, i.e., Electronic Toll Collection, leveraging the Microsoft Threat Modeling tool. This case study highlights the cryptographic vulnerabilities of a TCPS application.

In addition, this report, specifically, investigates the vulnerabilities of secured blockchain-based a Vehicular Ad-hoc Networks (VANET), which is an example of TCPS, and presents an impersonation attack model utilizing Shor's algorithm implemented in a quantum computer to target the trust-based architecture of such networks[1,2]. In this study, a potential threat is investigated in a blockchain-based VANET with an impersonation attack utilizing Shor's algorithm implemented in a quantum computer. Specifically, the impersonation attack using Shor's algorithm is created by compromising the Rivest-Shamir-Adleman (RSA) encrypted digital signatures of VANET, and thus a threat to the trust-based blockchain scheme of VANET is successfully established. We implemented an integrated simulation platform combining OMNET++, vehicles-in-network simulation (VEINS), and simulation of urban mobility (SUMO) traffic simulator. In addition, we incorporated vehicle-to-everything (V2X) communication in OMNET++ using the extended INET library. An impersonation attack on a blockchain-based VANET is implemented using IBM Qiskit, which is an open-source quantum software development kit. The findings reveal that an impersonation attack is feasible on a blockchain-based VANET, effectively compromising its trust chain. Consequently, this research underscores the critical need for a quantum-secured blockchain to enhance the security of VANETs and the urgency of transitioning to post-quantum cryptography (PQC) to mitigate these risks in TCPS.

The standards and guidelines from the National Institute of Standards and Technology (NIST) PQC Standardization Process, analyzing the security properties and implementation considerations of various PQC families in TCPS, are reviewed. The current NIST standardized PQC schemes, i.e., CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+, demonstrate diverse approaches to achieving quantum-resistant cryptographic security, each leveraging different mathematical foundations and design principles to address the challenges posed by quantum computing. This report provides a detailed experimental performance evaluation of CRYSTALS-Kyber, which is standardized by the National Institute of Standards and Technology (NIST) in 2024, offering practical insights into its suitability for securing TCPS[3,4]. The experimental evaluation of CRYSTALS-Kyber assessed its performance across diverse TCPS

[1] K. H. Shakib, M. Rahman, M. Islam, & M. Chowdhury. Impersonation attack using quantum Shor's Algorithm Against Blockchain-based Vehicular Ad-hoc Network. In *IEEE Transactions on Intelligent Transportation Systems*, 26(5), pp. 6530-6544.

[2] K. H. Hasan, M. Rahman, M. Islam, and M. Chowdhury. Impersonation attack modeling for blockchain-based vehicular ad-hoc network using quantum shor's algorithm. In *TraCR Annual Conference 2024*, Greenville, SC, USA, May 6-7 2024.

[3] A. Al Mamun, A. Abrar, M. Rahman, S. Salek, and M. Chowdhury. Enhancing Intelligent Transportation System Security: A Shift to Post-Quantum Cryptography. In *Transportation Research Board 104th Annual Meeting*, Washington, D.C., January 5-9, 2025.

[4] A. Al Mamun. Secure key exchange using post-quantum cryptography. Live outdoor demonstration presented at the *Future of Transportation Summit 2024*, U.S. Department of Transportation Headquarters, August 13-15, 2024.

communication scenarios, including both wired and wireless technologies. Specifically, the experimental assessment of CRYSTALS-Kyber demonstrated its practical feasibility across various peer-to-peer (P2P) communication scenarios, including wired (i.e., Ethernet) and wireless (i.e., LTE/C-V2X) environments for TCPS applications. The results indicate that Kyber's hierarchical security levels, while introducing increased computational and communication overhead with increasing levels, remain well-suited for different TCPS applications when paired with appropriate network infrastructures and communication-related performance requirements. For instance, high-bandwidth and low-latency Ethernet networks effectively mitigate Kyber's computational and communication overhead, making it a strong candidate for securing critical operations between static nodes. Examples include communication between a Payment Administration Center and Department of Motor Vehicles in electronic toll collection systems, as well as centralized traffic management systems, where secure and reliable data exchange between control centers and roadside infrastructure is critical. Similarly, results from the simulated LTE network, representing peer-to-peer C-V2X communication, reveal that while Kyber demonstrates feasibility in wireless communication scenarios, such as vehicle-to-vehicle data exchange, its current performance does not fully meet the stringent requirements of safety-critical TCPS applications. For example, the need to broadcast10 basic safety messages (BSMs) per second imposes strict latency and throughput constraints, posing challenges for the wireless application of Kyber in its existing form. This highlights the necessity for further optimization, particularly in high-speed, low-latency wireless networks such as 5G, to ensure compliance with these demanding standards. Thus, while CRYSTALS-Kyber proves effective in securing TCPS applications over high-bandwidth, low-latency Ethernet networks, this analysis highlights challenges in meeting the stringent latency requirements of safety-critical wireless applications within TCPS.

While the adoption of PQC represents a significant step forward in TCPS data and user security, challenges remain in ensuring interoperability, managing performance trade-offs, and addressing implementation constraints in the real-world transportation systems. Future research must prioritize the development of lightweight and hybrid PQC solutions tailored for real-time and resource-constrained environments, alongside extensive security evaluations under realistic TCPS conditions. Collaborative efforts among academia, industry, and government are essential to streamline standardization, incentivize adoption, and prepare transportation infrastructures for a quantum-secure future. Looking ahead, transitioning to PQC is essential to ensure the long-term sustainability and security of TCPS in the quantum era. By adopting these advancements, the transportation industry can safeguard critical infrastructure, fostering user trust and acceptance while ensuring confidentiality and the seamless operation of TCPS against emerging cyber threats.

CHAPTER 1

Introduction

The rapid evolution of connectivity and automation in transportation systems has given rise to transportation cyber-physical systems (TCPS), where physical elements—such as transportation infrastructure and vehicles—communicate seamlessly with cyber components through advanced communication technologies. This integration enhances the efficiency, safety, and sustainability of transportation networks, while also underscoring the critical need for robust cryptographic security to protect sensitive information. For example, electronic toll collection, traffic signal control, emergency response, commercial vehicle operations, transit security, and infrastructure-based surveillance systems all depend on secure encryption and authentication protocols to ensure data integrity, confidentiality, and authenticity, as emphasized in the United States Department of Transportation's Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT).

In parallel, blockchain-based Vehicular Ad-hoc Network (VANET) architectures have gained significant attention due to their distributed and decentralized nature, which facilitates efficient data transmission and secure data generation and broadcasting. These architectures typically employ rating-based or trust-value-based mechanisms supported by consensus protocols such as proof-of-work (PoW) and proof-of-stake (PoS) to uphold the trustworthiness of transmitted messages. Digital signatures generated using widely adopted asymmetric cryptography techniques like RSA (Rivest–Shamir–Adleman) form the cornerstone for verifying message authenticity in vehicle-to-everything (V2X) communications. Given the stringent low-latency requirements for real-time vehicle-to-vehicle (V2V) communication, small key-based encryption is often employed to minimize computational complexity and storage demands.

However, the advent of quantum computing poses a formidable threat to these established security paradigms. Quantum computers, with their capability to perform computations at exponentially faster speeds than classical systems, have the potential to break current cryptographic protections. For instance, Shor's algorithm can efficiently factor large numbers and solve discrete logarithm problems, thereby compromising cryptographic schemes such as RSA, Diffie–Hellman, the Digital Signature Algorithm, and Elliptic Curve Cryptography (including ECDSA). Similarly, Grover's algorithm dramatically reduces the complexity of brute-force attacks on symmetric key algorithms like the Advanced Encryption Standard (AES). In response to these vulnerabilities, the transportation industry is increasingly exploring post-quantum cryptography (PQC) as a means to develop quantum-resistant cryptographic algorithms, ensuring the long-term security and resilience of both TCPS and blockchain-based VANET systems.

Under the constraints of current quantum computing resources, this study presents a twofold investigation. On one front, a proof-of-concept impersonation attack on blockchain-based VANETs is demonstrated by intentionally scaling down the cryptographic key sizes used within the blockchain. In a controlled experimental scenario involving four vehicles and one Roadside Unit (RSU), a malicious vehicle successfully forges the digital signature of a legitimate vehicle using Shor's algorithm implemented on a quantum computer. As illustrated in **Figure 1**, the attacker generates an impersonation message reporting a false traffic crash, which is acknowledged by nearby vehicles and propagated through the RSU to achieve network consensus. In this attack scenario, the RSU is unable to identify the original malicious sender because the attacker has compromised the digital signature of a legitimate vehicle. Such an impersonation attack not only undermines the trust mechanism but also has the potential to cause severe consequences, including roadway traffic crashes, significant congestion, and extensive manipulation of vehicular communications.

Simultaneously, this report evaluates the quantum vulnerabilities of traditional cryptographic standards within TCPS and examines the potential of post-quantum cryptographic schemes to enhance system security. By analyzing the strengths and weaknesses of existing cryptographic approaches and assessing experimental performance metrics of PQC schemes such as CRYSTALS-Kyber, this study provides valuable insights into the development of robust security strategies for future transportation infrastructures. The objectives of this study are to analyze the vulnerabilities inherent in secured blockchain-based VANET architectures and to develop and validate an impersonation attack model that leverages Shor's algorithm to compromise trust-based security frameworks relying on asymmetric encryption. Additionally, the study aims to evaluate the quantum vulnerabilities of traditional cryptographic standards in TCPS and to assess the potential of PQC to enhance the security of these systems.

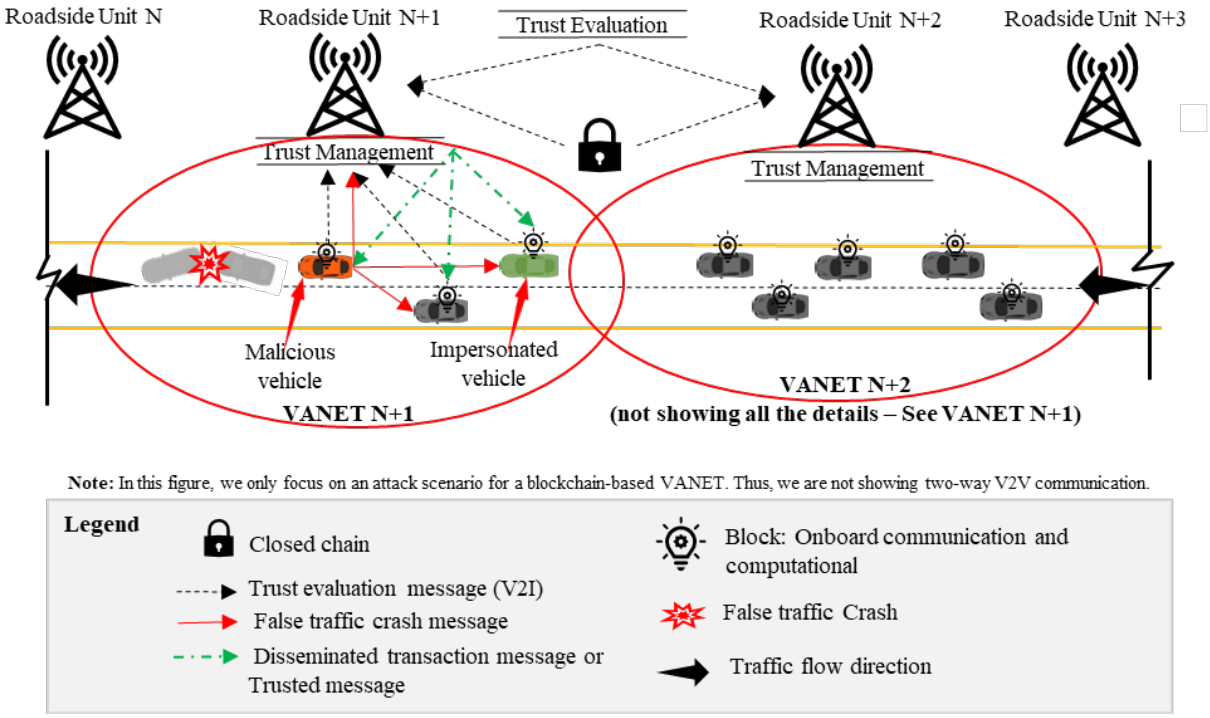


Figure 1. An example attack scenario for a Blockchain-based VANET.

This report is organized into five chapters. Chapter 1 provides this introduction. Chapter 2 presents a comprehensive literature review that covers both quantum computing vulnerabilities in blockchain systems and advancements in post-quantum cryptography for TCPS. Chapter 3 details the methods and experimental setups employed in this study. Chapter 4 discusses the results from the quantum-enabled impersonation attack and the performance evaluation of PQC schemes. Finally, Chapter 5 concludes the report with observations, implications for future research, and recommendations for enhancing the security of transportation cyber-physical systems.

CHAPTER 2

Literature Review

This literature review section contains an in-depth analysis of the vulnerabilities associated with traditional cryptographic schemes—such as RSA, Diffie–Hellman, and ECDSA—when confronted with the advanced threats posed by quantum computing, particularly through algorithms like Shor's and Grover's. It examines the limitations of these conventional approaches in the context of blockchain-based VANETs and TCPS, and then evaluates the emerging field of PQC as a viable alternative. The review details various PQC candidates, including performance assessments and experimental insights, and provides a comprehensive comparison between classical and quantum-resistant methods, thereby setting the stage for the subsequent sections on methodology and experimental results.

2.1. Vulnerabilities of Cryptographic schemes for TCPS Applications

2.1.1. Vulnerabilities of Traditional Cryptographic Schemes to Quantum Computing-Based Attack

Cryptographic schemes can be classified into several types based on their functions: public key cryptography, symmetric cryptography, digital signatures, and hashing functions (Menezes, Van Oorschot and Vanstone, 1997). Public key cryptography uses a pair of keys- a public key, which can be shared openly, and a private key, which is kept secret. It is primarily used for secure key exchange and digital signatures, with examples including RSA, DH, and ECC (Menezes, Van Oorschot and Vanstone, 1997). Symmetric cryptography, such as, the AES, uses a single key for both encryption and decryption processes, making it particularly efficient for encrypting large datasets (Menezes, Van Oorschot and Vanstone, 1997). However, this secret key needs to be securely communicated between parties before encryption and decryption can occur, often requiring additional mechanisms or protocols for key exchange, such as Key Encapsulation Mechanisms (KEMs) (Bos *et al.*, 2018). Digital signatures verify the authenticity and integrity of a message, providing non-repudiation; examples include the ECDSA and the DSA (Menezes, Van Oorschot and Vanstone, 1997). Hashing functions generate a fixed-size hash value from input data, ensuring data integrity, such as SHA-256 (Menezes, Van Oorschot and Vanstone, 1997).

The Institute of Electrical and Electronics Engineers (IEEE) 1609.2 standard for Wireless Access in Vehicular Environments (WAVE) incorporates a suite of cryptographic algorithms to ensure the integrity, confidentiality, and authenticity of data exchanged within TCPS ('IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities', no date). These algorithms include the ECDSA for digital signatures (Johnson, Menezes and Vanstone, 2001), AES-128 (National Institute of Standards and (NIST), 2016) and SM4 (Suo *et al.*, 2020) for symmetric encryption, and the Elliptic Curve Integrated Encryption Scheme (ECIES) (Gayoso Martinez *et al.*, 2010) and SM2 (Bai, Zhang and Yang, 2012) for key establishment and encryption. Hash functions such as SHA-256 (Handschuh, 2005) and SM3 (Xu *et al.*, 2022) are used for data integrity verification. However, the advent of quantum computing poses significant threats to these cryptographic protections. The next subsections will discuss the vulnerabilities of cryptographic schemes incorporated into the IEEE 1609.2 standard, as well as some commonly used cryptographic schemes.

2.1.1.1. Vulnerabilities in Public Key Cryptography and Digital Signatures

ECC schemes, including ECDSA and SM2, offer enhanced security compared to traditional methods using smaller key sizes. However, these systems are susceptible to Shor's algorithm (Shor, 1995), a quantum computing algorithm capable of efficiently solving the discrete logarithm problem, which forms the basis of ECC schemes. Shor's algorithm presents a considerable risk to digital signatures and key exchange protocols based on ECC. Research by Kirsch (2015) has extended their algorithm's capabilities to decrypt data encrypted with ECC, highlighting the vulnerability of ECC's smaller key space to quantum attacks

(Kirsch, 2015). Proos and Zalka's (2003) work further emphasize the potential impact of quantum computing on ECC. Their findings indicate that a 1000-qubit quantum computer could break 160-bit elliptic curves while factorizing a 1024-bit RSA key would require a more powerful 2000-qubit system (Proos and Zalka, 2003).

RSA relies on the difficulty of factoring large integers (Rivest, Shamir and Adleman, 1978), a problem that quantum computers can solve efficiently using Shor's algorithm. This makes RSA encryption insecure against quantum attacks. The study by Shakib et al. (2023) demonstrated that a quantum impersonation attack using Shor's algorithm could break RSA-encrypted digital signatures in a blockchain-based Vehicular Ad-hoc Network (VANET) (Shakib, Rahman and Islam, 2023). In addition, both DH and DSA are vulnerable to Shor's algorithm due to their reliance on the discrete logarithm problem. Quantum computers can solve this problem efficiently, compromising the security of these key exchange and digital signature schemes (Mavroeidis *et al.*, 2018). The implications of this vulnerability are significant, as DH and DSA are widely used in today's cryptographic infrastructure.

2.1.1.2. Vulnerabilities in Symmetric Key Cryptography

Both AES and SM4 are symmetric encryption algorithms susceptible to the quantum threat posed by Grover's algorithm (L K Grover, 1996). While AES generally offers stronger resistance due to its flexibility in key size, even AES-128, with a 128-bit key, can be effectively reduced to a 64-bit key through Grover's algorithm. SM4, using a fixed 128-bit key, faces similar vulnerabilities. Employing larger key sizes, such as AES-256, is necessary to mitigate these quantum risks. The impact of quantum attacks on symmetric encryption is exemplified by the Data Encryption Standard (DES). Bone and Castro (1997) demonstrated that Grover's algorithm could break DES, which uses a 56-bit key, with only 185 search attempts (Bone and Castro, 1997). This underscores the necessity for robust countermeasures against quantum threats in symmetric cryptography.

2.1.1.3. Vulnerabilities in Hash Functions

Hash functions, which produce fixed-size outputs (hash values) from arbitrary-length inputs (Menezes, Van Oorschot and Vanstone, 1997), are also vulnerable to quantum attacks. Grover's algorithm can significantly accelerate the process of finding collisions in hash functions, reducing their security. Specifically, a hash function with a 2^n-bit output can be broken with approximately $2^{n/2}$ operations using Grover's algorithm (L K Grover, 1996). Furthermore, a technique known as the quantum birthday attack, combining Grover's algorithm with the birthday paradox, can find collisions even more efficiently (Leurent, Nandi and Sibleyras, 2018). To counter these threats, hash functions require substantially longer outputs in the quantum era. For instance, according to Brassard et al. (1997), a hash function aiming for *b*-bits of security against Grover's attacks should produce a *3b*-bit output (Brassard, Høyer and Tapp, 1997). While many current hash algorithms fall short of this requirement, SHA-2 and SHA-3, with longer output sizes, offer greater resistance to quantum attacks.

The impact of quantum computing on various traditional cryptographic schemes is further summarized in **Table 1**. This table is adapted from NIST and illustrates how quantum computing compromises the security of traditional cryptographic algorithms, making schemes such as RSA, ECC, and DSA no longer secure (Chen *et al.*, 2016). Given the vulnerabilities, it is evident that current cryptographic schemes are insufficient in the face of advancing quantum computing technology. The next section explores PQC as a solution to this critical issue.

Table 1. Impact of Quantum Computing on Traditional Cryptographic Schemes. (Adapted from (Chen *et al.*, 2016))

Cryptographic Scheme	Type	Purpose	Impact from Large-Scale Quantum Computer
AES	Symmetric Key	Encryption	Larger key sizes needed
SHA-2, SHA-3	Hash Functions	Hashing	Longer output needed
RSA	Public Key	Signatures, Key Establishment	No longer secure
ECDSA, ECDH (ECC)	Public Key	Signatures, Key Exchange	No longer secure
DSA (Finite Field Cryptography)	Public Key	Signatures, Key Exchange	No longer secure

2.1.2. Post-Quantum Cryptography

PQC represents a new class of cryptographic algorithms designed to be secure against attacks from both classical and quantum computers. The primary goals of PQC are to develop cryptographic schemes that are secure against quantum attacks, ensure practical implementation across various applications, and facilitate a smooth transition from classical to quantum-resistant cryptographic systems (Chen *et al.*, 2016). Extensive research, public engagement, and the establishment of standards are critical components of this transition. The NIST has been at the forefront of PQC research and standardization. This section aims to provide a comprehensive overview of PQC by discussing the NIST PQC Standardization Process, the various families of PQC schemes, and the security requirements and evaluations that guide the selection of these schemes. We will also compare the claimed security levels, key sizes, and other relevant metrics of the NIST fourth-round finalists to illustrate the diverse approaches and trade-offs in PQC designs.

2.1.2.1. NIST PQC Standardization Process

To address the growing threat of quantum computers to current encryption standards, NIST initiated a standardization process for PQC in 2016. This multi-round evaluation aimed to select algorithms resistant to quantum attacks. From an initial pool of 69 candidate algorithms for public-key encryption/ KEMs and digital signatures, NIST narrowed down the field to 26 finalists in the second round, and subsequently to 15 in the third (Alagic *et al.*, 2019, 2022; Moody *et al.*, 2020). Ultimately, after the third-round evaluation, CRYSTALS-Kyber (Bos *et al.*, 2018) was chosen for standardization as a public-key encryption/KEM scheme, while CRYSTALS-Dilithium (Ducas *et al.*, 2018), Falcon ('Falcon - Fast-Fourier Lattice-based Compact Signatures over NTRU', 2024), and Stateless Practical Hash-based Incredibly Nice and Compact Signatures (SPHINCS+) (Bernstein *et al.*, 2019) were selected for standardization as digital signatures (Alagic *et al.*, 2022). On August 13, 2024, NIST finalized the standardization of three schemes: CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+, marking a significant milestone in post-quantum cryptography. These schemes have been renamed as part of their formal standardization: CRYSTALS-Kyber is now 'Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)' (National Institute of Standards and Technology, 2024b), CRYSTALS-Dilithium is 'Module-Lattice-Based Digital Signature Algorithm (ML-DSA)' (National Institute of Standards and Technology, 2024a), and SPHINCS+ is 'Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)' (National Institute of Standards and Technology, 2024c), reflecting their finalized status in the standards. As the process continues, four additional public-key encryption/KEM candidates (i.e., Bit Flipping Key Encapsulation [BIKE] ('BIKE - Bit Flipping Key Encapsulation', 2024), Classic McEliece ('Classic McEliece', 2024), Hamming Quasi-Cyclic [HQC] ('HQC - Hamming Quasi-Cyclic', 2024), and Supersingular Isogeny Key Encapsulation [SIKE] ('SIKE – Supersingular Isogeny Key Encapsulation', 2024)) advanced to the fourth round (Alagic

et al., 2022). This rigorous process evaluates algorithms based on security, performance, and implementation practicality to ensure robust protection of sensitive data in the quantum era.

2.1.2.2. PQC Scheme Overview

PQC includes a range of cryptographic algorithms designed to remain secure against attacks from both classical and quantum computers. From the literature review and NIST's extensive evaluation process, five main families of PQC schemes have been identified: lattice-based, code-based, multivariate polynomial-based, hash-based, and isogeny-based. This section briefly discusses the underlying mathematical problems and inherent security properties of these families.

2.1.2.2.1. Lattice-Based Cryptography

Lattice-based cryptography is built on hard mathematical problems related to lattices, such as the Shortest Vector Problem (SVP) (Micciancio and Goldwasser, 2002) and the Learning with Errors (LWE) (Albrecht, Player and Scott, 2015) problem. These problems involve finding short or close vectors in a high-dimensional lattice, which is computationally infeasible for both classical and quantum computers. The security of lattice-based schemes relies on the assumed hardness of these problems (Sabani, Savvas and Garani, 2024). Furthermore, the structured randomness and noise introduced in the LWE problems create additional layers of difficulty, making it extremely challenging for quantum algorithms like Shor's algorithm or Grover's algorithm to solve efficiently. Reflecting their strong security foundations, the NIST evaluation's third round led to the standardization of one lattice-based public-key encryption/KEM scheme (CRYSTALS-Kyber) and one lattice-based digital signature scheme (CRYSTALS-Dilithium), now formally recognized as 'ML-KEM' and 'ML-DSA', respectively (National Institute of Standards and Technology, 2024b) (National Institute of Standards and Technology, 2024a). The standardization process for Falcon, another lattice-based algorithm used as a digital signature scheme, is currently ongoing.

2.1.2.2.2. Code-Based Cryptography

Code-based cryptography relies on the hardness of problems related to error-correcting codes, particularly the General Decoding Problem (GDP) and the Syndrome Decoding Problem (SDP), both of which are NP-complete (Berlekamp, McEliece and Van Tilborg, 1978). One of the most well-known examples is the McEliece cryptosystem (McEliece, 1978), which has been extensively studied and remains resistant to cryptanalytic attacks (Bernstein, Lange and Peters, 2008). No efficient quantum algorithms have been found to solve these decoding problems, making code-based cryptography quantum-resistant. This resilience is why schemes like Classic McEliece have been selected as finalists in the NIST PQC Standardization Process (Alagic *et al.*, 2022). Classic McEliece offers strong security with fast encryption and decryption, despite its larger key sizes compared to other schemes. Another notable scheme is HQC, which also relies on the hardness of decoding random linear codes ('HQC - Hamming Quasi-Cyclic', 2024). In addition to Classic McEliece, HQC has been selected as a fourth-round finalist in the NIST PQC Standardization Process (Alagic *et al.*, 2022).

2.1.2.2.3. Multivariate Polynomial-Based Cryptography

Multivariate polynomial-based cryptography relies on the complexity of solving systems of multivariate polynomial equations over finite fields. These problems, such as the Multivariate Quadratic (MQ) problem, are known to be NP-hard, making them computationally infeasible to solve efficiently with either classical or quantum computers (Alagic *et al.*, 2022). The security of multivariate schemes is based on the assumed difficulty of finding solutions to these polynomial equations. Notable examples of multivariate polynomial-based schemes include Great Multivariate Short Signature (GeMSS) scheme ('GeMSS: A Great

Multivariate Short Signature', no date) and Rainbow signature scheme ('Rainbow Signature', 2024). Both schemes offered high security and efficient performance and were initially selected as finalists in the NIST PQC Standardization Process. However, both faced significant cryptanalytic challenges in the third round and therefore, were not selected to progress to the fourth round. GeMSS suffered a key-recovery attack that revealed the private key, making attempts to restore security impractical (Tao, Petzoldt and Ding, 2020, 2021). Similarly, Rainbow's security was significantly reduced by new attacks, necessitating extensive re-engineering to meet security targets, which negated its performance advantages (Alagic *et al.*, 2022).

2.1.2.2.4. Hash-Based Cryptography

Hash-based cryptography utilizes the security properties of cryptographic hash functions to construct secure digital signatures and other cryptographic primitives. The security of hash-based schemes is rooted in the collision resistance and preimage resistance of hash functions, making them inherently resistant to quantum attacks (Brassard, Høyer and Tapp, 1997). A notable example of a hash-based cryptographic scheme is SPHINCS+, which is a stateless hash-based signature scheme that offers long-term security guarantees with minimal reliance on external assumptions (Bernstein *et al.*, 2019). It provides strong security with efficient signing and verification processes. SPHINCS+ was selected for standardization after the third-round evaluation in the NIST PQC Standardization Process and is now formally recognized as 'SLH-DSA' after standardization in 2024 (National Institute of Standards and Technology, 2024c).

2.1.2.2.5. Isogeny-Based Cryptography

Isogeny-based cryptography leverages the hardness of problems related to finding isogenies between elliptic curves, specifically in the context of supersingular elliptic curve isogeny graphs (Galbraith and Vercauteren, 2018). The primary hard problem in this domain is the Supersingular Isogeny Diffie-Hellman (SIDH) problem, which involves finding a secret isogeny between two given supersingular elliptic curves (Alagic *et al.*, 2022). Isogeny-based schemes are attractive because they offer very small key sizes compared to other PQC families. The most well-known isogeny-based scheme is SIKE. SIKE was initially selected to advance to the fourth round of the NIST PQC Standardization Process. However, due to an efficient key-recovery attack that exploited vulnerabilities in the SIDH protocol (Castryck and Decru, 2022), the SIKE development team included a detailed postscript in their fourth round submission to the NIST PQC Standardization Process, outlining the attack and its implications, to ensure the information is documented and open for future research.

2.1.2.3. NIST Security Requirements and Evaluation

NIST requires PQC algorithms to resist both quantum and classical attacks (National Institute of Standards and (NIST), 2016). For encryption and key establishment, NIST aims to standardize schemes that offer "semantically secure" encryption against adaptive chosen ciphertext attacks (IND-CCA2 security), ensuring security even if an attacker can choose ciphertexts and get their plaintexts decrypted (Katz and Lindell, 2015). For ephemeral key exchanges, NIST considers IND-CPA security against chosen plaintext attacks (Katz and Lindell, 2015), which is sufficient for scenarios with controlled environments and single-use keys. For digital signatures, NIST seeks schemes that are existentially unforgeable against adaptive chosen message attacks (EUF-CMA security), ensuring that an attacker cannot forge signatures even if they can obtain signatures for chosen messages (Katz and Lindell, 2015).

Given the uncertainties in estimating post-quantum security, NIST defines broad security strength categories to facilitate performance comparisons and decision-making about key lengths (National Institute of Standards and (NIST), 2016). These uncertainties result from the evolving nature of quantum computing,

the potential for unforeseen quantum algorithms, and the challenges in predicting the future trajectory of quantum and classical computing. The security strength categories are presented in **Table 2**.

Security strength categories Level 1, 3, and 5, based on block cipher security, are particularly resistant to quantum attacks. Categories 2 and 4, defined by hash function security, are also resistant but require further research. Each category is defined by the computational resources required to break the cryptosystem, benchmarked against well-established symmetric schemes such as AES and SHA-3. Computational resources are measured using various metrics, including the number of classical elementary operations and quantum circuit size. To account for the practical limitations of long serial quantum computations, NIST introduces the parameter MAXDEPTH, which represents the maximum circuit depth for quantum attacks. Plausible values for MAXDEPTH range from 2^{40} logical gates, which is the approximate number of gates current quantum computing architectures are expected to perform serially in a year. This extends to 2^{64} logical gates, representing the number of gates classical computing architectures can perform serially in a decade. Finally, the upper bound of MAXDEPTH is 2^{96} logical gates, which is the approximate number of gates atomic scale qubits with speed-of-light propagation times could perform in a millennium (National Institute of Standards and (NIST), 2016).

NIST also considers additional security properties such as perfect forward secrecy, resistance to side-channel attacks, multi-key attacks, and misuse. These properties ensure that past session keys remain secure, the scheme is secure against physical attacks, multiple keys do not provide an advantage to attackers, and the scheme is robust against implementation errors (National Institute of Standards and (NIST), 2016).

Table 2. NIST Security Strength Categories and Computational Requirements. (National Institute of Standards and (NIST), 2016)

Security Strength Category	Description	Computational Resources Required
Level 1	Equivalent to breaking AES-128	2^{170}/MAXDEPTH quantum gates or 2^{143} classical gates
Level 2	Equivalent to breaking SHA3-256	2^{146} classical gates
Level 3	Equivalent to breaking AES-192	2^{233}/MAXDEPTH quantum gates or 2^{207} classical gates
Level 4	Equivalent to breaking SHA3-384	2^{210} classical gates
Level 5	Equivalent to breaking AES-256	2^{298}/MAXDEPTH quantum gates or 2^{272} classical gates

2.1.2.4. NIST Fourth-Round Finalists: A Comparative Overview

Table 3 summarizes the claimed security levels, key sizes, and other relevant metrics for the NIST fourth-round finalists in the PQC Standardization Process, including the three schemes that are being standardized: CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+. All public-key encryption schemes and KEMs (i.e., CRYSTALS-Kyber, Classic McEliece, BIKE, and HQC) in **Table 3** provide IND-CCA2 security (Alagic *et al.*, 2022). Similarly, all digital signature schemes (i.e., CRYSTALS-Dilithium, Falcon, and SPHINCS+) provide EUF-CMA security (Alagic *et al.*, 2022).

Table 3. Claimed Security Levels and Key Sizes of NIST Fourth-Round Finalists. (Adopted from (Alagic *et al.*, 2022))

PQC Candidate	Claimed NIST Security Category	Public Key (in bytes)	Private Key (in bytes)	Ciphertext/ Signature (in bytes)	Core SVP Estimate	Gate Count	Memory
CRYSTALS-Kyber512[a]	Level 1	800	1632	768	C:118 bits Q:107 bits	2^{151}	2^{94}
CRYSTALS-Kyber768[a]	Level 3	1184	2400	1088	C:183 bits Q:166 bits	2^{215}	2^{139}
CRYSTALS-Kyber1024[a]	Level 5	1568	3168	1568	C:256 bits Q:232 bits	2^{287}	2^{190}
Classic McEliece348864	Level 1	261120	6492	128	NA	NA	NA
Classic McEliece460896	Level 3	524160	13608	188	NA	NA	NA
Classic McEliece6688128	Level 5	104992	13932	240	NA	NA	NA
Classic McEliece6960119	Level 5	1047319	13948	226	NA	NA	NA
Classic McEliece8192128	Level 5	1357824	14120	240	NA	NA	NA
BIKE	Level 1	1540	280	1572	NA	NA	NA
	Level 3	3082	418	3114	NA	NA	NA
	Level 5	5122	580	5154	NA	NA	NA
HQC-128	Level 1	2249	40	4481	NA	NA	NA
HQC-192	Level 3	4522	40	9026	NA	NA	NA
HQC-256	Level 5	7245	40	14469	NA	NA	NA
CRYSTALS-Dilithium[a]	Level 2	1312	2528	2420	C:123 bits Q:112 bits	2^{159}	2^{98}
	Level 3	1952	4000	3293	C:182 bits Q:165 bits	2^{217}	2^{139}
	Level 5	2592	4864	4595	C:252 bits Q:229 bits	2^{285}	2^{187}
Falcon-512[b]	Level 1	897	7553	666	C:120 bits Q:108 bits	NA	NA
Falcon-1024[b]	Level 5	1793	13953	1280	C:273 bits Q:248 bits	NA	NA
SPHINCS+-128s[a]	Level 1	32	64	7856	NA	NA	NA
SPHINCS+-128f[a]	Level 1	32	64	17088	NA	NA	NA
SPHINCS+-192s[a]	Level 3	48	96	16224	NA	NA	NA
SPHINCS+-192f[a]	Level 3	48	96	35664	NA	NA	NA
SPHINCS+-256s[a]	Level 5	64	128	29792	NA	NA	NA
SPHINCS+-256f[a]	Level 5	64	128	49856	NA	NA	NA

Note: [a]Standardized by NIST on August 13, 2024; [b]Standardization process ongoing; C: Classical; Q: Quantum; SVP: Short Vector Problem; NA: Not Available

These public-key encryption/KEMs finalists in **Table 3** demonstrate a range of security levels from Level 1 to Level 5, with corresponding increases in key sizes and computational requirements. The key sizes and ciphertext lengths vary significantly among the schemes, reflecting different underlying cryptographic approaches and security trade-offs. For instance, lattice-based schemes, such as CRYSTALS-Kyber, have relatively small key sizes and ciphertexts, making them feasible for practical implementation, especially in resource-constrained environments. CRYSTALS-Kyber provides security levels ranging from Level 1 to Level 5, with its largest variant, CRYSTALS-Kyber1024, offering the highest security level but requiring

larger keys and ciphertexts. The Core SVP estimates for CRYSTALS-Kyber range from 118 bits classically (107 bits quantumly) for CRYSTALS-Kyber512, to 256 bits classically (232 bits quantumly) for CRYSTALS-Kyber1024, indicating robust security across all levels. It is to be noted that the Core SVP Estimate measures the difficulty of finding the shortest non-zero vector in a lattice, which is a central problem in lattice-based cryptography (Peikert, 2016). The higher the Core SVP estimate, the more secure the scheme is. Quantum gate counts increase with the security level, from 2^{151} for CRYSTALS-Kyber512 to 2^{287} for CRYSTALS-Kyber1024, reflecting their resistance to quantum attacks. Similarly, memory requirements increase from 2^{94} units for CRYSTALS-Kyber512 to 2^{190} units for CRYSTALS-Kyber1024, indicating the trade-offs between security and resource usage. Code-based schemes, such as Classic McEliece, provide robust security with significantly larger key sizes compared to lattice-based schemes. Despite its large public key sizes, Classic McEliece's small ciphertexts make it suitable for scenarios where bandwidth is a concern. BIKE and HQC, both code-based schemes, offer a balance between security and efficiency. BIKE's security ranges from Level 1 to Level 5, with moderate key sizes and ciphertexts. HQC also spans from Level 1 to Level 5, featuring compact private keys and moderate public keys and ciphertext sizes.

Among digital signature schemes, CRYSTALS-Dilithium, which is based on lattice problems, provides security levels up to Level 5. For example, at Level 5, CRYSTALS-Dilithium has a Core SVP estimate of 252 bits classically and 229 bits quantumly, with a gate count of 2^{285} and a memory requirement of 2^{187}. Falcon, another lattice-based scheme, emphasizes compact signatures and strong security guarantees, making it suitable for applications where signature size is critical. Falcon-1024, at Level 5, offers a core SVP estimate of 273 bits classically and 248 bits quantumly. SPHINCS+ provides security levels up to Level 5, with both small and large signature variants to accommodate different application needs.

The selection of a PQC scheme requires a careful evaluation of specific application requirements, including security level, efficiency, and resource constraints. The data presented in **Table 3** aids in making informed decisions by comparing the trade-offs between different schemes. The ongoing NIST PQC standardization process is important for developing robust cryptographic solutions to safeguard against the quantum computing threat. By understanding the diverse range of PQC schemes and their characteristics, organizations can make informed decisions to protect sensitive data in the quantum era.

2.2 Blockchain-based Vehicular Ad-hoc Network

For non-quantum-based attacks, prime factorization, which is a major part of cryptography used in ownership mechanism, cannot be broken in polynomial time (Shor, 1994). Note that modular exponentiation is one of the necessary steps in prime factorization. However, modular exponentiation cannot be executed in polynomial time by classical computing algorithms, and it requires sub-exponential time(Crandall and Pomerance, 2001). Because of the superposition property of qubits, quantum computers can execute modular exponentiation in sub-exponential time. For example, it is possible to do factorization in polynomial time with a quantum computer, where a classical computer needs sub-exponential time to perform prime factorization (Shor, 1994). Due to the nature of finding non-trivial factors in every iteration, Shor's algorithm estimates and is more likely to find factors in a polynomial time (Shor, 1994).

Quantum attacks can be formulated using two different algorithms implemented in a quantum computer: (i) Shor's algorithm (Shor, 1994) because of its ability of factorization; and (ii) Grover's algorithm due to its searching capability (Lov K. Grover, 1996). The Shor's algorithm provides a threat on asymmetric cryptography through prime factorization and discrete logarithm problem-solving capability, which covers the basis for a wide range of cryptographic techniques. On the other hand, Grover's algorithm is applicable for symmetric cryptography through inversing the hash functions (Fernandez, Orue and Arroyo, 2021). In this study, we have leveraged the efficacy of Shor's algorithm for developing an impersonation attack scheme due to our focus on PoS based architecture and our impersonation attack. The Practical Byzantine

Fault Tolerance (PBFT) (Diallo, Dib and Al Agha, 2021; Sehar *et al.*, 2023) one of the popular consensus algorithms for blockchain-based VANETs, could be vulnerable to quantum attacks. The PBFT relies on digital signatures and secure message exchanges to maintain trust and consensus in private or semi-decentralized networks. However, Shor's algorithm could pose a similar threat by compromising the authenticity of messages as presented in this report.

Grover's algorithm is more appropriate for PoW-based scheme. The authors in (*Quantum Computing - The Impending End for the Blockchain?*, no date) presented two primary applications of Grover's algorithm. Firstly, the algorithm can enable quadratic speedup for solving hash functions and creating attacks (Rodenburg and Pappas, 2017). The attacker, who controls more than half of network's mining rate as miner, can monopolize the data and even rewrite the blocks by creating forks as well. Secondly, the attacker can search for hash collisions (Rodenburg and Pappas, 2017; Cui, Dou and Yan, 2020) to replace certain parts of blocks without breaking the chain. Moreover, the attacker can construct a more reliable chain by maintaining the hash pointer of the block identically, as the pointer of the previous block will then reference the same block. Currently, researchers explore the complexity of securing communications in VANETs, emphasizing the challenges posed by the highly dynamic and fast-paced nature of vehicle interactions. Traditional approaches, such as public key infrastructure (PKI) (Azees, Vijayakumar and Deboarh, 2017), and identity-based signature schemes(Ali, Lawrence and Li, 2020), face issues related to certificate management, key escrow problems, and computational overhead. Various attempts, including certificateless public key cryptography (CL-PKC) (Gayathri *et al.*, 2018; Majid Bayat *et al.*, 2020)and certificateless aggregate signature schemes (CLAS)(Mei *et al.*, 2021), certificateless lattice-based schemes like CLLS(Xu *et al.*, 2024), aim to address these challenges but encounter heavy computation power and communication latency. To enhance efficiency in CL-PKC, Mei et al. (Mei *et al.*, 2021)presented a CLAS scheme, which relies on bilinear pairing and map-to-point hash functions, demanding resources beyond the capacity of onboard units (OBUs). In another study, Ali et al.(Ali, Lawrence and Li, 2020) incorporated blockchain to enhance revocation transparency, allowing participants to efficiently verify revoked pseudo-identities without relying on a trusted authority (TA). Despite this, their scheme's efficiency is compromised due to the necessity of a bilinear pairing during signature verification.

On the other hand, attacks that do not utilize quantum computers, such as Sybil attacks(Lim *et al.*, 2020), one can exploit weaknesses in cryptographic mechanisms that use bilinear pairings, such as identity-based encryption schemes (Lalit Negi and Kumar, 2024). Since bilinear pairings allow operations across different groups, an attacker can manipulate inputs to link multiple fake identities to a single key, tricking the network into recognizing multiple Sybil nodes as legitimate entities. To counter such threats, recent studies have proposed blockchain-driven authentication protocols that ensure secure data exchange between vehicles and infrastructure, mitigating risks associated with malicious activities. For example, handover authentication mechanisms in these protocols (Dwivedi *et al.*, 2023; Xie *et al.*, 2023; Tian, Shen and Wang, 2024) use smart contracts to automate authentication during handover, ensuring trust without significant latency. Blockchain systems also facilitate key exchanges by assigning temporary identities to vehicles and periodically changing cryptographic keys, which enhances security against replay and impersonation attacks. However, all these studies rely on the complexity of cryptographic solutions and their inherent property of computational infeasibility, which ensures that adversaries cannot feasibly reverse-engineer keys or signatures without incurring prohibitive computational costs, thereby maintaining secure communication even in the presence of malicious actors.

To ensure such secure communication, blockchains typically rely on robust digital signature methods for encryption, such as ECDSA, known for its strength but demanding considerable computational time. For instance, the Ethereum blockchain utilizes ECDSA, which takes nearly 10 milliseconds (ms) for a single signature and verification process (*Ethereum Glossary | ethereum.org*, no date), this would exponentially grow with aggregate signature schemes. To mitigate this delay, a lightweight encryption algorithm like RSA-1024 (Suaib Akhter *et al.*, 2021; Fuad A. Ghaleb *et al.*, 2023) was employed, offering 80-bit security

strength and requiring only one-third of the time compared to ECDSA-RSA-1024. The authors in(Stewart *et al.*, 2018) describe a transaction hijacking scenario in cryptocurrency platforms using the public key, which is published to the network or revealed from transactions sitting in the memory pools. They present an attack model that uses the Shor's algorithm on a known public key to decrypt the private key. Then, using that decrypted private key creates a conflicting transaction spending the same value. They created a commit-delay-reveal architecture to safeguard the reveal of public key encryption. However, such a scheme can fail in a broadcasting scenario, such a delay will cause a lack of trust. Another limitation of the study was the failure to provide proof-of-concept and the effectiveness of such attacks with experiments or simulations.

In another study (Kearney and Perez-Delgado, 2021), the authors explored vulnerabilities of five cryptocurrencies and their variations: Bitcoin, Ehereum, Litecoin, Monero and ZCash. Among these, Bitcoin exhibited vulnerability to duplicate transactions due to its signature scheme, while Ethereum faced potential replication issues with its consensus-based approach relying on digital logarithm-based public keys. Similarly, Litecoin shared vulnerabilities with Bitcoin due to its analogous structure. Monero employed ECDSA and a bulletproof protocol to hide transaction amounts, while ZCash, which uses consensus-based scheme, utilized ECDSA. The focus was on assessing the susceptibility of these cryptocurrencies to quantum attacks targeting their signature schemes and consensus algorithms. The study revealed vulnerabilities against transaction forging and duplication attacks. While offering theoretical proof of the cryptocurrencies' vulnerability against algorithms like Shor's and Grover's, the authors do not provide experimental analysis to quantify these vulnerabilities with a comprehensive attack model. In contrast, the presented method in this study not only identifies vulnerabilities within blockchain and cryptocurrency-based systems but also presents both comprehensive experimental analysis and an attack strategy against PoS-based blockchain schemes, along with a generic attack model applicable to PoW-based blockchains.

The authors in (Aggarwal *et al.*, 2018) discussed attacks using quantum computers on Bitcoin and potential countermeasures to protect against them. Their research specifically focuses on the impact of quantum attacks on Bitcoin and other cryptocurrencies. They examined the susceptibility of Bitcoin's PoW to quantum attacks, considering the public key disclosure through address reuse, along with the vulnerability of the cryptographic ECDSA algorithm employed in Bitcoin transactions. They found that while the current specialized application specific integrated circuit (ASIC) miners make the PoW relatively resistant to quantum speedup, the ECDSA signature scheme is more vulnerable and could be broken by a quantum computer as early as 2027. The study explores a detailed analysis of the time required for quantum computers to perform attacks on hash function using Grover's algorithm and compares the estimated quantum computing power against the total hashing power of the Bitcoin network. It also explores alternative PoW schemes and reviews various post-quantum signature schemes as countermeasures. However, as this is theoretical proof of concept only, it lacks comprehensive analysis. Existing literature lacks a practical attack model that uses quantum computers to test (without only theoretical analysis) against the traditional asymmetric cryptographic schemes and lightweight key structure feasible for dynamic VANET scenarios. This indicates the importance of this research and the gap in existing literature.

The literature review establishes that while classical cryptographic schemes are increasingly susceptible to quantum computing attacks, post-quantum cryptographic solutions offer promising pathways to secure both VANETs and TCPS. Nonetheless, given the rapid evolution of quantum technologies and the inherent challenges in scaling and optimizing PQC implementations, further research is essential to refine these approaches and ensure robust, long-term security for modern transportation infrastructures.

CHAPTER 3

Methods

The Methods section details the comprehensive approach undertaken to evaluate the security of TCPS and blockchain-based VANET in the context of emerging quantum threats. This section begins by presenting a case study on cryptographic vulnerabilities within a TCPS application, specifically focusing on the electronic toll collection (ETC) service as defined in ARC-IT. The analysis employs threat modeling using the Microsoft Threat Modeling Tool to identify critical vulnerabilities within the communication architecture, and discusses how these weaknesses can be exploited by quantum computing techniques. The section then transitions to an experimental evaluation of CRYSTALS-Kyber, a PQC scheme, detailing its security features, parameter sets, and performance in various wired and wireless simulation scenarios modeled using OMNeT++, INET, SimuLTE, and SUMO. Furthermore, the methods encompass a detailed description of a blockchain-based VANET threat model, including the design and implementation of an impersonation attack scheme that leverages Shor's algorithm within a quantum computing environment. This comprehensive approach integrates both classical and quantum simulation environments, as well as quantum circuit implementation using Qiskit, to validate the feasibility of the proposed attack model and assess the resilience of current cryptographic mechanisms against quantum adversaries.

3.1. PQC for TCPS Applications

3.1.1. Case Study on Cryptographic Vulnerabilities in a TCPS Application

This section aims to illustrate the vulnerabilities of current cryptographic systems in TCPS with a case study. By examining one of the Traffic Management (TM) service packages, i.e., TM10: Electronic Toll Collection (ETC), from the ARC-IT version 9.2 (United States Department of Transportation (USDOT), 2024), we highlight the potential risks posed by quantum computing to existing cryptographic mechanisms and underscore the necessity of transitioning to PQC. This analysis demonstrates how quantum attacks could exploit weaknesses in traditional cryptographic algorithms using threat modeling in the Microsoft Threat Modeling Tool 2017 (Microsoft, 2024) and provides insights into mitigating these threats using PQC solutions.

Figure 2 illustrates the data flow and communication architecture within the TM10 service package. In our threat modeling, we focus only on the communications marked inside the black dotted box in **Figure 2**. This is because, according to the ARC-IT, the other communications depicted in **Figure 2** are initiated only if discrepancies occur during toll collection, meaning they are not activated under normal operation conditions (United States Department of Transportation (USDOT), 2024). The excluded portion involves various components, including the Traffic Management Center, Department of Motor Vehicles (DMV), Enforcement Center, Financial Center, and Fleet and Freight Management Center, which interact with the Payment Administration Center for tasks such as license requests, payment violations, financial settlements, toll data requests, and toll coordination. These components handle auxiliary functions that are critical but do not participate directly in the routine toll collection process.

Within the included portion, critical communications occur to facilitate the primary functions of electronic toll collection. The components involved are the Payment Administration Center, ITS Roadway Payment Equipment, Light Vehicle On-Board Equipment (OBE), Light Vehicle Payment Service, and Payment Device. The Payment Administration Center handles payment administration requests and disseminates payment information. It communicates with the ITS Roadway Payment Equipment to process payment instructions, authorization requests, and transactions. The ITS Roadway Payment Equipment serves as an intermediary, ensuring secure transfer of payment information and authorizing payments based on the data received. The Light Vehicle OBE is responsible for updating vehicle payment information and securing payment transactions, which it performs by interacting closely with the Light Vehicle Payment Service.

This service manages toll and parking payments. The Payment Device, which could be a smart card, smartphone, or other electronic payment support devices, interfaces with the Light Vehicle OBE to actuate secure payments and update payment statuses. The red arrows in **Figure 2** represent communications/data flow that require encryption and authentication to ensure secure and reliable transactions.

Figure 2. Data flow of TM10: Electronic Toll Collection (Adopted from ARC-IT version 9.2).

We implemented the communications marked inside the black dotted box of **Figure 2** using the Microsoft Threat Modeling Tool (Microsoft, 2024). Figure 2 illustrates the data flow between the Payment Administration Center, ITS Roadway Equipment, and Light Vehicle OBE of the ETC system using the Microsoft Threat Modeling Tool. The tool generated a report on potential threats, summarized in **Table 4**. In **Figure 2**, the 'Trust Border Boundary' delineates the perimeter within which all components and communications are considered secure and trusted, assuming that internal threats are minimal or controlled. In contrast, the 'Trust Line Boundary' indicates the transition between trusted and untrusted zones, where external threats might be more likely to penetrate or where data is more susceptible to interception and tampering. The Payment Administration Center and ITS Roadway Payment Equipment are situated within the Trust Border Boundary, implying that communications between these components are generally secure.

However, the Light Vehicle OBE, which lies outside the Trust Border Boundary and is connected through wireless communications, crosses the Trust Line Boundary. This indicates a higher risk area where data transmitted between the Light Vehicle OBE and the other components may be vulnerable to external attacks.

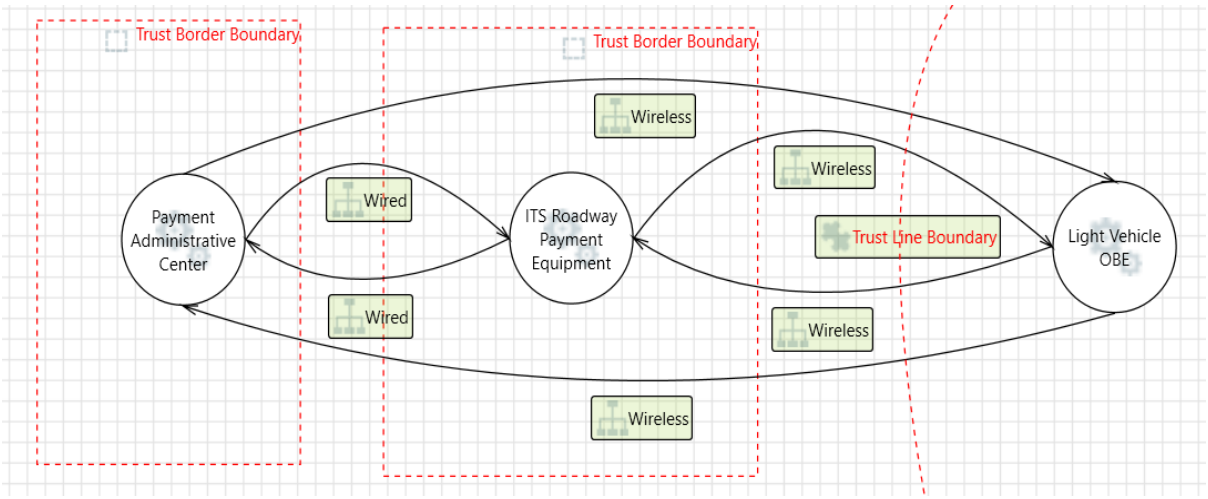


Figure 3. Data Flow between the Payment Administration Center, ITS Roadway Equipment, and Light Vehicle OBE using Microsoft Threat Modeling Tool.

Table 4. Summary of Microsoft Threat Modeling Tool Report.

Title	Category	Interaction	Priority
Weak Authentication Scheme	Information Disclosure	Wired	High
Collision Attacks	Tampering	Wired	High
Replay Attacks	Tampering	Wired	High
Elevation Using Impersonation	Elevation of Privilege	Wired	High
ITS Roadway Payment Equipment May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of Privilege	Wireless	High
Elevation by Changing the Execution Flow in Light Vehicle OBE	Elevation of Privilege	Wireless	High
ITS Roadway Payment Equipment May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of Privilege	Wired	High
Elevation by Changing the Execution Flow in ITS Roadway Payment Equipment	Elevation of Privilege	Wired	High
Payment Administration Center May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of Privilege	Wireless	High
Elevation by Changing the Execution Flow in Payment Administration Center	Elevation of Privilege	Wireless	High
Light Vehicle OBE May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of Privilege	Wireless	High

Table 4 highlights vulnerabilities that are all highly susceptible to quantum attacks. These vulnerabilities are critical because quantum computing can efficiently break the underlying mechanism of cryptographic techniques that are currently available. For example, weak authentication schemes and collision attacks have become feasible with the advent of quantum computing capabilities (Bone and Castro, 1997; Brassard, Høyer and Tapp, 1997). **Table 4** also highlights various threat categories, such as information disclosure,

tampering, elevation of privilege, denial of service, and repudiation, indicating a high priority for mitigation. Elevation of privilege using impersonation, remote code execution, and changing the execution flow in ITS Roadway Payment Equipment and Light Vehicle OBE are among the most severe threats identified.

Table 5 elaborates on the vulnerabilities identified in **Table 4**, specifically highlighting those susceptible to quantum attacks. For each vulnerability, **Table 5** describes the potential quantum attack that could be exploited, the impact of such an attack, and the suggested mitigation using PQC techniques. For example, weak authentication schemes are vulnerable to quantum attacks using Shor's algorithm, necessitating the adoption of lattice-based PQC algorithms, such as CRYSTALS-Kyber (Bos *et al.*, 2018) or Falcon ('Falcon - Fast-Fourier Lattice-based Compact Signatures over NTRU', 2024). Collision attacks can be mitigated by hash-based PQC algorithms, such as SPHINCS+ (Bernstein *et al.*, 2019), to prevent unauthorized data modifications. Replay attacks, enhanced by quantum computing, can be countered with time-based PQC protocols to ensure transaction uniqueness. Elevation using impersonation requires strong identification verification mechanisms provided by lattice-based PQC schemes to prevent unauthorized access. Finally, elevation by changing the execution flow can be mitigated through robust quantum-resistant algorithms and secure coding practices to maintain system integrity.

Table 5. Summary of Microsoft Threat Modeling Tool Report.

Vulnerability	Potential Quantum Attack	Impact	Suggested Mitigation
Weak Authentication Scheme	Shor's algorithm can efficiently factorize large integers and solve discrete logarithms, breaking RSA and ECC.	Unauthorized access and breached confidentiality	Use PQC digital signatures, such as CRYSTALS- Dilithium or Falcon
Collision Attacks	Grover's algorithm can find the pre-image of a hash function with a quadratic speedup, reducing the security level.	Data tampering	Use hash-based PQC algorithms like SPHINCS+
Replay Attacks	With compromised cryptographic protocols, attackers can intercept and retransmit valid data packets.	System manipulation, repeated transactions, and fraud	Implement time-based protocols and secure communication channels with PQC
Elevation Using Impersonation	Attackers can impersonate legitimate users or devices by breaking the underlying cryptographic keys.	Unauthorized actions and security breaches	Use PQC digital signatures, such as CRYSTALS- Dilithium or Falcon
Elevation by Changing Execution Flow	If the encryption used to secure communication is compromised, attackers can insert malicious code.	System takeover and data breaches	Secure communication with PQC algorithms and implement robust input validation and security checks (secure PQC coding practices)

In conclusion, this case study underscores the pressing need to transition to PQC to secure critical transportation infrastructures against the impending threat of quantum computing. By adopting PQC solutions, we can safeguard the integrity, confidentiality, and authenticity of essential TCPS applications, such as electronic toll collection, ensuring their resilience in a post-quantum world.

3.1.2. Experimental evaluation and security Assessment of CRYSTALS-Kyber FOR TCPS

This section presents a comprehensive evaluation of CRYSTALS-Kyber (Kyber), focusing on its applicability and effectiveness as a PQC mechanism for TCPS. Kyber has been selected for this evaluation for its robust security framework, which meets the strict demands of TCPS to ensure the integrity, confidentiality, and authenticity of critical data exchanges. Standardized by NIST on August 13, 2024, as the "Module-Lattice-Based Key-Encapsulation Mechanism," Kyber is designed to secure communication

against both classical and quantum attacks (Avanzi *et al.*, 2021). Kyber's foundational reliance on the Module Learning with Errors (MLWE) problem ensures its resistance to quantum algorithms such as Shor's Algorithm, which compromise traditional cryptographic schemes, such as RSA and ECC. Additionally, its compliance with advanced security standards, such as IND-CCA2, highlights its ability to prevent adaptive chosen ciphertext attacks, which is essential for maintaining the integrity of TCPS communication networks.

To analyze Kyber's effectiveness comprehensively, this section integrates both the security and performance perspectives. The following subsections begin by discussing Kyber's critical security features to support TCPS, including its foundational strengths, resistance to known attack vectors, and a discussion on the resource estimates required to breach its defenses. Subsequently, the experimental setup and simulation scenarios used to evaluate Kyber's performance across diverse peer-to-peer (P2P) communication networks in TCPS are detailed. This comprehensive evaluation demonstrates Kyber's feasibility as a foundation of PQC for securing critical TCPS applications.

3.1.2.1. Security Features of Kyber to Support TCPS

3.1.2.1.1. Fundamental Security Features

Kyber's security derives from the hardness of the MLWE problem, a lattice-based problem resistant to classical and quantum attacks (Bos *et al.*, 2018). Unlike RSA and ECC, which are vulnerable to Shor's algorithm, Kyber's lattice-based structure remains secure due to its inherent complexity of solving lattice-based problems. This complexity is further reinforced by Kyber's carefully chosen parameter sets, which balance cryptographic strength, computational efficiency, and decryption failure probability. These parameter sets play a crucial role in ensuring Kyber's robustness against cryptanalytic attacks, including brute-force attack accelerated by quantum algorithms, such as Grover's algorithm (Avanzi *et al.*, 2021).

Table 6. Parameter Sets for Kyber (Avanzi *et al.*, 2021)

Kyber variant	n	k	q	η	τ	(d_u, d_v)	δ
Kyber-512	256	2	3329	3	2	(10, 4)	2^{-139}
Kyber-768	256	3	3329	2	2	(10, 4)	2^{-164}
Kyber-1024	256	4	3329	2	2	(11, 5)	2^{-174}

Kyber defines three parameter sets for three different Kyber variants, i.e., Kyber-512, Kyber-768, and Kyber-1024, corresponding to NIST security levels 1, 3, and 5, respectively (**Table 6**). Each parameter set specifies the following critical values (Avanzi *et al.*, 2021):

- n: Polynomial degree, fixed at 256 for all variants, which defines the size of the polynomial ring used in Kyber. This choice ensures computational efficiency and high levels of security.
- k: Number of polynomials in the key and ciphertext. This parameter scales with the desired security level, with higher values of k providing greater cryptographic strength (e.g., $k = 2$ for Kyber-512 and $k = 4$ for Kyber-1024).
- q: Modulus for polynomial coefficients, fixed at 3329 for all variants. This modulus prevents coefficient overflow while preserving the hardness of the MLWE problem.
- η: Error distribution parameter that introduces noise into the MLWE framework, adding cryptographic strength by obscuring the relationship between plaintext and ciphertext.
- τ: Number of noise terms sampled during the key encapsulation process, ensuring additional randomness and robustness against attacks.
- d_u, d_v: Bit lengths for compressing the ciphertext components u and v. These compression parameters optimize the storage and transmission of ciphertexts without compromising security.

- δ: Decryption failure probability, representing the likelihood of decryption errors. Kyber's parameter sets ensure that δ remains negligible, ensuring compliance with stringent security standards.

Kyber's use of the above parameter sets ensures its compliance with high standards for IND-CPA and IND-CCA2 security (Avanzi *et al.*, 2021). CPA security ensures that attackers cannot infer plaintext information from the ciphertext, protecting initial key exchanges. CCA security protects against active attacks where manipulated ciphertexts could otherwise expose the system to vulnerabilities. These properties are critical for TCPS, ensuring data integrity and authenticity in dynamic environments susceptible to tampering and eavesdropping.

3.1.2.1.2. Core SVP Estimates, Resistance to Primal and Dual Attacks, and Quantum Resource Requirements for Kyber

The security of Kyber is further quantified through Core SVP estimates, which indicate the computational difficulty of solving its lattice problems. These estimates are derived based on the complexity of primal and dual attacks, which are the two main methods used to attack lattice-based cryptographic schemes (Albrecht, Player and Scott, 2015; Laarhoven and Walter, 2021; Zhang, Zheng and Wang, 2022). Primal attacks focus on directly recovering the secret key by finding the shortest vector in the lattice that corresponds to the error term in Kyber's MLWE framework. Advanced lattice reduction techniques, like the Block Korkine-Zolotarev (BKZ) algorithm and lattice sieving, are employed to approximate this vector (Ducas, 2017; Mariano *et al.*, 2017; Miller, 2020; Tateiwa *et al.*, 2024). Dual attacks, on the other hand, aim to distinguish between encrypted vectors and random noise by exploiting structural discrepancies in the lattice. Techniques, such as Fourier analysis and lattice sieving, are employed to construct distinguishers capable of isolating distinctive distributions within the MLWE framework (Albrecht, 2017; Chunhuan *et al.*, 2019).

The Core SVP estimates for Kyber-512, Kyber-768, and Kyber-1024 (**Table 3)** reflect their resistance to known attacks, quantifying the computational effort required to compromise their security. For instance, Kyber-512 has a Core SVP estimate of 118 bits in the classical setting and 107 bits in the quantum setting, requiring approximately 2^{118} classical or 2^{107} quantum operations to compromise its security. Higher variants, such as Kyber-1024 offer even greater security margins, i.e., Core-SVP estimates of 256 bits in a classical setting and 236 bits in a quantum setting, making them ideal for TCPS where stronger security is critical.

Furthermore, these Core SVP estimates align closely with NIST-defined security levels for PQC schemes (**Table 2**), which are benchmarked against the equivalent security provided by AES. Specifically, NIST Security Level 1 corresponds to the security of AES-128, Level 3 to AES-192, and Level 5 to AES-256. Kyber-512, Kyber-768, and Kyber-1024 are designed to meet these security levels, respectively, offering protection analogous to their AES counterparts. For example, based on studies by Gheorghiu and Mosca (2025), a quantum attack using Grover's algorithm on AES-256, which provides NIST Security Level 5, would require approximately 2^{240} physical qubits and 2^{205} quantum CPUs operating in parallel for one year, assuming a very low physical error rate (Gheorghiu and Mosca, 2025). Similarly, AES-192 (NIST Security Level 3) demands approximately 2^{165} physical qubits and 2^{140} quantum CPUs, while AES-128 (Security Level 1) requires approximately 2^{100} physical qubits and 2^{80} quantum CPUs for the same attack duration (Gheorghiu and Mosca, 2025). Mapping these requirements to Kyber, the resource demands for compromising Kyber-1024 align with AES-256, demonstrating Kyber's robustness at Security Level 5 against quantum adversaries. Similarly, Kyber-768 and Kyber-512 reflect the computational challenges associated with AES-192 and AES-128, respectively, aligning with their respective security levels.

However, current quantum computing capabilities fall significantly short of these requirements. For instance, IBM's quantum roadmap and similar efforts by Google and Quantinuum project quantum systems scaling to thousands of qubits over the coming years ('IBM Quantum Roadmap', 2024; 'Google Quantum

Computing Roadmap', 2024; 'Quantinuum Quantum Computing Roadmap', 2024). Despite these advancements, the projected systems remain orders of magnitude below the 2^{240} physical qubits and 2^{205} quantum CPUs needed to compromise Kyber-1024. Even for Kyber-512, the minimum physical and computational requirements far exceed the capabilities of existing or near-term quantum computers. This contrast between resource requirements and current projections highlights the immense resilience of Kyber against foreseeable quantum threats. As a result, Kyber remains a robust and practical PQC solution for securing critical systems like TCPS, where long-term data protection is paramount.

3.1.2.1.3. Resistance to Algebraic and Symmetric Primitive Attacks

Kyber also exhibits strong resilience to algebraic attacks (Avanzi *et al.*, 2021). Quantum algorithms targeting the Ideal Shortest Vector Problem (Ideal-SVP) (Biasse and Song, 2016; Cramer, Ducas and Wesolowski, 2016) face significant computational challenges when applied to Kyber's MLWE structure, which is more complex than simpler lattice types like Ring-LWE. The additional complexity ensures that Kyber's cryptographic foundation remains secure against these advanced algebraic attacks (Avanzi *et al.*, 2021). Kyber's use of symmetric functions, particularly Keccak-derived algorithms, such as SHAKE-128 and SHAKE-256 (Bertoni *et al.*, 2013), enhances its resistance to cryptanalysis by providing strong pseudo-randomness, high resistance to differential and linear attacks, and robustness against quantum adversaries due to their well-studied and secure design (Avanzi *et al.*, 2021). These functions are critical for key encapsulation and pseudorandom generation, providing robust protection against both classical and quantum adversaries.

3.1.2.1.4. Protection against Decryption Failures

Kyber minimizes decryption failure probabilities, a key aspect of maintaining CCA security (Avanzi *et al.*, 2021). Low decryption failure rates reduce the risk of attackers exploiting modified ciphertexts to infer secret keys. For example, Kyber-512 has a decryption failure probability of approximately 2^{-69} (2^{-82} for Kyber-768 and 2^{-87} for Kyber-1024) under quantum assumptions (Bos *et al.*, 2018; Avanzi *et al.*, 2021). Specifically, this means if an attacker attempts to exploit this probability, they would need to submit 2^{69} ciphertexts to statistically observe at least one decryption failure that might reveal sensitive information, ensuring that Grover's algorithm cannot feasibly exploit this vulnerability. These design choices reinforce Kyber's reliability in high-stakes environments like TCPS, where secure communication is essential.

For TCPS, this assessment underscores the strong security features and robustness of Kyber's lattice-based cryptographic mechanisms. Furthermore, the immense physical qubit and quantum processor requirements for breaking Kyber, which remain far beyond the current capabilities of quantum technology, suggest that Kyber could remain a secure PQC option for encrypting sensitive data and ensuring authentication within TCPS applications. This includes safeguarding communication in ITS and V2X networks, where low-latency and high-reliability security protocols are paramount. Thus, the alignment of Kyber's inherent security features, resistance to known attack vectors, and compatibility with the projected limitations of quantum computing reinforces its viability as a quantum-resistant solution for critical infrastructure protection in TCPS. To further evaluate Kyber's practical applicability, the next section delves into the simulation scenarios and experimental setup used to test its performance in diverse P2P communication networks within TCPS. These simulations provide critical insights into Kyber's operational feasibility in real-world environments.

3.1.3. Simulation Scenarios and Setup

For the simulation of the Kyber KEM within a P2P communication network, Objective Modular Network Testbed in C++, also known as OMNeT++ ('OMNeT++ Discrete Event Simulator', 2023) was selected as the simulation platform. offers a modular and extensible architecture that is well-suited for implementing

custom cryptographic protocols. Furthermore, the platform's scalability and robust visualization tools enable detailed performance analysis, which is essential for evaluating the feasibility of Kyber in practical communication network scenarios. We implemented the INET framework ('INET Framework', 2023) to our OMNeT++ environment to provide a comprehensive suite of internet protocols, which enabled realistic modeling of both wired and wireless P2P networks. Additionally, SimuLTE (Virdis, Stea and Nardini, 2014) was implemented to simulate LTE-based wireless communication scenarios, allowing for the evaluation of Kyber in wireless cellular environments. Specifications of simulation parameters are presented in **Table 7**.

Table 7. Simulation Environment Setup

Parameter	Details/Specification
Main Machine	Intel(R) Core (TM) i7-7700 CPU @ 3.60GHz
Virtual Machine	Instant-veins-5.2-i1
Operating System (OS) of the Virtual Machine	Debian 11, Linux 5, GNOME 3
Number of CPU for the Main Machine	8
Number of CPU assigned to the Virtual Machine	8
RAM size for Main Machine	32 Gigabytes (GB)
RAM size for Virtual Machine	24 GB
Time per clock cycle	0.29 nanoseconds (ns)
OMNeT++ version	5.7
INET Framework version	4.2.8
SimuLTE version	1.2.0

We simulated four different scenarios to analyze the performance and applicability of Kyber in TCPS P2P communication. First, we evaluated wired communication between two static nodes. This represents the wired Ethernet communication between two stationary nodes in TCPS, for example, the communication between the Payment Administration Center and DMV in ARC-IT service package TM10: Electronic Toll Collection, as shown in **Figure 2**. Then, we evaluated wireless communication between two static nodes. We can consider the communication between ITS Roadway Payment Equipment and the Payment Administration Center in TM10 as an example of this. After that, we evaluated wireless communication between one static and one dynamic node. We can consider the communication between ITS Roadway Payment Equipment and a moving vehicle as an example of this. Finally, we evaluated wireless communication between two dynamic nodes, which can be depicted as the communication between two moving vehicles, for example exchanging BSMs between two connected vehicles. These four scenarios depict all the possible P2P communication in TCPS and are illustrated in **Figure 4**.

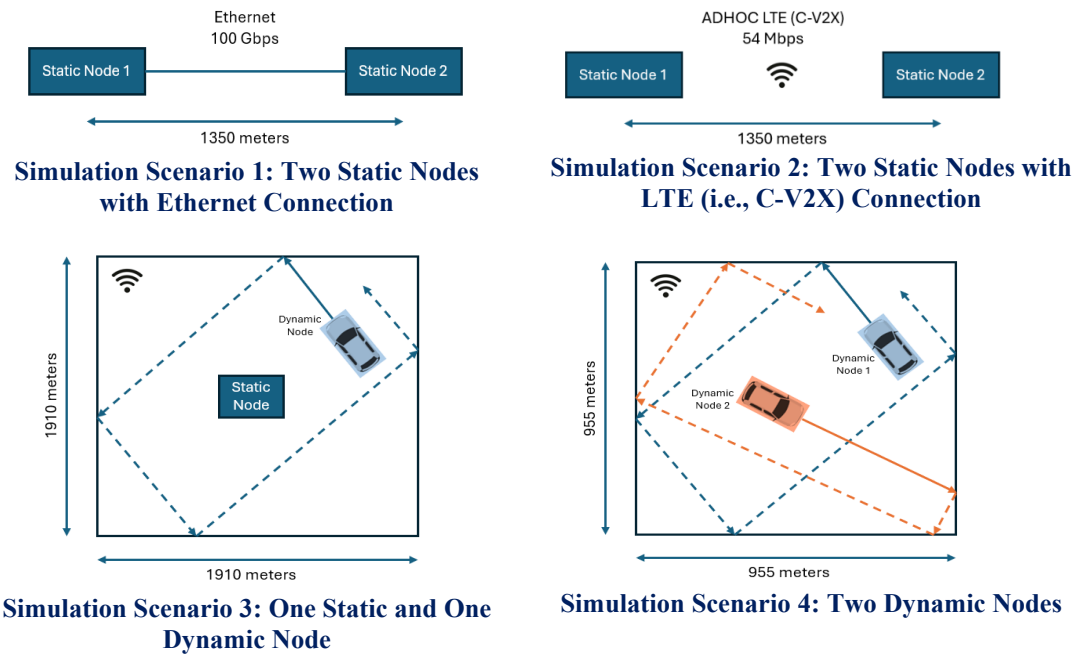


Figure 4. Simulation Scenarios for Evaluating Kyber in Wired and Wireless Communication Networks in TCPS.

The distances and mobility configurations for each scenario were designed to align with real-world TCPS communication requirements. For scenarios 1 and 2, involving two static nodes, the distance between the nodes was set to 1350 meters, reflecting the typical communication range of Cellular Vehicle-to-Everything (C-V2X) technology (Qualcomm Technologies, no date). While this distance is not a limiting factor for Ethernet-based communication due to its high bandwidth and low-latency characteristics, we adopted the same configuration to maintain consistency across all scenarios and facilitate a fair comparison between wired and wireless setups. In scenarios 3 and 4, where dynamic nodes were introduced, a linear waypoint mobility model was employed to simulate their movement within defined bounding boxes ('INET Mobility Models', no date). Each dynamic node moved at a constant speed of 40 meters per second, a value representative of typical freeway speeds.

For simulation scenario 3, the static node was placed at the center of a bounding box with sides measuring 1910 meters. This configuration ensured that the maximum distance between the static and dynamic nodes was 1350 meters, occurring when the dynamic node was positioned at the corner of the bounding box. In simulation scenario 4, the bounding box was reduced to 955 meters on each side, ensuring that the maximum distance between the two dynamic nodes remained 1350 meters when they occupied opposite corners of the box. These configurations allowed for a realistic evaluation of communication performance under varying mobility and distance constraints.

For wired communication, we utilized the Ethernet with a bandwidth of 100 Gigabits per second (Gbps), providing a high-speed, low-latency network suitable for modern TCPS infrastructure. In our wireless communication simulations, we employed ad hoc LTE with a bandwidth of 54 Megabits per second (Mbps). This choice aligns with data rates observed in real-world LTE networks under typical operating conditions. Ad hoc LTE represents peer-to-peer C-V2X communication, enabling direct communication between vehicles and other devices without relying on network infrastructure. For instance, the IEEE 802.11g standard, operating in the 2.4 GHz band, supports a maximum data rate of 54 Mbps, which is commonly utilized in ad hoc network configurations (Ho, Tweed and Le-Ngoc, 2017). Additionally, studies have

shown that LTE networks can achieve data rates up to 54 Mbps in various scenarios, including vehicular networking applications (Hameed Mir and Filali, 2014). These data rates are consistent with moderate network congestion and typical signal strengths found in urban and suburban environments.

To implement the cryptographic operations, the liboqs library ('liboqs', 2024) was employed for Kyber KEM, and OpenSSL ('OpenSSL', no date) was utilized for AES-256 for symmetric key encryption and decryption. First, a shared secret key was established between the two peers using Kyber. One peer generated a Kyber public-private key pair and shared the public key with the other peer, while keeping the private key securely stored. The second peer used the received public key to generate a ciphertext and a shared secret key. The ciphertext was then transmitted back to the first peer. Upon receiving the ciphertext, the first peer used its private key to recover the shared secret key, ensuring that both peers possessed the same shared secret key. After establishing the shared secret key, each peer utilized that key to encrypt and decrypt data (32-byte message) with AES-256 symmetric cryptographic scheme. AES-256 was chosen because, even if an attacker with a quantum computer attempts to decrypt the ciphertext using Grover's algorithm, AES-256 could still provide 128 bits of security (i.e., 2^{128} brute-force iterations to break the ciphertext). The simulation was conducted with all three Kyber variants, e.g., Kyber-512, Kyber-768, and Kyber-1024, to analyze the computational and communication overhead associated with different key sizes. Key sizes and ciphertext payload sizes were matched to the specifications of Kyber's three variants (see **Table 3)** for consistency. To simplify the analysis, the effect of packet fragmentation was not considered. Instead, payload sizes were set to correspond directly to the public key and ciphertext sizes of each cryptographic scheme.

3.2. Blockchain-Based VANET and Threat Model

This section presents an architecture of blockchain-based VANET and identifies its vulnerabilities against an attack that uses quantum computers.

3.2.1. Blockchain-based VANET Architecture

The blockchain-based VANET architecture has not been standardized yet. However, two different mechanisms, i.e., PoW and PoS based consensus (Li *et al.*, 2019; Yang *et al.*, 2019), are available in literature for implementing VANET architecture. Unlike PoW, which requires the computational power for solving cryptographic puzzles (i.e., solving SHA-X), PoS considers all the vehicles as stakeholders of the system, and trustworthy vehicles or randomly selected vehicles to be considered as the 'Miner' criteria. In PoW and according to the consensus mechanism, a vehicle sends a traffic crash warning message, and it goes to the "Mempool" of the RSU/Miner. The Mempool is where the unauthenticated messages or transactions stay as long as there are no similar reports from other vehicles regarding the message (Diallo *et al.*, 2021). On the other hand, the consensus mechanism of PoS checks the traffic crash message with other vehicles' (stakeholders') consensus/opinion about the message and finally validated by validators/miners. PoS can find malicious transaction through horizontal trust (HT) in V2V communication and vertical trust (VT) in V2I communication (Achref Haddaji, Ayed and Fourati, 2020).

The trust-chain is a trust-based blockchain architecture with asymmetric encryption to identify ownership using the digital signatures of the vehicles and their trust values, which increase with every authenticated transaction. A trust chain-based blockchain architecture verifies authenticity in two steps. Firstly, it verifies the ownership of the digital signature that is encrypted with RSA/ECDSA. Secondly, it checks the authenticity of the message using the consensus mechanism. As presented below in **Table 8**, system configuration can be defined from the enrollment, transaction handling, consensus mechanism, storing the authentic request to blockchain record, miner/validator selection, trust value calculations and blocking of malicious vehicles after some transactions, which act as fault tolerance threshold. Based on the above

definitions, attacks can be defended through authentication, transparency and non-repudiation nature of blockchain networks. For example, a vehicle with vehicle ego-motion information with false trajectories (e.g., speed-difference and distance), false digital signature, or false information about a traffic crash can be identified using a consensus mechanism.

3.2.2. Threats and Vulnerabilities of a Blockchain-based VANET

The threats to a blockchain-based VANET system can be considered low if the trustworthiness of the system is maintained. Tempering of data and sniffing in ongoing VANET conversations (V2V and/or V2I) are considered less possible because of trustworthy encryption, such as RSA, hashing of the data, and distributed transparent ledger. However, the digital signature of a vehicle, which is part of each disseminated message, can be used to create an attack algorithm that uses quantum computers and makes a trust-based system vulnerable and can have a catastrophic impact on VANET, even creating the possibility of multi-vehicle collisions and changing the routes of vehicles. As illustrated in **Figure 1**, a general attack scenario on the PoS mechanism is presented, where a malicious vehicle generates a false message. Through the blockchain's consensus mechanism, the malicious activity is detected, tracked, and ultimately blocked. Then, a digital signature from disseminated packets of RSU is used to forge the digital signature of a legitimate vehicle.

Table 8. Components and Their Corresponding Functionalities for Blockchain Based VANET

System architecture components	Description
Enrollment to the blockchain network	System interactions with blockchain network is initialized by all the agent nodes (vehicles as moving nodes and RSU's act as static nodes) downloading and updating following the architecture presented in (Shrestha *et al.*, 2020) and the blockchain as a module (as Certificate Authority based authentication is not needed for PoS based architecture) with digital signature generated by RSU. Current blockchain transaction history has also been downloaded with respective trust values when a new vehicle joins the architecture
Transaction handling	There is a forward dissemination of packets from RSU (local administrator) to all vehicles within its wireless communication coverage to let every other vehicle know about any transactions and corresponding trust values to vote for the transaction authenticity.
Consensus mechanism	Voting is conducted by horizontal trust result (trusted=1 and not trusted=0) created by every transaction, which is sent to RSU (as VT step) for consensus. RSU calculates majority voting (greater than the threshold trust value) for every transaction and classifies malicious transactions. This threshold changes with increasing trust of the vehicles.
Blockchain record	Verified transactions with the approval of stakeholders are stored in the blockchain as a new block by the validator and dissipated to every agent node to maintain transparency in local blockchain module.
Miner/validator selection	To generate a block, entities called miners/validators (special agent nodes) with high trust value verifies in accordance with RSU's trust result, writes verified data to new block of blockchain in accordance to defined rule (threshold in voting or trust value calculation) through smart contracts. A vehicle with the highest trust value (the highest stake value) or a randomly selected vehicle (if many vehicles have the same trust value) serves as a validator/miner in PoS.
Trust value calculation	This trust value offset has been calculated as described in the reference (Yang *et al.*, 2019). Trust value can be increased with every vehicle authenticity check and message validation (adds 5 per transaction in this report), with identifying false transactions (adds 10 per transaction), and with adding new validators/miners (20 for mining) upon writing onto the block. If a malicious vehicle tries to do double spending with the same gas value (i.e., compensation value for a transaction to store in a block), it can be identified too.
Block malicious vehicle	The RSU blocks the malicious vehicle after a threshold of transactions. Trust values are carried to other RSUs, and if a vehicle is blocked by any RSU, it cannot enter a new block of other RSUs.

A malicious vehicle creates an impersonation attack by broadcasting a false message of a traffic crash with the forged digital signature. The system tries to block malicious vehicle identification through the digital signature with the majority votes of the stakeholders. In this way, a blockchain-based VANET blocks a "legitimate" vehicle as a malicious vehicle. So, with quantum computers (M Bayat *et al.*, 2020), if we can figure out and break the encryption, such an attack would be possible (Bard, Kearney and Perez-Delgado, 2022). An attacker gains the trust of the system, gets miner responsibilities, and verifies malicious transactions as authentic messages. Thus, the consensus of majority voting fails to remove the malicious vehicle as it has more stakes in the system by adding and verifying malicious vehicles as legitimate vehicles (increasing trust values) and using their votes to influence the system. The attacker starts double spending the initial gas amount at the beginning and spams the VANET with more false messages. The PoW mechanism also acts on the consensus mechanism using the consensus mechanism in an unauthenticated mempool (Diallo *et al.*, 2021). A malicious vehicle can report the same traffic crash with other vehicles' digital signatures and authenticate the message. An attacker could have 10 minutes to either figure out how to crack the puzzle to act as a miner using Grover's algorithm (F A Ghaleb *et al.*, 2023) or the digital signature using Shor's algorithm utilizing quantum computers of other vehicles to spread the traffic crash notification from the mempool.

3.2.3. Impersonation Attack Scheme

Our attempt to breach the blockchain's trust mechanism originates from the vulnerabilities associated with asymmetric cryptography, or public-key cryptography method. In asymmetric cryptography, a sender employs their private key (SK) to sign a transaction intended for recording on the blockchain, generating a digital signature. Subsequently, the sender broadcasts the transaction along with their public key (PK). The public key serves as a means for receiving nodes to validate that the digital signature originates from the rightful person. Asymmetric cryptography relies on either prime number factorization or the discrete logarithm problem to generate these key pairs. If one can break this algorithm with Shor's algorithm, it is possible to forge the private key and hence forge the digital signature. With the forged private key or digital signature, a sender (i.e., a malicious vehicle) broadcasts false messages or transactions to other legitimate vehicles and corresponding RSU within its communication range in the blockchain. These private-public key pairs are formed using the prime factorization in RSA. By using Shor's algorithm implemented in a quantum computer, a malicious vehicle can guess the prime factor and figure out the private key, thus forming the attack scheme.

This section presents an attack scheme that will be used to launch an impersonation attack using Shor's algorithm implemented in a quantum computer on a blockchain-based VANET. In this scheme, the trust chain's dependency on the corresponding trust value is exploited to detect any discrepancy by verifying the digital signatures and messages. **Figure 5** presents an impersonation attack scheme against trust-based architectures using quantum Shor's algorithm, which is a sub-process to forge the digital signature and use it to broadcast a false message (e.g., traffic crash) with a forged digital signature. An attacker checks if the system is PoW-based architecture or not, as it must decide if there is a time constraint (key refresh time and block interval) for the attack to be successful. An attacker with a forged digital signature sends out false messages and gains trust by pinning its blame on legitimate vehicles using their forged digital signatures. As a malicious vehicle takes on the miners'/validators' responsibilities, it will improve the trust values of new malicious vehicles and help to get a majority in voting. A double-spending attack happens when it sends multiple transactions with the same gas value to save up its transaction limits (see **Table 8** for more details).

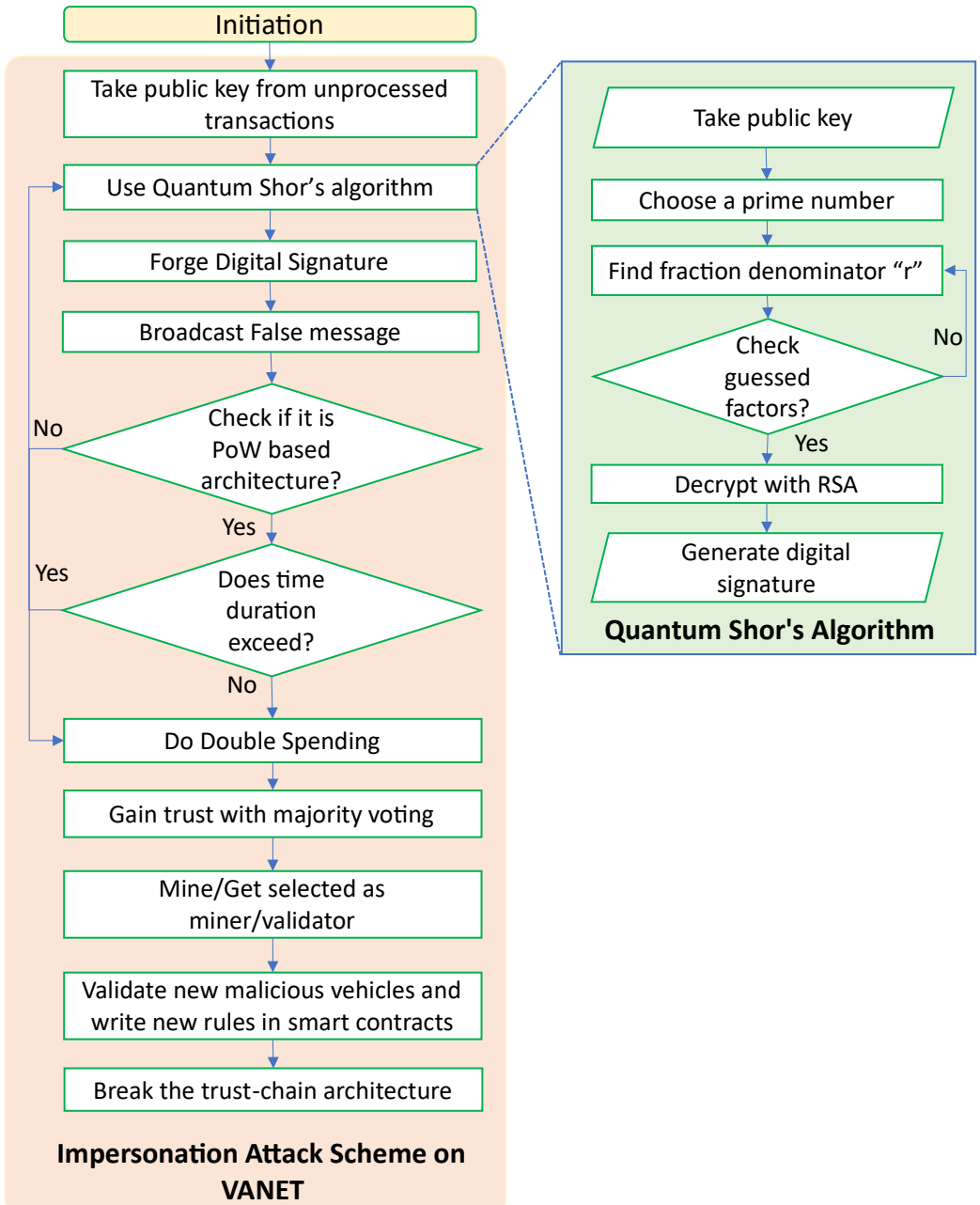


Figure 5. Impersonation attack scheme using Shor's algorithm implemented in a quantum computer for blockchain-based VANET.

As a subprocess, Shor's algorithm implemented uses period finding (phase) in superposition states to perform modular exponentiation in polynomial time (see **Figure 5**) to break RSA. Note that Shor's algorithm uses the Quantum Fourier Transform (QFT) to find the period of a modular multiplication function efficiently. The modular multiplication function takes two integers, say m and x, and computes the remainder of the product of m and x divided by some modulus, N. In other words, it computes $m^x \ mod\ N$. To factor a composite number N using Shor's algorithm, we first choose a random prime number m between 1 and N-1. Then we apply the modular multiplication function repeatedly to compute $m^x \ \ mod\ N$ for a series of values of x until we find two values of x, say x_1 and x_2, such that $(m^{x_1}$ mod $N)$

$= (m^{x_2} \bmod N)$. The period of the modular multiplication function is then given by the difference between x_1 and x_2, i.e., $p = x_1 - x_2$. Finding the period, *p,* is the key step in Shor's algorithm, and it can be done efficiently using QFT. The QFT is a quantum version of the classical Fourier transform, which is a mathematical tool for analyzing periodic functions. By applying the QFT on the superposition states corresponding to the outputs of the modular multiplication function, the algorithm can find the period . If the phase is odd or check $m^{\frac{r}{2}}$ (*m* is a prime number) and it is congruent to 1 (mod *N*, where *N* is a public key), it is in the order of *r/2* (*r* is a fraction denominator). Then, the $GCD(m^{(\frac{r}{2}-1)}, N)$ *and* $GCD(m^{(\frac{r}{2}+1)}, N)$ are applied to obtain prime factors of *N*.

3.2.4. Experimental Setup and Implementation

In order to validate the effectiveness of the impersonation attack using Shor's algorithm implemented in a quantum computer, the performance evaluations of a blockchain-based VANET are conducted utilizing a simulation platform, i.e., Objective Modular Network Testbed in C++ (OMNET++) (OMNeT++ Discrete Event Simulator, no date b; Haddaji, Ayed and Fourati, 2020).

3.2.4.1. VANET Setup

For implementing this simulation platform, the simulation environment is divided into three modules: mobility, VANET, and quantum computing, as shown in **Figure 6**. To set up the mobility module, we used Simulation for Urban Mobility (SUMO) (*Eclipse SUMO - Simulation of Urban MObility*, no date), which interacts with VEINS (*Veins - Vehicles in Network Simulation*, no date) and contains the road network and vehicle trajectory information. Overall, we simulated blockchain-based VANET using OMNET++, extended INET (*INET Framework - INET Framework*, no date) library for V2V and V2I communication, as well as VEINS and SUMO for vehicular mobility. VANET has been tested and implemented using OMNET++ 5.6.2 version with the help of SUMO.

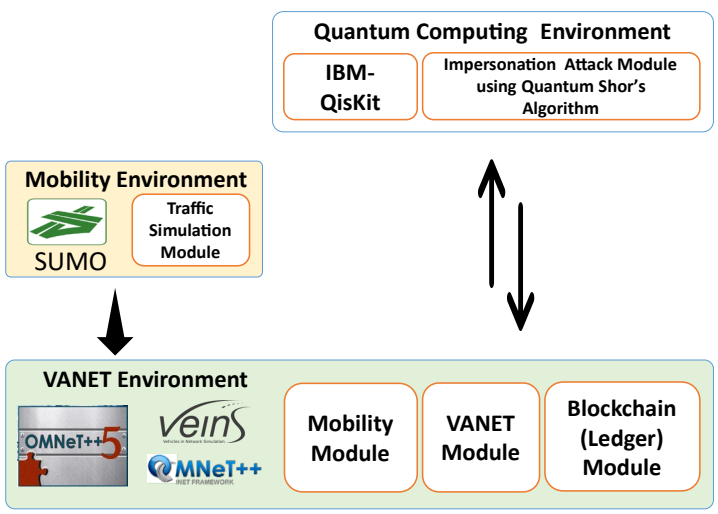


Figure 6. Block diagram of system interaction architecture.

The VEINS (5.21 version)-SUMO integration has been done to set up the simulation of a traffic crash scenario. INET (version 4) is used to implement V2RSU (V2I) and V2V communication. Our experimental scenario is limited to four vehicles and a RSU to serve as proof of concept. In this setup, the attack propagates throughout the entire simulation due to the interoperability of the trust chain facilitated by message passing through a RSU. The vehicles provide consensus, while the RSU acts solely as a local administrator without participating in the voting process. Therefore, this constraint on network size does

not impede the validity of the proof of concept. We implement the blockchain using C++ in OMNET++ with five nodes, where four moving nodes act as vehicles and one static node, i.e., RSU. In the omnetpp.ini file, we declare the simulation conditions, initial money, data rate, connectivity protocols, delays, number of malicious vehicles, and number of malicious transactions (acts as fault-tolerance limit, considered two in our simulation). In the network (.ned) file, we declare all the V2V and V2I communication protocols. In the vehicle files (vehicles and RSU), we define the message relay, packet generation (packet length, packet type, digital signatures, timestamp, hashed messages), receive, acknowledgment, block creation request, verification, and routing information. The success of the trust chain depends on successfully decrypting, validating, and verifying authenticated messages and finding malicious transactions and suspected vehicles at any point in time. We generate log messages (timestamp and trust value) for every transaction within the blockchain-based VANET. The RSU aggregates the voting of every vehicle to make malicious vehicle identification decisions as per the consensus mechanism.

As illustrated in **Figure 7**, after downloading the blockchain module and joining the network, every vehicle's onboard unit (OBU) has three modules: mobility, VANET, and local blockchain ledger. The mobility module consists of the roadway network and the vehicle's trajectory information. The VANET module enables V2V and V2I communication. The blockchain ledger module consists of records of transactions that contain a digital signature, a message, a timestamp, and transaction value details. Each vehicle uses the blockchain ledger module to send votes for each transaction. The RSU has the VANET module as it receives messages and disseminates transaction messages. It also contains a ledger module, which checks authenticity using majority voting, and maintains a list of suspected vehicles and their corresponding block lists. We use VEINS and SUMO to generate vehicle trajectory information. A dedicated ledger module is coded in OMNET++, and INET is used for VANET communication. For each message, a sender (a vehicle or an RSU) generates a packet, encrypts it with RSA using an asymmetric key, and broadcasts it to a receiver (a vehicle or a RSU). This communication between a sender and a receiver will be stored in their respective ledgers. This ledger information consists of their transaction value, which is a gas value as defined above, their digital signature, message, and timestamp. If both sender and receiver are vehicles, these transaction details are also sent to the RSU by the receiver, and the RSU disseminates this transaction to other vehicles to maintain consistency in the ledgers of other vehicles. Each vehicle generates the creditability of this transaction and uploads its trust value using either "1" or "0." Here, "1" represents a trusted transaction, and "0" represents a non-trusted transaction.

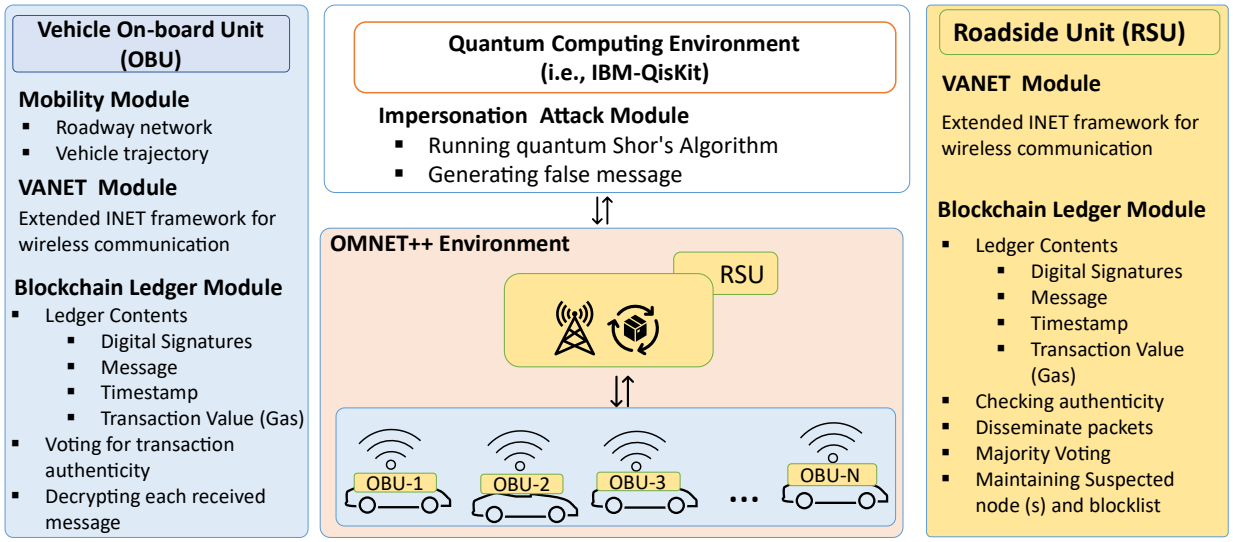


Figure 7. Implementation of impersonation attack model utilizing Shor's algorithm implemented in a quantum computer.

The RSU then checks the transaction's digital signature and corresponding gas value for double spending scenarios. In addition, the RSU checks the overall authenticity of the transaction, and the corresponding message based on majority voting. The trustworthiness of each transaction is decided based on a trust threshold value. If trusted, it increases the trust value of the overall system; otherwise, it puts the vehicle on a suspected list. At least two transactions are needed to identify a malicious vehicle as fault tolerance, block it, and pass it to other RSUs. The transaction value (or gas spent in every transaction) and trust value are calculated. The key parameters related to Shor's algorithm-based attack model are provided in **Table 9**.

Table 9. Key Parameters.

Parameters	Values
Number of vehicles	4
Number of RSU	1
Packet size	100 bytes
Encryption type	RSA
Hash algorithm	SHA-256

3.2.4.2. Blockchain Setup

Incorporating the trust chain architecture into OMNET++, the system features a non-blocking transaction system designed for efficient communication among agents, supporting multiple simultaneous transactions. Each agent owns and maintains their data, establishing local trust levels for scalability and stable performance. Every transaction creates a new block encompassing transaction data, previous block information, sequence numbers, public keys, and digital signatures. Initiated by the genesis block, the ledger progresses with subsequent blocks and agreed-upon transactions (using the consensus mechanism), ensuring transparency and security in a decentralized network.

In a network of five nodes, including one static RSU and four vehicle nodes, trust-chain facilitates transactions through four operations in each vehicle: (i) transaction request (TR), (ii) chain request (CR), (iii) chain replay message (CRM), and (iv) transaction confirmation (TC); and four operations in each RSU: (i) transaction verification (TV), (ii) dissemination (DM), (iii) chain verification (CV) and (iv) chain confirmation (CC). The initialization step sets up parameters, initializes structures, and registers signals for logging. Incoming messages initiated by each vehicle go through the transaction request (TR) process. Then, the messages are processed by RSU with the transaction handling, taking various actions such as transaction verification (TV), dissemination (DM), chain verification (CV) and chain confirmation (CC) based on message types like transaction or chain requests.

To ensure blockchain integrity, local and global logs are maintained in the log database, preventing duplicate entries. The RSU validates received transaction information against the global chain, and the vehicle checks its validity or duplicity against the local chain. The RSU oversees the successful dissemination of messages to vehicles through acknowledgement. At the TV step, the RSU checks authentication of messages. The system fortifies against malicious nodes through various functionalities, including randomized hashed addresses in the CR process, verification of digital signature in TV, and setting up public-private keys in initiation. With the voting phase in TC, the local and global trust levels are calculated, determining the threat levels of nodes. To ensure a message doesn't sit on the unprocessed transactions indefinitely, the chain records the start and end timings of transactions and discards the request after 10 minutes. Note that the simulation stops if malicious transactions by an entity (vehicle or RSU) exceed a threshold number of malicious transactions.

Trust-chain's gas values, equivalent to the concept of transaction fees in Ethereum (ETH), are dynamically calculated based on the complexity and resources required for transactions. Unlike Ethereum's fixed gas fees, trust-chain employs a flexible gas pricing model that adjusts based on network demand and computational intensity. This approach ensures cost-efficient transactions while accommodating varying computational loads. In this simulation, we considered a gas value of 100 ETH. Since an Ethereum transaction typically consumes 21,000 units of gas and the base fee is established at 10 gwei (a smaller unit of Ether), the calculation for gas per transaction amounts to (21,000 * 10) = 210,000 gwei [transaction fee = (gas unit * (base fee per gas + max priority fee per gas)] as per (*Transactions | ethereum.org*, no date), which is equivalent to 0.00021 ETH. The maximum priority fee is assumed to be 0 for this scenario. As a result, this simulation has the capacity to accommodate a number of transactions within the specified fee parameters to accommodate this simulation. The adversary detection model assumes any node may be malicious, with trust-chain tested under adversarial conditions involving false message injection and double-spending attacks at intervals to evaluate performance.

3.2.4.3. Quantum Computing Environment Setup

In our quantum simulation, we employ a small key RSA-based message encryption implemented in the Qiskit software development kit (SDK), which is part of the IBM Quantum environment (A Haddaji, Ayed and Fourati, 2020). RSA-based encryption utilizes prime factorization through Shor's algorithm to forge digital signatures of neighboring vehicles. The quantum Shor's algorithm is applied to decipher the digital signature of the sender, allowing the generation of false messages with forged digital signatures for creating an impersonation attack within the VANET. The IBM Quantum Lab (L Negi and Kumar, 2024) is utilized for conducting this simulation experiment.

For our experiment, we used the quantum simulator (Aer Simulator) to execute the quantum circuit implemented in Qiskit. The factorization relies on the Quantum Phase Estimation (QPE) algorithm, which iteratively determines the phase, which is then converted into a fraction to deduce the period *r*. Based on *r*, it calculates potential factors of *N* using guesses and validates them. Initially, Hadamard gates are applied to initialize the qubits into a state of superposition. Subsequently, controlled unitary operations are used to execute modular exponentiation

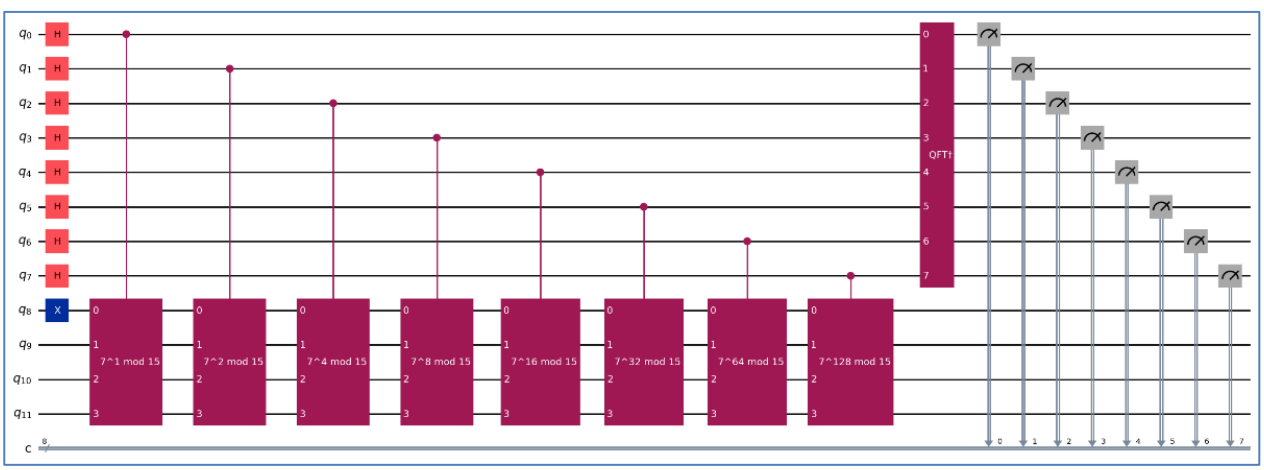


Figure 8. Quantum circuit implementation of modular exponentiation for this study using IBM Qiskit.

The QFT is then applied to the qubits to extract the phase. Upon extracting the phase, the inverse QFT operation is performed using a combination of Hadamard gates and controlled phase rotation gates. Once these operations are completed, the quantum circuit is compiled into a basis gate set suitable for simulation

on quantum hardware. The circuit is then executed using a quantum simulator, specifically the AerSimulator.

Utilizing the Qiskit SDK, we can efficiently determine the co-prime of a small prime number (15) capable of encrypting any number between 0 and 9 as a digital signature. Moreover, it can encrypt up to any of 14 sequential letters out of the 26 alphabets in English, serving as messages in V2V communications. This capability allows us to break the small key RSA algorithm using Shor's algorithm. Subsequently, we generate messages with forged digital signatures from a vehicle chosen as the malicious entity in our simulation. The quantum attack compromises the entire trust mechanism of the blockchain, as it incorrectly identifies another vehicle as malicious while failing to pinpoint the original malicious vehicle. Consequently, the trust value of the falsely accused vehicle increases, leading it to be selected as the miner in the blockchain network. The malicious vehicle, now acting as the miner, introduces more fraudulent transactions from other vehicles into the new block, further jeopardizing the integrity of the VANET. This simulation demonstrates the vulnerability of the trust mechanism against an attack model implemented in a quantum computer, emphasizing the importance of quantum-resistant cryptographic methods in securing V2V communications in a blockchain-based VANET.

Figure 8 depicts the quantum circuit implementation with 8 qubits(q) and 4 classical bits (c) for the prime factorization of 15, where $m=7$ and $N=15$. Four of the counting qubits ($q_0, q_1, q_2, q_4, q_5, q_6$ and q_7) are into superposition states of (|0>, |1>) with equal probability using the Hadamard gate (see "H" in **Figure 8**). Then, we use X-gate or Pauli-X gate (see "X" in **Figure 8**) to convert qubit(q_8) from State-0 (an auxiliary qubit) to State-1. After that, m is raised to the power of 2^q *modulo N* using a controlled operation to find the modular exponentiation. Later, all gates are appended to aggregate every qubit, q, in each iteration of modulo operation to form the circuit. After that, an inverse QFT is performed on the counting qubits to determine the period finding value (state $|s>$) from the frequency domain (superposition state $|t>$) and appended (with every qubit q) to get the circuit. Then, the counting qubits are measured and stored the results in the classical bits.

The methods employed in this study combine case-based threat modeling, detailed simulation of TCPS and VANET environments, and quantum circuit implementation to evaluate the vulnerabilities of traditional cryptographic systems and the efficacy of post-quantum cryptographic solutions. The experimental setups, spanning from the simulation of secure communication protocols in realistic network scenarios to the demonstration of a quantum-enabled impersonation attack, provide valuable insights into both the weaknesses of existing security architectures and the potential of PQC schemes like CRYSTALS-Kyber. Given the rapidly evolving quantum landscape and the complexity of real-world transportation networks, further research is essential to refine these methodologies, optimize performance, and ensure robust, scalable security solutions for future transportation infrastructures.

CHAPTER 4

Results

The results section is organized into two primary parts. The first part, "PQC for TCPS Applications – Performance Evaluation," presents simulation results for Kyber's KEM in both wired Ethernet and wireless ad hoc LTE (C-V2X) scenarios. It details key performance metrics including execution times for key generation, encapsulation, and decapsulation, along with communication delays for transmitting public keys, ciphertexts, and encrypted data across different network media. The second part, "Blockchain-based VANET Architecture – Evaluation Outcomes," comprises several subsections. It covers blockchain data generation and communication characteristics in a non-attack scenario, evaluates the failure of the trust-based system under an impersonation attack, analyzes vehicular trust value profiles, assesses the computational time required for executing a quantum-based impersonation attack, and discusses a roadmap for overcoming RSA-2048 with quantum computing.

4.1 PQC for TCPS Applications – Performance Evaluation

The performance evaluation was conducted by simulating Kyber's KEM in both wired Ethernet and wireless ad hoc LTE (i.e., C-V2X) network scenarios, which are commonly encountered in TCPS. Two primary performance metrics were analyzed: (1) execution time for cryptographic operations and (2) communication delays across different network media. For execution time metrics (**Table 10**), average values from five simulation runs were reported to account for variability. For communication delay metrics (**Table 11**), maximum, minimum, and average values from the simulation runs were recorded to provide a comprehensive view of performance under varying conditions.

Table 10 presents the execution times for key cryptographic operations, i.e., key generation, encapsulation, and decapsulation, for each variant of Kyber (Kyber-512, Kyber-768, and Kyber-1024). The data indicate that execution time increases with the complexity of the cryptographic variant. For instance, Kyber-512 requires 44 microseconds (µs) for key generation, while Kyber-1024 requires 107 µs. Similarly, encapsulation times range from 53 µs for Kyber-512 to 121 µs for Kyber-1024, and decapsulation times range from 65 µs to 147 µs across the three variants. This increase in execution time is primarily attributed to the larger key and ciphertext sizes in higher variants, which necessitate additional computational steps for cryptographic operations.

Table 10. Execution time for cryptographic operations.

PQC Scheme	Key Generation (cycle count/time (μs))	Encapsulation (cycle count /time (μs))	Decapsulation (cycle count /time (μs))
Kyber-512	155365 / 44	191358 / 53	232691 / 65
Kyber-768	272804 / 75	320600 / 89	365776 / 101
Kyber-1024	387324 / 107	436250 / 121	531310 / 147

Table 11 presents the communication delays incurred when transmitting public keys, ciphertexts, and encrypted data over the Ethernet and the ad hoc LTE network (i.e., C-V2X) mediums. In the Ethernet medium, communication delays are minimal and consistent across all PQC schemes. Public Key and Encrypted Data transmission delays typically average around 5 µs, while Ciphertext transmission takes up to 10 µs. These results indicate that in a wired network with high bandwidth and low latency, the variation in key sizes and cryptographic operations have a negligible impact on communication delays.

Table 11. Communication delay (in µs) for different simulation scenarios.

PQC Scheme	Simulation Scenario	Medium		Public Key	Ciphertext	Encrypted Data
Kyber-512	Static-Static	Ethernet	Maximum (max)	5.0029	10.0078	5.0056
			Minimum (min)	5.0023	10.0056	5.0031
			Average (avg)	5.0027	10.0060	5.0045
	Static-Static	ADHOC LTE (C-V2X)	max	1,126.13	1,001,948	676.10
			min	1,125.97	1,001,948	676.03
			avg	1,126.05	1,001,948	676.05
	Static-Dynamic	ADHOC LTE	max	1,135.15	1,001,960	685.15
			min	1,122.40	1,001,941	672.40
			avg	1,129.16	1,001,952	679.16
	Dynamic-Dynamic	ADHOC LTE	max	1,374.73	1,002,139	1,564.72
			min	1,362.00	1,002,122	1,532.00
			avg	1,369.25	1,002,132	1,547.24
Kyber-768	Static-Static	Ethernet	max	5.0035	10.0064	5.0053
			min	5.0021	10.0061	5.0046
			avg	5.0029	10.0063	5.0048
	Static-Static	ADHOC LTE	max	1,254.08	1,002,184	676.08
			min	1,254.02	1,002,183	676.01
			avg	1,254.05	1,002,183	676.05
	Static-Dynamic	ADHOC LTE	max	1,263.16	1,002,196	685.16
			min	1,122.40	1,001,943	672.40
			avg	1,206.14	1,002,093	679.33
	Dynamic-Dynamic	ADHOC LTE	max	1,502.73	1,002,375	1,672.72
			min	1,490.01	1,002,358	1,640.01
			avg	1,497.19	1,002,368	1,659.19
Kyber-1024	Static-Static	Ethernet	max	5.0037	10.0064	5.0046
			min	5.0032	10.0056	5.0040
			avg	5.0036	10.0061	5.0045
	Static-Static	ADHOC LTE	max	1,001,477	1,002,661	676.25
			min	1,001,469	1,002,641	676.18
			avg	1,001,473	1,002,656	676.20
	Static-Dynamic	ADHOC LTE	max	1,001,492	1,002,685	685.18
			min	1,001,471	1,002,651	672.50
			avg	1,001,484	1,002,672	680.36
	Dynamic-Dynamic	ADHOC LTE	max	1,001,731	1,002,864	1,933.21
			min	1,001,710	1,002,830	1,892.01
			avg	1,001,722	1,002,849	1,915.99

Conversely, in the ad hoc LTE (i.e., C-V2X) network, communication delays increase significantly, particularly for larger key sizes and scenarios involving dynamic nodes. For Kyber-512 in the Static-Static scenario, the maximum delay for transmitting the Public Key is around 1,126 µs, while the Ciphertext delay peaks at approximately 1,001,948 µs. These delays escalate further in the Dynamic-Dynamic scenario, where Public Key transmission delay reaches 1,374 µs and Encrypted Data transmission delay rises to 1,564 µs.

For Kyber-768, the increased key size results in marginally higher delays. In the Static-Static LTE scenario, Public Key transmission reaches up to a maximum of 1,254 µs, with Ciphertext delays peaking at 1,002,184 µs. In the Dynamic-Dynamic scenario, Public Key delay increases to 1,502 µs, and Encrypted Data delay reaches to 1,672 µs. The largest key size, Kyber-1024, incurs the most significant delays in ad hoc LTE networks. In the Static-Static LTE scenario, Public Key transmission peaks around 1,001,477 µs, while Ciphertext transmission peaks at 1,002,661 µs. These delays further increase in the Dynamic-Dynamic

scenario, with maximum Public Key transmission delay reaching 1,001,731 µs and Encrypted Data delay peaking at 1,933 µs.

The results presented in **Table 11** demonstrate a contrast in communication performance between the wired Ethernet and the wireless ad hoc LTE network when implementing all variants of Kyber for various TCPS communication scenarios. Average communication latencies for all Kyber variants over Ethernet networks remain consistently low, with delays of approximately 5 µs (5×10^{-3} milliseconds [ms]) for public key and encrypted data transmissions, and around 10 µs (10^{-2} ms) for ciphertext transmission. These results highlight the capability of high-bandwidth, low-latency Ethernet networks to efficiently handle the increased payload sizes associated with higher-level PQC variants, such as Kyber-1024. This makes Ethernet a suitable medium for real-time TCPS applications, including safety-critical systems requiring latencies under 100 ms, e.g., vehicle collision warning and lane change assistance, as stipulated by standards such as Society of Automative Engineers (SAE) J2735 (V2X Core Technical Committee, no date) and European Telecommunications Standards Institute (ETSI) TR 102 638 ((ITS), 2009).

In contrast, the ad hoc LTE network demonstrates significantly higher communication delays, particularly for scenarios involving larger cryptographic payloads for mobile vehicular nodes. For instance, in a static-dynamic scenario, the average public key transmission latency for Kyber-512 is approximately 1.13 ms, increasing further to 1.21 ms for Kyber-768 and exceeding 1 second for Kyber-1024. Ciphertext transmission in the same scenario experiences delays exceeding 1 second (1,000 ms) for all Kyber variants. These delays far exceed the 100-ms latency requirement for safety-critical TCPS applications, making ad hoc LTE impractical for real-time safety-critical TCPS applications such as collision warning. Furthermore, it is important to note that the current simulation does not account for the effects of packet fragmentation, which becomes a critical factor for larger cryptographic payloads like Kyber's public keys and ciphertexts. Packet fragmentation in real-world TCPS data transmission networks would introduce additional delays due to the need for reassembly and retransmission processes, further increasing the observed communication latencies.

In summary, while high-bandwidth Ethernet networks demonstrate that it is feasible to implement Kyber to satisfy latency requirements of real-time TCPS applications, ad hoc LTE networks face significant limitations due to their inherent bandwidth constraints and higher latency. To address these challenges in wireless environments, future research should explore the integration of new-generation wireless technologies, such as 5G, which offer lower latency and greater bandwidth. Additionally, optimizing PQC schemes for reduced payload sizes, developing lightweight PQC solutions, and designing hybrid PQC schemes that integrate traditional public-key cryptography with PQC algorithms could help mitigate latency impacts, enhancing the viability of wireless PQC implementations for TCPS.

4.2. Blockchain-based VANET Architecture – Evaluation Outcomes

This section is structured into five subsections. The first subsection focuses on setting up the simulation platform by showing blockchain based VANET communication characteristics with the simulation time. The second subsection discusses the evaluation of the failure of a trust-based PoS-VANET system if it has been affected by an impersonation attack that uses a quantum computer. The accumulated trust value was calculated by adding offsets in every triggered event and by generating event logs. In the third subsection, we evaluate the failure of the trust mechanism due to an impersonation attack by examining each vehicle profile. The fourth subsection assesses the computational time required for a quantum computing-powered attack to meet the time-limited consensus-based VANET's blockchain architecture. Finally, we analyze IBM's existing roadmap concerning the required number of noisy qubits for the factorization of RSA-2048 bits.

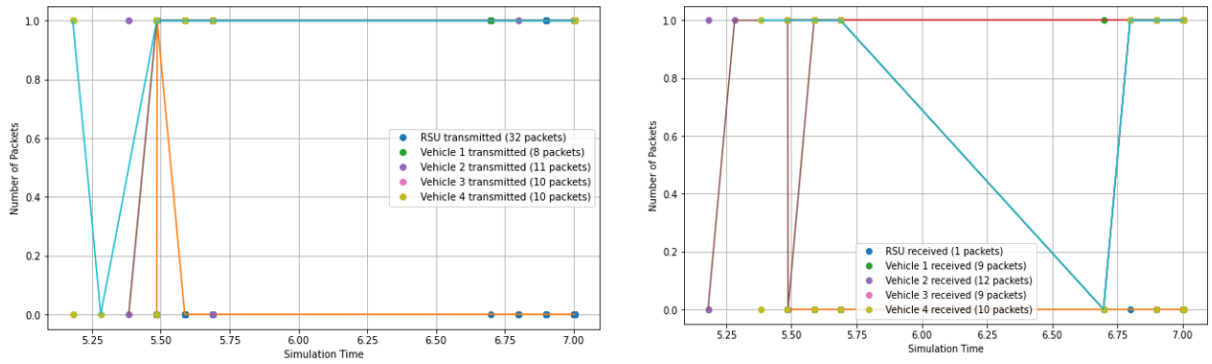
4.2.1. Blockchain Data Generation and Communication Characteristics without Impersonation Attack

In this subsection, we first generated blockchain data logs to assess the communication characteristics that established the framework for a thorough analysis of attack scenarios. This subsection helps to evaluate the system performance and throughput of the architecture in a non-attack scenario. Generating such simulation data by logging and calculating trust values ensures system security and integrity. During the phase of system setup, a public-private key pair is generated, and hash functions required for digital signatures are created to maintain security. Data logging starts with tracking and analyzing initial transactions, the dissemination and reception of messages, and the state of trust chain. These data logs contain detailed repositories of transactional information in the simulation, including timestamped events detailing the routing of packets and information about source, destination, and transaction amount. The logging process also shows transaction acknowledgement of packet transmission and reception, providing information about the start and end of data transfer between vehicles and RSUs. The RSU disseminates messages about the transaction. These dissemination messages provide packet propagation across the network and hold details, such as timestamps, transaction amounts, and sender and recipient signatures.

Logging also includes trust value calculation details, such as voting messages for consensus from vehicles. Finally, trust chain logs work as comprehensive repositories for trust value statistics and transaction information, essential for ensuring system security and validating transaction integrity. For instance, at a particular timestamp, both global and local trust-chain provide insights into trust chain behavior and initiates validator/miner chain requests and chain logs during packet handling and transmission.

From the logging of messages, we observe the vehicular and RSU communication over the simulation time, such as transmitted messages, chain request messages, disseminated messages, voting messages, and transaction acknowledgement (Ack) messages. Vehicle authentication and message verification with voting results and dissemination messages increase communication overhead with simulation time. **Figure 9** depicts a segment of the logging of the simulation being conducted over a time span from 0 to 7.003 seconds, with the transmission starting at 5.180 seconds. During this period, messages were transmitted and received from the RSU and four vehicles. Within the simulation time, RSU transmitted 32 messages, which includes disseminated messages from RSU to all vehicles: Vehicle#1 transmitted 8 messages, Vehicle#2 transmitted 11 messages, Vehicle#3 transmitted 10 messages, and Vehicle#4 transmitted 10 messages. Analyzing the reception of messages, the RSU received 1 message within this time period (as there was no voting done, no voting messages were exchanged, and only one chain request was made to RSU), Vehicle#1 received 9 messages, Vehicle#2 received 12 messages, Vehicle#3 received 9 messages, and Vehicle#4 received 10 messages. This results in an average transmission rate of approximately 10.42 messages per 100 seconds and an average reception rate of approximately 8.5 messages per 100 seconds. RSU has a higher transmission rate as it is responsible for disseminating messages.

It is worthy to note that the throughput of the communication network—both in non-attack and attack scenarios—remains relatively unchanged due to the nature of the impersonation attack, which does not directly alter the volume of messages, or the data transmission rates within a network. This characteristic makes the impersonation attack particularly difficult to maintain the integrity of messages through traditional blockchain-based system monitoring and throughput analysis alone. The attack seamlessly integrates within the trust-based framework, maintaining typical throughput levels while subtly compromising trust integrity through forged digital signatures. This highlights the importance of enhanced security mechanisms beyond mere throughput analysis to detect such intelligent attacks.



(a) (b)

Figure 9. No of packets vs simulation time over a time span from 0 to 7.003 seconds (a) data transmission, (b) data reception.

4.2.2. Evaluation of Trust-based System Failure

We present a trust-based VANET architecture using simulation parameters (as shown in**Table 9**) that fails to detect and increases the trust value of a malicious vehicle (i.e., Vehicle #2). Note that Vehicle #2 impersonates a legitimate vehicle, i.e., Vehicle #3, to complete a malicious transaction. As shown in **Figure 10**, we observe that the accumulated trust value in the RSU increases even if a malicious transaction or impersonation attack creates false messages that occur within the VANET. Trust value increases if the blockchain finds a malicious vehicle responsible for the false message transaction. However, this creates controversy on the trust-based VANET system, as it cannot decrease the trust until it finds a malicious transaction that has been impersonated and compromised by a malicious vehicle itself. This proves the vulnerability of the trust-based system. We also observe that a new block has been written by the validator, even if it is a malicious transaction, which leads to more malicious transactions in the VANET.

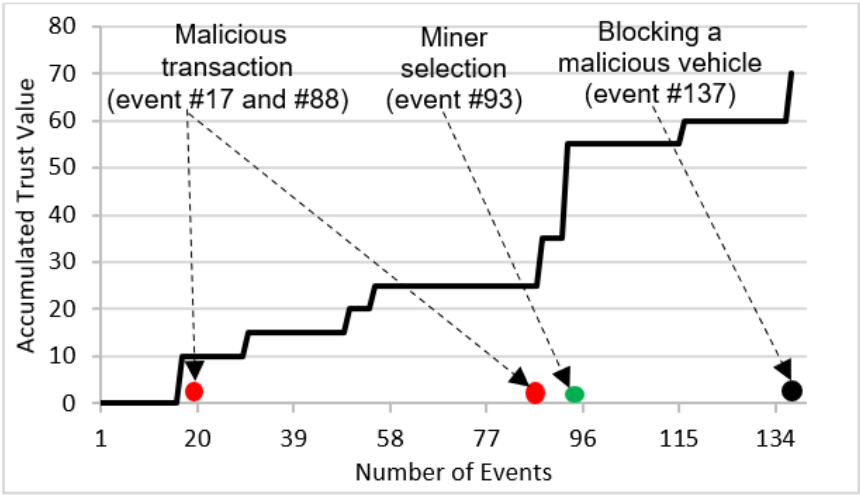


Figure 10. Variation of accumulated trust value in RSU.

We found (see **Figure 10**) that the accumulated trust value increases for an event with an increment of 10 even if a malicious transaction occurs (indicated as red circles). On the other hand, the accumulated trust value increases for an event with an increment of 20 due to mining a new block (see the green circle), whereas the trust value increases with an increment of 5 for an authenticated transaction. This shows how

a trust-based architecture fails to resist an impersonation attack and assigns mining responsibilities even if a malicious transaction occurs.

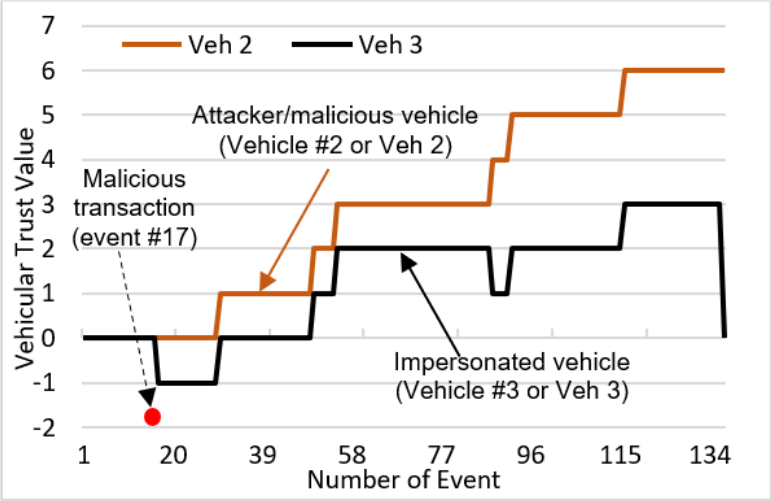


Figure 11. Vehicular trust value profiles.

4.2.3. Evaluation of Vehicular Profile of Trust Value

In this subsection, we evaluate trust-chain value of each vehicle at the vehicular level without considering trust offsets. **Figure 11** illustrates the trust value profiles for Vehicle #2 and Vehicle #3. As Vehicle #2 executes as an impersonation attack utilizing a quantum computer on Vehicle #3, it forges the digital signature of Vehicle #3, causing the trust value of Vehicle #3 to decline for each malicious transaction. However, the trust value of Vehicle #2 increases, making it appear like a trusted node in VANET. We observe that Vehicle #3 gets blocked, and its trust value reaches zero when it appears to perform malicious transactions more than the threshold. **Figure 11** shows that Vehicle #3 gets suspected of a malicious transaction by blockchain consensus mechanism at event 17, and the trust value reduces to -1. Vehicle #2 does this impersonation attack, but it does not get suspected due to its forging of digital signature, and its trust value increases to +1. Again, the same happens at events #88 and #137, where Vehicle #2 pins the blame on Vehicle #3, and the trust value of Vehicle #3 declines and eventually gets to 0 as it gets blocked. Vehicle #2, despite being the malicious node, becomes the miner at event #93 by highest trust values gets selected as the miner. This depicts the evaluation of individual vehicular level trust mechanism and failure of PoS-based trust-chain architecture (as stakeholders' consensus fails to identify the malicious vehicle).

4.2.4. Computational Time Requirement

We assess the time required for generating a quantum-based private key to satisfy the computational time requirement for RSA. To model an impersonation attack that uses a quantum computer, it is first necessary to break RSA, decrypt the received message, and forge digital signatures. Note that the private keys change with a predefined frequency of 10 mins as per PoW mechanism-based blockchain. Our approach only takes polynomial time complexity and can identify the factors for a small key efficiently, which acts as a proof of concept. In our case, factoring a 4-bit number like 15 takes between 5 to 17 seconds. The experiment was conducted 30 times, as this sample size of 30 is considered significant for any central limit probability distribution. We developed this impersonation attack with a small key RSA (4 bits in our experiment) as proof of concept due to existing limited computational capacity to break 2048-bit RSA. **Figure 12** shows that the mean factorization time is 10.4 seconds using a Poisson probability distribution of 30 trials. In

addition to this factorization time, additional computational time is required to decrypt a message and create a false message packet with forged digital signature. The OMNET++ stores the total computational time (factorization time, message decryption and forged message creation) in a log file as shown below.

Total Computational Time = Factorization Time + Message Decryption + Forged Message Creation

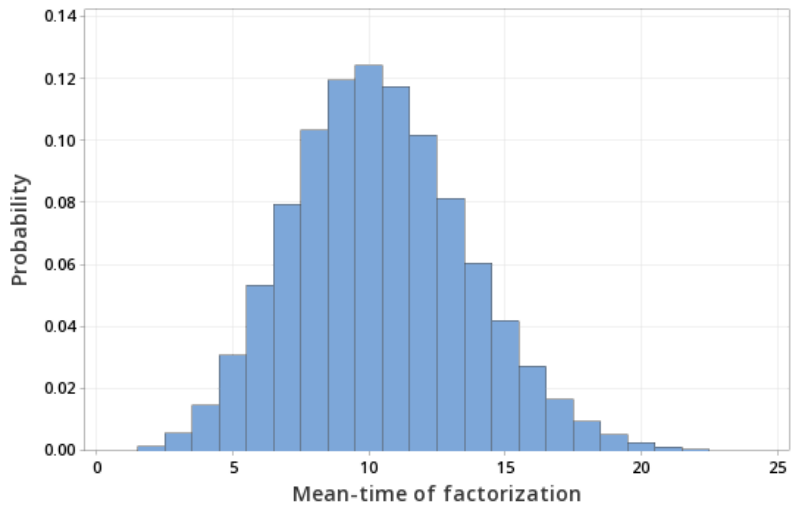


Figure 12. Probability distribution of required time (in seconds) for factorization.

Overall, it takes a mean of 115 seconds, which is significantly lower than the 10 minutes required to hack into the current block. This ensures that the false message in "mempool" gets sufficient votes within the time constraint. Thus, our cyber-attack generation technique utilizes Shor's algorithm implemented in a quantum computer and takes advantage of the current limitation of blockchain-based VANET.

4.2.5. Advancing Toward Computational Requirements to Overcome RSA-2048 Bits

We developed this impersonation attack with a 4 bits RSA as a proof of concept due to the existing limited computational capacity to break a 2048-bit RSA. For evaluating the feasibility of the impersonation attack utilizing Shor's algorithm implemented in a quantum computer, particularly for breaking cryptographic schemes like RSA-2048, it is necessary to show a roadmap toward achieving quantum speedup in the Noisy Intermediate Scale Quantum (NISQ) era. Shor's algorithm, a key component of our impersonation attack scheme, demonstrated its potential in 2019 by successfully factoring the number 35. For the application of Shor's algorithm in factorizing an n-bit integer, the quantum circuit, as outlined in (Beauregard, 2002), utilizes a total of 2n + 3 qubits. These qubits are specifically allocate for various tasks, including modular addition, overflow prevention, and ancillary registers for modular multiplication. Applying this formula to 2,048-bit integer results in a requirement of 4099 qubits (2*2048+3). By analyzing IBM's quantum computing roadmap, which incorporates the dynamics of noisy qubits, our projection in **Figure 13** suggests that between 2032 and 2044, IBM's quantum infrastructure may have the capacity to efficiently factorize RSA-2048 efficiently. This prediction relies on exponential and linear regression modeling.

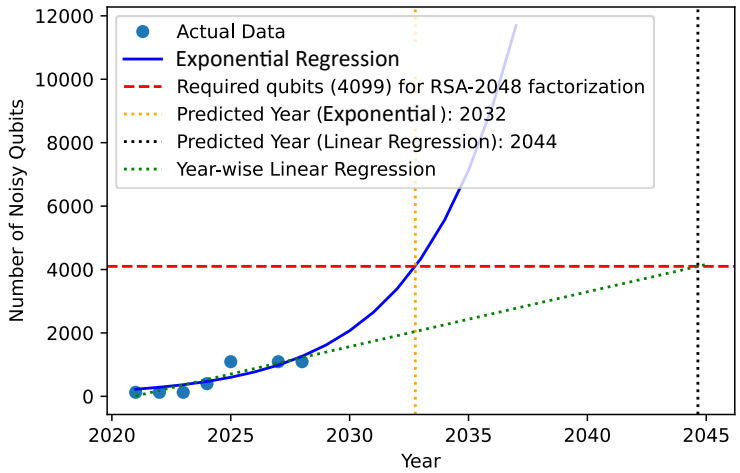


Figure 13. IBM quantum roadmap for factorizing RSA-2048 bits.

Although linear regression assumes a linear time-qubit relationship, which does not fully capture quantum computing's growth, it serves as a conservative baseline for comparison, representing a worst-case scenario. Despite efforts to predict quantum computing progress, there's a disparity between the number of qubits and their quality (fidelity), posing obstacles to predict the roadmap towards factorization of 2048-bits. While companies like D-Wave and IBM have experienced exponential growth in qubit numbers which is greater than its competitors, advancements in high-quality qubits characterized by extended coherence times and low error rates have progressed more slowly (Ezratty, 2023). IBM utilizes "quantum volume" as a metric to assess the performance and quality of its quantum computers. Quantum Volume measures both the number of qubits and the depth of quantum circuits, offering insights into the system's capabilities. The IBM quantum roadmap for factorizing RSA-2048 bits shows the necessity of understanding quantum computing's current constraints, advancements, and potential future progress in securing cryptographic applications (see **Figure 13**).

In summary, the results indicate that while high-bandwidth Ethernet networks demonstrate the feasibility of implementing Kyber to satisfy the latency requirements of real-time TCPS applications, the ad hoc LTE network exhibits significant limitations due to inherent bandwidth constraints and higher communication delays, especially in dynamic scenarios. The experimental data reveal that execution times for cryptographic operations increase with the complexity of the Kyber variant and that communication delays in LTE environments, particularly for Kyber-1024, far exceed the stringent requirements of safety-critical TCPS applications, where latencies under 100 ms are essential. Furthermore, the evaluation outcomes from the blockchain-based VANET architecture indicate that the trust-based system fails to detect impersonation attacks, as evidenced by the increasing accumulated trust values even when malicious transactions occur, and that individual vehicular trust profiles are manipulated through forged digital signatures. The computational time assessment confirms that the impersonation attack model, utilizing Shor's algorithm on a scaled-down 4-bit RSA, is feasible within current quantum computing limitations, serving as a proof of concept for potential future attacks on more robust systems such as RSA-2048. Overall, these findings underscore the urgent need for further optimization of PQC schemes, especially for wireless environments, and for the development of lightweight, hybrid cryptographic solutions that can be seamlessly integrated into resource-constrained, real-time TCPS and VANET applications. Future research must prioritize addressing these performance trade-offs and enhancing the resilience of both cryptographic and blockchain-based security mechanisms to ensure the robust protection of critical transportation infrastructures against emerging quantum-enabled cyber threats.

CHAPTER 5

Conclusions

Quantum computers pose a significant threat to the cryptographic foundations of TCPS to meet its confidentiality and integrity requirements. The vulnerabilities of traditional cryptographic schemes against quantum computing-based cyberattacks, with a particular focus on the data communication aspects of TCPS, are identified in this report. The case study on electronic toll collection further emphasized the vulnerabilities inherent in traditional cryptographic schemes in TCPS, showcasing how quantum threats could exploit these weaknesses. By employing the Microsoft Threat Modeling Tool, we identified potential risks. Furthermore, the impersonation attack model presented in this report—with Shor's algorithm implemented in a quantum computer—demonstrates a proof of concept to expose the vulnerabilities of a blockchain-based VANET. Even though existing quantum computers do not have the necessary computational efficiency to break a 2048-bit RSA, the impersonation attack on a 4-bit RSA serves as a proof-of-concept for such an attack. This report showcases the feasibility of an impersonation attack that, by scaling down the current blockchain encryption standards, can compromise the trust chain of the blockchain-based VANET. This vulnerability in the trust-based framework of blockchain—particularly in VANETs—is formulated and examined by the potential for impersonation attacks, wherein malicious actors can forge digital signatures, thus undermining the integrity of the trust mechanism. Specifically, our investigation reveals that the vulnerability of vertical trust (the vehicle-to-infrastructure trust chain using the aggregated trust profile at the RSU) and horizontal trust (the vehicle-to-vehicle trust chain using each vehicle's trust profile) can be successfully broken by a quantum computing-based impersonation attack. We have also analyzed a timeline and discussed a roadmap outlining the progression of quantum computers required for such an attack to succeed. All these underscores the urgency of integrating PQC into existing and future TCPS data communication to ensure the integrity and confidentiality of critical TCPS.

Through a comprehensive review of the NIST PQC Standardization guidelines and analysis of various PQC schemes, we identified promising public-key encryption/KEM candidates—such as CRYSTALS-Kyber, Classic McEliece, BIKE, and HQC—and digital signature candidates—such as CRYSTALS-Dilithium, Falcon, and SPHINCS+—which offer robust security claims against quantum attacks. Implementing PQC in real-world transportation systems involves various practical considerations, requiring a careful balance between security, performance, and resource constraints. Each PQC family offers distinct advantages and trade-offs, making their suitability dependent on specific TCPS requirements. For example, lattice-based schemes such as CRYSTALS-Kyber and CRYSTALS-Dilithium provide robust security and efficiency but may demand higher computational resources, while code-based schemes such as Classic McEliece excel in security with larger key sizes—making them suitable for bandwidth-insensitive applications but less ideal for real-time, safety-critical TCPS applications due to their high communication overhead. Multivariate polynomial-based schemes show potential for compact key sizes but are still undergoing active security evaluation, and hash-based schemes, attractive for constrained environments like low-power or low-memory devices, require significant memory for key generation and storage. Isogeny-based schemes, offering high-performance potential, remain under continued security analysis. These considerations highlight that while PQC is a promising path forward, the selection and implementation of a suitable scheme must be carefully matched to the operational demands of the transportation environment.

Our experimental assessment of CRYSTALS-Kyber demonstrated its practical feasibility across various peer-to-peer communication scenarios, including wired (Ethernet) and wireless (LTE/C-V2X) environments for TCPS applications. The results indicate that Kyber's hierarchical security levels, although associated with increased computational and communication overhead at higher levels, remain well-suited for different TCPS applications when paired with appropriate network infrastructures and communication-related performance requirements. For instance, high-bandwidth and low-latency Ethernet networks

effectively mitigate Kyber's overhead, making it a strong candidate for securing critical operations between static nodes such as communication between a Payment Administration Center and a DMV. Similarly, while simulations of LTE networks—representing peer-to-peer C-V2X communication—demonstrate that Kyber is feasible in wireless scenarios, its current performance does not fully meet the stringent requirements of safety-critical TCPS applications, where the need to broadcast 10 per second imposes strict latency and throughput constraints. This highlights the necessity for further optimization, particularly in high-speed, low-latency wireless networks such as 5G, to ensure that PQC solutions like Kyber can be effectively integrated into demanding operational environments.

While the adoption of PQC represents a significant step forward in TCPS data and user security, challenges remain in ensuring interoperability, managing performance trade-offs, and addressing implementation constraints in the real-world transportation systems. Future research must prioritize the development of lightweight and hybrid PQC solutions tailored for real-time and resource-constrained environments, alongside extensive security evaluations under realistic TCPS conditions. Collaborative efforts among academia, industry, and government are essential to streamline standardization, incentivize adoption, and prepare transportation infrastructures for a quantum-secure future. Looking ahead, transitioning to PQC is essential to ensure the long-term sustainability and security of TCPS in the quantum era. By adopting these advancements, the transportation industry can safeguard critical infrastructures, foster user trust and acceptance while ensuring confidentiality and the seamless operation of TCPS against emerging cyber threats.

REFERENCES

Aggarwal, D. *et al.* (2018) 'Quantum Attacks on Bitcoin, and How to Protect Against Them', *Ledger*, 3. Available at: https://doi.org/10.5195/LEDGER.2018.127.

Alagic, G. *et al.* (2019) *Status report on the first round of the NIST post-quantum cryptography standardization process*. Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.IR.8240.

Alagic, G. *et al.* (2022) *Status report on the third round of the NIST Post-Quantum Cryptography Standardization process*. Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.IR.8413-upd1.

Albrecht, M.R. (2017) 'On Dual Lattice Attacks Against Small-Secret LWE and Parameter Choices in HElib and SEAL', in J.-S. Coron and J.B. Nielsen (eds) *Advances in Cryptology – EUROCRYPT 2017*. Cham: Springer International Publishing, pp. 103–129. Available at: https://doi.org/10.1007/978-3-319-56614-6_4.

Albrecht, M.R., Player, R. and Scott, S. (2015) 'On the concrete hardness of Learning with Errors', *Journal of Mathematical Cryptology*, 9(3), pp. 169–203. Available at: https://doi.org/10.1515/jmc-2015-0016.

Ali, I., Lawrence, T. and Li, F. (2020) 'An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs', *Journal of Systems Architecture*, 103, p. 101692. Available at: https://doi.org/10.1016/J.SYSARC.2019.101692.

Avanzi, R. *et al.* (2021) 'CRYSTALS-Kyber (version 3.02) – Submission to round 3 of the NIST post-quantum project'.

Azees, M., Vijayakumar, P. and Deboarh, L.J. (2017) 'EAAP: Efficient Anonymous Authentication with Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks', *IEEE Transactions on Intelligent Transportation Systems*, 18(9), pp. 2467–2476. Available at: https://doi.org/10.1109/TITS.2016.2634623.

Bai, L., Zhang, Y. and Yang, G. (2012) 'SM2 cryptographic algorithm based on discrete logarithm problem and prospect', in *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*. Yichang, China: IEEE, pp. 1294–1297. Available at: https://doi.org/10.1109/CECNet.2012.6201878.

Bard, D.A., Kearney, J.J. and Perez-Delgado, C.A. (2022) 'Quantum advantage on proof of work', *Array*, 15. Available at: https://doi.org/10.1016/J.ARRAY.2022.100225.

Bayat, Majid *et al.* (2020) 'NERA: A new and efficient RSU based authentication scheme for VANETs', *Wireless Networks*, 26(5), pp. 3083–3098. Available at: https://doi.org/10.1007/s11276-019-02039-x.

Bayat, M *et al.* (2020) 'NERA: A new and efficient RSU based authentication scheme for VANETs', *Wireless Networks*, 26(5), pp. 3083–3098. Available at: https://doi.org/10.1007/s11276-019-02039-x.

Beauregard, S. (2002) 'Circuit for Shor's algorithm using 2n+3 qubits', *Quantum Information and Computation*, 3(2), pp. 175–185. Available at: https://doi.org/10.26421/qic3.2-8.

Berlekamp, E., McEliece, R. and Van Tilborg, H. (1978) 'On the inherent intractability of certain coding problems (Corresp.)', *IEEE Transactions on Information Theory*, 24(3), pp. 384–386. Available at: https://doi.org/10.1109/TIT.1978.1055873.

Bernstein, D.J. *et al.* (2019) 'The SPHINCS+ Signature Framework', in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. London, United Kingdom: ACM, pp. 2129–2146. Available at: https://doi.org/10.1145/3319535.3363229.

Bernstein, D.J., Lange, T. and Peters, C. (2008) 'Attacking and Defending the McEliece Cryptosystem', in J. Buchmann and J. Ding (eds) *Post-Quantum Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 31–46. Available at: https://doi.org/10.1007/978-3-540-88403-3_3.

Bertoni, G. *et al.* (2013) 'Keccak', in D. Hutchison et al. (eds) *Advances in Cryptology – EUROCRYPT 2013*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 313–314. Available at: https://doi.org/10.1007/978-3-642-38348-9_19.

Biasse, J.-F. and Song, F. (2016) 'Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields', in *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*. USA: Society for Industrial and Applied Mathematics (SODA '16), pp. 893–902.

'BIKE - Bit Flipping Key Encapsulation' (2024) *BIKE* [Preprint]. Available at: https://bikesuite.org/.

Bone, S. and Castro, M. (1997) 'A Brief History of Quantum Computing', *Surveys and Presentations in Information Systems Engineering (SURPRISE)*, 4(3), pp. 20–45.

Bos, J. *et al.* (2018) 'CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM', in *2018 IEEE European Symposium on Security and Privacy (EuroS\&{P})*. London: IEEE, pp. 353–367. Available at: https://doi.org/10.1109/EuroSP.2018.00032.

Brassard, G., Høyer, P. and Tapp, A. (1997) 'Quantum cryptanalysis of hash and claw-free functions', *SIGACT News*, 28(2), pp. 14–19. Available at: https://doi.org/10.1145/261342.261346.

Castryck, W. and Decru, T. (2022) 'An efficient key recovery attack on SIDH'.

Chen, L. *et al.* (2016) *Report on Post-Quantum Cryptography*. Available at: https://doi.org/10.6028/NIST.IR.8105.

Chunhuan, Z. *et al.* (2019) 'Distinguishing LWE Instances Using Fourier Transform: A Refined Framework and its Applications'.

'Classic McEliece' (2024) *Classic McEliece* [Preprint]. Available at: https://classic.mceliece.org/.

Cramer, R., Ducas, L. and Wesolowski, B. (2016) 'Short Stickelberger Class Relations and application to Ideal-SVP'.

Crandall, R. and Pomerance, C. (2001) 'Subexponential Factoring Algorithms', *Prime Numbers*, pp. 227–283. Available at: https://doi.org/10.1007/978-1-4684-9316-0_6.

Cui, W., Dou, T. and Yan, S. (2020) 'Threats and Opportunities: Blockchain Meets Quantum Computation'. Available at: https://doi.org/10.23919/CCC50068.2020.9189608.

Diallo, E.H. *et al.* (2021) 'When Proof-of-Work (PoW) based blockchain meets VANET environments', *2021 12th International Conference on Information and Communication Systems, ICICS 2021*, pp. 336–343. Available at: https://doi.org/10.1109/ICICS52457.2021.9464609.

Diallo, E.H., Dib, O. and Al Agha, K. (2021) 'An Improved PBFT-based Consensus for Securing Traffic Messages in VANETs', in *2021 12th International Conference on Information and Communication Systems, ICICS 2021*. Institute of Electrical and Electronics Engineers Inc., pp. 126–133. Available at: https://doi.org/10.1109/ICICS52457.2021.9464606.

Ducas, L. (2017) 'Shortest Vector from Lattice Sieving: a Few Dimensions for Free'.

Ducas, L. *et al.* (2018) 'CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme', *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 238–268. Available at: https://doi.org/10.46586/tches.v2018.i1.238-268.

Dwivedi, S.K. *et al.* (2023) 'B-HAS: Blockchain-Assisted Efficient Handover Authentication and Secure Communication Protocol in VANETs', *IEEE Transactions on Network Science and Engineering*, 10(6), pp. 3491–3504. Available at: https://doi.org/10.1109/TNSE.2023.3264829.

Eclipse SUMO - Simulation of Urban MObility (no date). Available at: https://www.eclipse.org/sumo/ (Accessed: 19 March 2023).

Ethereum Glossary | ethereum.org (no date). Available at: https://ethereum.org/en/glossary/ (Accessed: 23 May 2024).

Ezratty, O. (2023) 'Is there a Moore's law for quantum computing?' Available at: https://arxiv.org/abs/2303.15547v1 (Accessed: 28 May 2024).

'Falcon - Fast-Fourier Lattice-based Compact Signatures over NTRU' (2024) *Falcon* [Preprint]. Available at: https://falcon-sign.info/.

Fernandez, V., Orue, A.B. and Arroyo, D. (2021) 'Securing blockchain with quantum safe cryptography: When and how?', *Advances in Intelligent Systems and Computing*, 1267 AISC, pp. 371–379. Available at: https://doi.org/10.1007/978-3-030-57805-3_35/COVER.

Galbraith, S.D. and Vercauteren, F. (2018) 'Computational problems in supersingular elliptic curve isogenies', *Quantum Information Processing*, 17(10), p. 265. Available at: https://doi.org/10.1007/s11128-018-2023-6.

Gayathri, N.B. *et al.* (2018) 'Efficient Pairing-Free Certificateless Authentication Scheme with Batch Verification for Vehicular Ad-Hoc Networks', *IEEE Access*, 6, pp. 31808–31819. Available at: https://doi.org/10.1109/ACCESS.2018.2845464.

Gayoso Martinez, V. *et al.* (2010) 'A comparison of the standardized versions of ECIES', in *Proceedings of the 2010 Sixth International Conference on Information Assurance and Security*. Atlanta, GA: IEEE, pp. 1–4. Available at: https://doi.org/10.1109/ISIAS.2010.5604194.

'GeMSS: A Great Multivariate Short Signature' (no date).

Ghaleb, Fuad A. *et al.* (2023) 'Intelligent Proof-of-Trustworthiness-Based Secure Safety Message Dissemination Scheme for Vehicular Ad Hoc Networks Using Blockchain and Deep Learning Techniques', *Mathematics*, 11(7). Available at: https://doi.org/10.3390/math11071704.

Ghaleb, F A *et al.* (2023) 'Intelligent Proof-of-Trustworthiness-Based Secure Safety Message Dissemination Scheme for Vehicular Ad Hoc Networks Using Blockchain and Deep Learning Techniques', *Mathematics*, 11(7). Available at: https://doi.org/10.3390/math11071704.

Gheorghiu, V. and Mosca, M. (2025) 'Quantum resource estimation for large scale quantum algorithms', *Future Generation Computer Systems*, 162, p. 107480. Available at: https://doi.org/10.1016/j.future.2024.107480.

'Google Quantum Computing Roadmap' (2024).

Grover, L K (1996) 'A fast quantum mechanical algorithm for database search', in *Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 212–219. Available at: https://doi.org/10.1145/237814.237866.

Grover, Lov K. (1996) 'A fast quantum mechanical algorithm for database search', *Proceedings of the Annual ACM Symposium on Theory of Computing*, Part F129452, pp. 212–219. Available at: https://doi.org/10.1145/237814.237866.

Haddaji, Achref, Ayed, S. and Fourati, L.C. (2020) 'Blockchain-based Multi-Levels Trust Mechanism against Sybil Attacks for Vehicular Networks', *Proceedings - 2020 IEEE 14th International Conference on Big Data Science and Engineering, BigDataSE 2020*, pp. 155–163. Available at: https://doi.org/10.1109/BIGDATASE50710.2020.00028.

Haddaji, A, Ayed, S. and Fourati, L.C. (2020) 'Blockchain-based Multi-Levels Trust Mechanism against Sybil Attacks for Vehicular Networks', in *Proceedings of the 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE 2020)*, pp. 155–163. Available at: https://doi.org/10.1109/BIGDATASE50710.2020.00028.

Hameed Mir, Z. and Filali, F. (2014) 'LTE and IEEE 802.11p for vehicular networking: a performance evaluation', *EURASIP Journal on Wireless Communications and Networking*, 2014(1), p. 89. Available at: https://doi.org/10.1186/1687-1499-2014-89.

Handschuh, H. (2005) 'SHA Family (Secure Hash Algorithm)', in H.C.A. Tilborg (ed.) *Encyclopedia of Cryptography and Security*. Springer US, pp. 565–567. Available at: https://doi.org/10.1007/0-387-23483-7_388.

Ho, Q.-D., Tweed, D. and Le-Ngoc, T. (2017) 'IEEE 802.11/Wi-Fi Medium Access Control: An Overview', in *Long Term Evolution in Unlicensed Bands*. Cham: Springer International Publishing, pp. 31–41. Available at: https://doi.org/10.1007/978-3-319-47346-8_4.

'HQC - Hamming Quasi-Cyclic' (2024) *HQC* [Preprint]. Available at: https://pqc-hqc.org/.

'IBM Quantum Roadmap' (2024).

'IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities' (no date).

'INET Framework' (2023).

INET Framework - INET Framework (no date). Available at: https://inet.omnetpp.org/ (Accessed: 19 March 2023).

'INET Mobility Models' (no date) *INET Framework* [Preprint]. Available at: https://inet.omnetpp.org/docs/showcases/mobility/basic/doc/.

(ITS), E.T.C.I.T.S. (2009) *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*. Available at: https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/01.01.01_60/tr_102638v010101p.pdf.

Johnson, D., Menezes, A. and Vanstone, S. (2001) 'The Elliptic Curve Digital Signature Algorithm (ECDSA)', *International Journal of Information Security (IJIS)*, 1(1), pp. 36–63. Available at: https://doi.org/10.1007/s102070100002.

Katz, J. and Lindell, Y. (2015) *Introduction to modern cryptography*. Second edition. Boca Raton: CRC Press/Taylor & Francis (Chapman & hall/crc cryptography and network security series).

Kearney, J.J. and Perez-Delgado, C.A. (2021) 'Vulnerability of blockchain technologies to quantum attacks', *Array*, 10, p. 100065. Available at: https://doi.org/10.1016/J.ARRAY.2021.100065.

Kirsch, Z. (2015) *Quantum Computing: The Risk to Existing Encryption Methods*. Tufts University. Available at: https://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf.

Laarhoven, T. and Walter, M. (2021) 'Dual Lattice Attacks for Closest Vector Problems (with Preprocessing)', in K.G. Paterson (ed.) *Topics in Cryptology – CT-RSA 2021*. Cham: Springer International Publishing, pp. 478–502. Available at: https://doi.org/10.1007/978-3-030-75539-3_20.

Leurent, G., Nandi, M. and Sibleyras, F. (2018) 'Generic Attacks Against Beyond-Birthday-Bound MACs', in H. Shacham and A. Boldyreva (eds) *Advances in Cryptology – CRYPTO 2018*. Cham: Springer International Publishing, pp. 306–336. Available at: https://doi.org/10.1007/978-3-319-96884-1_11.

Li, H. *et al.* (2019) 'Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET', *Peer-to-Peer Networking and Applications*, 12(5), pp. 1178–1193. Available at: https://doi.org/10.1007/s12083-019-00786-4.

'liboqs' (2024).

Lim, K. *et al.* (2020) 'A Sybil Attack Detection Scheme based on ADAS Sensors for Vehicular Networks', *2020 IEEE 17th Annual Consumer Communications and Networking Conference, CCNC 2020* [Preprint]. Available at: https://doi.org/10.1109/CCNC46108.2020.9045356.

Mariano, A. *et al.* (2017) 'A Practical View of the State-of-the-Art of Lattice-Based Cryptanalysis', *IEEE Access*, 5, pp. 24184–24202. Available at: https://doi.org/10.1109/ACCESS.2017.2748179.

Mavroeidis, V. *et al.* (2018) 'The Impact of Quantum Computing on Present Cryptography'.

McEliece, R.J. (1978) *A Public-Key Cryptosystem Based On Algebraic Coding Theory*.

Mei, Q. *et al.* (2021) 'Efficient Certificateless Aggregate Signature With Conditional Privacy Preservation in IoV', *IEEE Systems Journal*, 15(1), pp. 245–256. Available at: https://doi.org/10.1109/JSYST.2020.2966526.

Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A. (1997) *Handbook of Applied Cryptography*. Boca Raton: CRC Press.

Micciancio, D. and Goldwasser, S. (2002) 'Shortest Vector Problem', in *Complexity of Lattice Problems*. Boston, MA: Springer US, pp. 69–90. Available at: https://doi.org/10.1007/978-1-4615-0897-7_4.

Microsoft (2024) 'Microsoft Threat Modeling Tool'.

Miller, S. (2020) *Algorithms in Lattice-Based Cryptanalysis*. Clemson University. Available at: http://libproxy.clemson.edu/login?url=https://www.proquest.com/dissertations-theses/algorithms-lattice-based-cryptanalysis/docview/2443928396/se-2.

Moody, D. *et al.* (2020) *Status report on the second round of the NIST post-quantum cryptography standardization process*. Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.IR.8309.

National Institute of Standards and (NIST), T. (2016) *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*.

National Institute of Standards and Technology (2024a) *Module-Lattice-Based Digital Signature Standard*. Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.FIPS.204.

National Institute of Standards and Technology (2024b) *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.FIPS.203.

National Institute of Standards and Technology (2024c) *Stateless Hash-Based Digital Signature Standard*. Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.FIPS.205.

Negi, Lalit and Kumar, D. (2024) 'A Bilinear Mapping Based Ring Signature Scheme with Batch Verification for Applications in VANETs', *Wireless Personal Communications*, 134(4), pp. 1987–2011. Available at: https://doi.org/10.1007/S11277-024-10962-2/METRICS.

Negi, L and Kumar, D. (2024) 'A Bilinear Mapping Based Ring Signature Scheme with Batch Verification for Applications in VANETs', *Wireless Personal Communications*, 134(4), pp. 1987–2011. Available at: https://doi.org/10.1007/S11277-024-10962-2/METRICS.

'OMNeT++ Discrete Event Simulator' (2023).

OMNeT++ Discrete Event Simulator (no date). Available at: https://omnetpp.org/ (Accessed: 19 March 2023).

'OpenSSL' (no date).

Peikert, C. (2016) 'A Decade of Lattice Cryptography', *FNT in Theoretical Computer Science*, 10(4), pp. 283–424. Available at: https://doi.org/10.1561/0400000074.

Proos, J. and Zalka, C. (2003) 'Shor's discrete logarithm quantum algorithm for elliptic curves'.

Qualcomm Technologies, Inc. (no date) 'C-V2X Technical Performance'. Available at: https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/c-v2x_technical_performance_faq.pdf.

'Quantinuum Quantum Computing Roadmap' (2024).

Quantum Computing - The Impending End for the Blockchain? (no date). Available at: https://www.sitm.wiwi.uni-due.de/research/publications/publication-list/quantum-computing-the-impending-end-for-the-blockchain-15595/ (Accessed: 28 January 2023).

'Rainbow Signature' (2024) *Rainbow* [Preprint]. Available at: https://www.pqcrainbow.org/.

Rivest, R.L., Shamir, A. and Adleman, L.M. (1978) 'A Method for Obtaining Digital Signature and Public-key Cryptosystems', *Communications of the ACM*, 21. Available at: https://doi.org/10.1145/359340.359342.

Rodenburg, B. and Pappas, S.P. (2017) *Blockchain and Quantum Computing*.

Sabani, M.E., Savvas, I.K. and Garani, G. (2024) 'Learning with Errors: A Lattice-Based Keystone of Post-Quantum Cryptography', *Signals*, 5(2), pp. 216–243. Available at: https://doi.org/10.3390/signals5020012.

Sehar, N. us *et al.* (2023) 'Blockchain enabled data security in vehicular networks', *Scientific Reports 2023 13:1*, 13(1), pp. 1–15. Available at: https://doi.org/10.1038/s41598-023-31442-w.

Shakib, K.H., Rahman, M. and Islam, M. (2023) 'Quantum Cyber-Attack on Blockchain-based VANET'.

Shor, P.W. (1994) 'Algorithms for quantum computation: discrete logarithms and factoring', in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134. Available at: https://doi.org/10.1109/SFCS.1994.365700.

Shor, P.W. (1995) 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer'.

Shrestha, R. *et al.* (2020) 'A new type of blockchain for secure message exchange in VANET', *Digital Communications and Networks*, 6(2), pp. 177–186. Available at: https://doi.org/10.1016/J.DCAN.2019.04.003.

'SIKE – Supersingular Isogeny Key Encapsulation' (2024) *SIKE* [Preprint]. Available at: https://sike.org/.

Stewart, I. *et al.* (2018) 'Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack', *Royal Society Open Science*, 5(6). Available at: https://doi.org/10.1098/RSOS.180410.

Suaib Akhter, A.F.M. *et al.* (2021) 'A blockchain-based authentication protocol for cooperative vehicular ad hoc network', *Sensors (Switzerland)*, 21(4), pp. 1–21. Available at: https://doi.org/10.3390/s21041273.

Suo, S. *et al.* (2020) 'Implementation of The High-Speed SM4 Cryptographic Algorithm Based On Random Pseudo Rounds', in *2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA)*. Chongqing, China: IEEE, pp. 112–117. Available at: https://doi.org/10.1109/ICIBA50161.2020.9276502.

Tao, C., Petzoldt, A. and Ding, J. (2020) 'Improved Key Recovery of the HFEv- Signature Scheme'.

Tao, C., Petzoldt, A. and Ding, J. (2021) 'Efficient Key Recovery for All HFE Signature Variants', in T. Malkin and C. Peikert (eds) *Advances in Cryptology – CRYPTO 2021*. Cham: Springer International Publishing, pp. 70–93. Available at: https://doi.org/10.1007/978-3-030-84242-0_4.

Tateiwa, N. *et al.* (2024) 'Development and analysis of massive parallelization of a lattice basis reduction algorithm', *Japan Journal of Industrial and Applied Mathematics*, 41(1), pp. 13–56. Available at: https://doi.org/10.1007/s13160-023-00580-z.

Tian, J., Shen, Y. and Wang, Y. (2024) 'Blockchain-based fast handover authentication protocol for Internet of Vehicles in small industrial parks', *Vehicular Communications*, 50, p. 100848. Available at: https://doi.org/10.1016/J.VEHCOM.2024.100848.

Transactions | ethereum.org (no date). Available at: https://ethereum.org/en/developers/docs/transactions/ (Accessed: 27 August 2023).

United States Department of Transportation (USDOT) (2024) 'ARC-IT v9.2: Architecture Reference for Cooperative and Intelligent Transportation'.

V2X Core Technical Committee (no date) 'V2X Communications Message Set Dictionary'.

Veins - Vehicles in Network Simulation (no date). Available at: https://omnetpp.org/download-items/Veins.html (Accessed: 19 March 2023).

Virdis, A., Stea, G. and Nardini, G. (2014) 'SimuLTE – A Modular System-level Simulator for LTE/LTE-A Networks based on OMNeT++', in *Proceedings of the 4th International Conference on Simulation and Modeling Methodologies, Technologies and Applications*. Vienna, Austria: SCITEPRESS - Science and Technology Publications, pp. 59–70. Available at: https://doi.org/10.5220/0005040000590070.

Xie, Q. *et al.* (2023) 'Provable Secure and Lightweight Blockchain-Based V2I Handover Authentication and V2V Broadcast Protocol for VANETs', *IEEE Transactions on Vehicular Technology*, 72(12), pp. 15200–15212. Available at: https://doi.org/10.1109/TVT.2023.3289175.

Xu, S. *et al.* (2024) 'CLLS: Efficient certificateless lattice-based signature in VANETs', *Computer Networks*, 255, p. 110858. Available at: https://doi.org/https://doi.org/10.1016/j.comnet.2024.110858.

Xu, Y. *et al.* (2022) 'Optimized Design Implementation and Research of SM3 Hash Algorithm Based on FPGA', in *2022 2nd International Conference on Computer Science and Blockchain (CCSB)*. Wuhan, China: IEEE, pp. 111–117. Available at: https://doi.org/10.1109/CCSB58128.2022.00027.

Yang, Z. *et al.* (2019) 'Blockchain-based decentralized trust management in vehicular networks', *IEEE Internet of Things Journal*, 6(2), pp. 1495–1505. Available at: https://doi.org/10.1109/JIOT.2018.2836144.

Zhang, X., Zheng, Z. and Wang, X. (2022) 'A detailed analysis of primal attack and its variants', *Science China Information Sciences*, 65(3), p. 132301. Available at: https://doi.org/10.1007/s11432-020-2958-9.