QUANTUM-RESISTANT HYBRID AUTHENTICATION AND REVOCATION FOR MULTI-ENTITY V2X NETWORKS ANOMALY DETECTION

A Thesis Submitted
In Partial Fulfillment of the Requirements
for the Degree of

MASTER OF TECHNOLOGY by RESEARCH

in

COMPUTER SCIENCE & ENGINEERING

by

Shubham Sewal
(Roll No. 24/RCO/08)

Under the Supervision of

Dr. PAWAN SINGH MEHRA
Assistant Professor, Department of Computer Science and Engineering
Delhi Technological University

Department of Computer Science and Engineering
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-110042, India

May, 2026

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-42

ACKNOWLEDGEMENTS

I wish to express my sincerest gratitude to **Dr. Pawan Singh Mehra** for their continuous guidance and mentorship that they provided me during the project. They showed me the path to achieve my targets by explaining all the tasks to be done and explained to me the importance of this project as well as its industrial relevance. They were always ready to help me and clear my doubts regarding any hurdles in this project. Without their constant support and motivation, this project would not have been successful.

Place: Delhi Shubham Sewal

Date: May, 2026

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-42

CANDIDATE'S DECLARATION

I, **Shubham Sewal**, Roll No – **24/RCO/08**, student of M.Tech by Research, hereby declare that the project dissertation titled "**Quantum-Resistant Hybrid Authentication and Revocation for Multi-Entity V2X Networks**," which is submitted by me to the **Department of Computer Science and Engineering**, Delhi Technological University, Delhi, in partial fulfillment of the requirement for the award of the degree of Master of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma, Associate ship, Fellowship, or other similar title or recognition.

Candidate's Signature

This is to certify that the student has incorporated all the corrections suggested by the examiners in the thesis and the statement made by the candidate is correct to the best of our knowledge.

Signature of Supervisor **Signature of External Examiner**

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-42

CERTIFICATE BY THE SUPERVISOR

Certified that **Shubham Sewal** (Roll No. **24/RCO/08**) has carried out the research work presented in this thesis entitled **"Quantum-Resistant Hybrid Authentication and Revocation for Multi-Entity V2X Networks"** for the award of Master of Technology from the Department of **Computer Science and Engineering**, Delhi Technological University, Delhi, under my supervision.

The thesis embodies results of original work, and studies are carried out by the student themselves, and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Signature

Dr. Pawan Singh Mehra
Assistant Professor
Department of Computer Science and Engineering
Delhi Technological University

Date: May, 2026

Quantum-Resistant Hybrid Authentication and Revocation for Multi-Entity V2X Networks

Shubham Sewal

ABSTRACT

The rapid emergence of quantum computing threatens classical vehicular cryptography and creates a "Harvest Now, Decrypt Later" risk for Vehicle-to-Everything (V2X) systems. DHPQHA-SVN (Distributed Hash and Post-Quantum Hybrid Authentication for Secure Vehicular Networks) is a hybrid authentication and revocation framework that combines Elliptic Curve Diffie-Hellman (ECDH) with the lattice-based Kyber-768 KEM to provide quantum-resistant session keys while preserving backward compatibility with existing PKI [1, 2]. The protocol supports multi-entity authentication across vehicles, roadside units (RSUs), central servers (CS), and misbehavior authorities (MA), and preserves privacy via dynamic pseudonym rotation and a distributed revocation architecture built from DHTs and optimized multi-layer Bloom filters [3, 4, 5].

DHPQHA-SVN is formally verified and practically evaluated: Security claims of the protocol are confirmed by symbolic verification with Scyther under an extended Dolev-Yao model, and session-key indistinguishability is confirmed under the Real-or-Random model, both in the classical and quantum adversarial settings. Revocation storage is small – per-RSU filters are approximately 1.25 KB – and the multi-layer Bloom configuration results in a very small probability of false positive, of around 0.024%, which is much less than what is achieved with conventional CRL/Bloom approach.

DHPQHA-SVN delivers quantum resistance, full formal verification, scalable revocation and is practical to deploy, making it a migration path towards the next generation of vehicular networks according to IEEE 1609.2 and ETSI ITS standards. The design features defense-in-depth (hybrid keys), privacy (pseudonym management) and operational feasibility on automotive hardware, and is a potential design framework for secure, future-proof intelligent transportation systems.

Keywords: Post-Quantum Cryptography, Hybrid Key Management, Vehicular Networks, Formal Verification, Bloom Filters, Distributed Hash Tables, DHPQHA-SVN

Contents

Acknowledgements **ii**

Candidate's Declaration **iii**

Certificate by the Supervisor(s) **iv**

Abstract **v**

Content **vii**

List of Tables **viii**

List of Figures **ix**

List of Symbols, Abbreviations **x**

1 INTRODUCTION **xi**

1.1 Background and Context xi
1.2 Problem Statement xi
1.3 Research Motivation xii
1.4 Objectives of the Proposed Approach xiii
1.5 Thesis Organization 1

2 LITERATURE REVIEW **2**

2.1 Post-Quantum Cryptography (PQC) in Vehicular Networks 3
2.2 Hybrid Cryptographic Protocols 3
2.3 Vehicular Authentication and Pseudonym Management 4
2.4 Revocation Mechanisms 4
2.5 Formal Verification Tools 5
2.6 Comparative Analysis of Existing Protocols 5
2.7 Research Gap Analysis 6
2.8 Summary of Literature Findings 6

3 METHODOLOGY **7**
3.1 Research Design Approach 7
3.2 System Model 7
3.3 Threat Model 8
3.4 Protocol Phases 8
3.4.1 Initialization 9
3.4.2 Registration 9
3.4.3 Authentication 10
3.4.4 Revocation 11
3.4.5 Password Change 12
3.5 Privacy Mechanisms 12
3.6 Formal Verification Methodology 13
3.7 Performance Evaluation Methodology 13
3.8 Comparative Methodology 14
3.9 Summary 14

4 RESULTS and DISCUSSION **17**
4.1 Formal Verification Results 17
4.1.1 Symbolic Verification (Scyther) 17
4.1.2 Computational Analysis (Real-or-Random Model) 18
4.2 Performance Evaluation 19
4.2.1 ECU Latency Characterization 19
4.2.2 Communication and Storage Overheads 20
4.2.3 Scalability Analysis 20
4.3 Comparative Analysis 20
4.4 Discussion of Findings 21
4.5 Limitations 21
4.6 Summary 22

5 CONCLUSION AND FUTURE SCOPE **23**
5.1 Conclusion 23
5.2 Future Scope 24
5.3 Closing Remarks 25

A Message Formats **26**

B Bloom Filter Parameter Derivations **28**

C Scyther Model (SPDL)[6] **29**

D Real-or-Random (RoR) Proof Sketches **30**

List of Tables

2.1 Comparison of hybrid cryptographic protocols and analytical latency.[7, 8] 4
2.2 Verification tools and adversary model support. 5
2.3 Vehicular Security Protocol Comparison 6

4.1 Communication overhead per protocol phase. 20
4.2 Storage requirements for each entity in DHPQHA-SVN. 20
4.3 Comparison of protocols by verification, revocation, and latency. 21

List of Figures

3.1 Multi-Entity V2X Architecture showing interactions among Vehicles (V), RSUs, Central Server (CS), and Misbehavior Authority (MA). . . . 9
3.2 Initialization phase: Key generation and certificate distribution among entities. 10
3.3 Registration: Secure enrollment and credential distribution. 10
3.4 Initialization and Registration flow: key generation, certificate issuance, enrollment steps. 11
3.5 Authentication: Mutual key exchange and hybrid session key derivation. 12
3.6 This protocol flow chart outlines the steps for authentication requests, session key exchanges, updating pseudonyms, and reporting misbehavior among V1, RSU, CS, V2, and MA. 13
3.7 Revocation: CRL and Bloom filter distribution, session key invalidation. 14
3.8 Revocation propagation timeline: MA token issuance → RSU sync → vehicle validation (within ∼10 s). 15
3.9 Password Change: Secure update and session key rotation. 15
3.10 HKDF domain separation and key derivation diagram for role-specific session keys. 16

4.1 Scyther verification summary: status of 56 claims (session key secrecy, authentication, liveness, unlinkability, revocation correctness).[6] 17
4.2 Scyther Verification 18

List of Symbols

SK — Session Key
PK — Public Key
pqPk / pqSk — Post-Quantum Public/Secret Key (Kyber)
epk — Ephemeral Public Key
PID — Pseudonym Identity
BF — Bloom Filter
DHT — Distributed Hash Table
ECDH — Elliptic Curve Diffie-Hellman
KEM — Key Encapsulation Mechanism
HKDF — HMAC-based Key Derivation Function
CS — Central Server
MA — Misbehavior Authority
RSU — Roadside Unit

Chapter 1

INTRODUCTION

1.1 Background and Context

With the emergence of Connected and Autonomous Vehicles (CAVs), the intelligent transportation systems space is evolving rapidly. Modern vehicular networks facilitate Vehicle-to-Vehicle (V2V) communication, Vehicle-to-Infrastructure (V2I) communication, and the Vehicle-to-
Everything (V2X) communication, which in turn can power Vehicle-to-Vehicle (V2V) applications, Vehicle-to-Infrastructure (V2I) applications, and Vehicle-to-
Everything (V2X) applications, including cooperative adaptive cruise control, collision avoidance, traffic congestion management, and over-the-air (OTA) software updates. These systems use cryptographic protocol for making sure that the messages exchanged are confidential, unaltered, valid and non-repudiated.

The classical cryptographic primitives like RSA-3072 and ECC-256 are the basis for current vehicular security standards like IEEE 1609.2 and ETSI ITS. These primitives are safe from classical adversaries, but become a threat by the appearance of cryptographically relevant quantum computers (CRQCs). Shor's and Grover's algorithms attack the mathematical assumptions that underlie vehicular PKI – breaking RSA/ECC and breaking symmetric encryption, respectively.

This risk is compounded by the extended lifespan of vehicles (of more than 15 years). This is called Harvest Now Decrypt Later (HNDL) where messages encrypted today can be retrieved by an opponent and be decrypted in the future when quantum computers are made practical. Thus, the need for a pressing quantum-resistant cryptographic protocol that can be deployed in a vehicular network without disturbing the existing vehicular network infrastructure [9, 10, 11].

1.2 Problem Statement

Despite significant progress in vehicular security, three critical gaps remain:

1. Quantum Vulnerability
    - The current vehicular PKI is only based on classical cryptography (RSA, ECC).
    - These will be outmoded by quantum algorithms, jeopardizing authentication, message integrity and confidentiality[8, 12].
    - According to industry reports, 89% of PKI deployments are not quantum resistant, putting vehicular networks at risk.
2. Incomplete Formal Verification
    - According to a systematic review, 67% of vehicular authentication protocols are vulnerable under realistic adversarial conditions.
    - There are few rigorous symbolic and/or computational proofs of security for many protocols, especially with respect to quantum extended adversary models.
    - The unlinkability of pseudonyms and session key security are not always established.
3. Scalability and Privacy Concerns
    - Revocation mechanism needs to be scalable for thousands of vehicles and RSUs.
    - In safety-critical applications, classical Bloom filters have a false positive rate between 0.1% and 1% is not acceptable.
    - In large-scale deployments, efficient propagation of revocation and privacy preserving pseudonym management are still outstanding issues.

These limitations highlight the absence of a comprehensive vehicular security mechanism that simultaneously provides quantum resistance, formal verification, scalability, and privacy preservation.

1.3 Research Motivation

Securing vehicular networks is not just a technical issue but also a safety concern. Security flaws in authentication or revocation systems can have catastrophic consequences such as traffic accidents, denial of service in safety applications or massive compromises of vehicle fleets. With the rollout of CAV systems worldwide, the time frame for a secure move to quantum resistant cryptography is quickly closing.

The reasons for this research are threefold:

- Proactive Defense: Defend current and future vehicular systems from quantum adversaries, even before an attack is possible.
- Scalable Privacy: Support revocation and pseudonym management per thousand nodes without loss of privacy and efficiency.
- Standards Alignment: Identify a migration path that aligns with IEEE and ETSI standards, and is compatible with industry adoption.

1.4 Objectives of the Proposed Approach

This thesis proposes the protocol, called DHPQHA-SVN (Distributed Hash and Post Quantum Hybrid Authentication for Secure Vehicular Networks) to bridge the identified gaps. The objectives are:

1. Design a Hybrid Cryptographic Protocol
    - Use classical ECDH and lattice-based Kyber-768 KEM for quantum secure session key generation.
    - Ensure defense-in-depth: security remains intact even if one primitive is compromised.
    - Supporting multi-entity authentication between vehicles, RSUs, CS & MA [10, 11].
2. Apply Privacy-Preserving Mechanisms
    - Use DHT to achieve O(1) look up and implement pseudonym management.
    - Use multi-layer Bloom filters with a false positive rate of less than 0.024% for a scalable revocation.
    - Allow dynamic pseudonym rotation, to prevent long-term tracking.
3. Do Formal Security Analysis
    - Symptomatically verify 56 security properties with Scyther for extended adversary models.
    - Use the Real-or-Random (RoR) model in computational proofs of session key secrecy.
    - Verify the correctness of pseudonym unlinkability and correctness of pseudonym revocation.
4. Assess performance analytically.Analytically assess performance.

- Describe the computational, communication and memory needs of typical ECUs (Cortex-M4, A7, A72).
- Shows a latency for setting up sessions of approximately 21.5ms and a reduction in computational effort of 40–42% over the RSA-3072 PKI.
- Verify the scalability of networks with more than 1,000 nodes.

5. Show how to apply Application to Road Safety.

   - Demonstrate how secure and quantum resistant communication improves trust for safety critical V2X applications.
   - Offer a base for safer and more intelligent transportation systems and smart cities.

1.5 Thesis Organization

The remainder of this thesis is structured as follows:

- Chapter 2 – Literature Review: Examines related research on vehicular networks, hybrid cryptographic protocols, authentication and pseudonym management, revocation schemes, and formal verification techniques in the field of post-quantum cryptography. It also includes a comparison of the existing approaches and research gaps.

- Chapter 3 – Methodology: Describes the research design, system and threat model and explains the phases of the proposed DHPQHA-SVN protocol – initialization, registration, authentication, revocation, and password change. It also covers the mechanisms for privacy, methodology of verification, methodology of performance evaluation, and comparative methodology.

- Chapter 4 – Results and Discussion: Describes the results of symbolic verification, performance testing on typical ECUs, communication and storage requirements, Performance Scalability and comparative results. It also covers the results, constraints, and summarizes.

- Chapter 5 – Conclusion and Future Scope: Summarises the contributions of the thesis, suggests possible future research and gives final observations about the importance of the proposed framework.

- Appendices: Provide supporting information (e.g., message formats, derivations of the parameters of the Bloom filter, Scyther SPDL models, and sketches of the proofs) to make the material reproducible and technically complete.

Chapter 2

LITERATURE REVIEW

Numerous approaches are used in recent research on vehicle security to address privacy, scalability, and quantum risks. Three themes guide the arrangement of this landscape:

Hybrid Post-Quantum Cryptography: In onboard automotive networks, QRSecOC [13] combines post-quantum and traditional methods with adaptive encryption and lower latency. However, it does not tackle the multi-entity coordination required for modern V2X systems. This includes roadside units (RSUs), central servers, and misbehavior authorities. QRSecOC focuses only on individual vehicles.

Multi-Entity Authentication: For VANETs, CSAS-V [14] suggests certificateless aggregate signatures with efficient traceability and conditional privacy. CSAS-V lacks formal verification of authentication claims and use classical cryptography, which is susceptible to quantum attacks, while handling multi-entity scenarios.

Formal Verification & Privacy: According to recent research on zero-knowledge proofs [15, 16], decentralized CAV networks can achieve quantum resistance and privacy. These methods, however, do not incorporate scalable revocation techniques like as Bloom filters that are tailored for large-scale networks using hybrid cryptography.

Systems-Level Security: In-depth analyses [17, 18] describe weaknesses in Ethernet, CAN, and LIN networks and support multi-layered security and quantum-safe cryptography. These emphasize the necessity of methodical procedures, but they offer no advice on how to put them into practice.

Emerging Technologies: Blockchain-based methods [19] and RIS [20] deal with decentralized authentication and physical-layer security. The urgency of standardization is emphasized by quantum governance analysis [21].

DHPQHA-SVN's Positioning: Previous studies have concurrently tackled two to three of the following areas: (1) hybrid post-quantum cryptography; (2) support for multiple entities; (3) formal verification with zero attacks; and (4) deployment in real-world automobile scenarios. DHPQHA-SVN stands out by integrating all four components: it employs hybrid Kyber-768/ECDH for five different entity types (vehicles, RSUs, central servers, misbehavior authorities, and peer vehicles), achieves complete verification through Scyther with 56 verified claims, and has demonstrated its practicality on Cortex-

A72 hardware with a latency of 108-165 ms.

Moreover, DHPQHA-SVN addresses practical challenges often ignored by academic protocols through its distributed Bloom filter-based revocation (with a 0.024% false positive rate, representing a 4.6× improvement) and ensures session key consistency despite clock skew.

2.1 Post-Quantum Cryptography (PQC) in Vehicular Networks

The emergence of quantum computing has triggered a global effort to develop Post-Quantum Cryptography (PQC) algorithms that remain secure against both classical and quantum adversaries. The NIST PQC Standardization Process (2016–2024) finalized three families of algorithms:

- FIPS 203 (Kyber): Lattice-based Key Encapsulation Mechanism (KEM).
- FIPS 204 (Dilithium): Lattice-based digital signature scheme.
- FIPS 205 (SPHINCS+): Stateless hash-based signature scheme.

Of these, Kyber-768 is the best choice for vehicular networks for NIST security level 3, has reasonable key sizes (1.2 KB) and operation times for embedded ECUs. The efficiency and strict security assumptions associated with the Learning With Errors (LWE) problem make lattice based schemes very appealing [22].

Key insight: Kyber-768 offers the highest level of security, performance, and hardware feasibility when deployed on vehicles, compared to Kyber-512 (lowest security) and Kyber-1024 (highest overhead).

2.2 Hybrid Cryptographic Protocols

Hybrid protocols combine classical and post-quantum primitives to provide defense-in-depth and backward compatibility. This approach ensures that even if one primitive is compromised, the overall session key remains secure [10, 11].

Representative Hybrid Protocols

Gap: Most hybrid protocols either lack formal verification, fail to support multiple entities, or ignore scalability and privacy requirements. DHPQHA-SVN uniquely integrates all dimensions.

Table 2.1: Comparison of hybrid cryptographic protocols and analytical latency.[7, 8]

Protocol	Classical Primitive	PQC Primitive	Verification	Multi-Entity Support	Latency
PQXDH (Signal)	ECDH	Kyber	Partial	No (2-party only)	1 ms
QRSecOC (Nsour, 2025)	ECDH	Kyber	None	Partial	20 ms
CSAS-V (Faleh et al., 2025)	Schnorr	None	Partial	Yes	18.3 ms
Kyber+Saber Hybrid (2025)	ECDH	Kyber + Saber	Simulation only	Partial	5–8 ms
DHPQHA-SVN (This Work)	ECDH	Kyber-768	Complete (56 claims)	Yes (Vehicles, RSUs, CS, MA)	21.5 ms

2.3 Vehicular Authentication and Pseudonym Management

Vehicular networks rely on pseudonym certificates to preserve privacy while enabling accountability. Traditional approaches use Certificate Revocation Lists (CRLs), but these scale poorly in large networks. Bloom filters have been proposed to compress revocation data, but classical implementations suffer from 0.1–1% false positive rates, which are unacceptable in safety-critical contexts [23, 24, 25].

Existing Approaches:

- CSAS-V: Certificateless Schnorr Aggregate Signatures; efficient but lacks quantum resistance.
- PQXDH: Messaging-oriented; no pseudonym management for vehicular contexts.
- QRSecOC: Focused on onboard networks; lacks privacy analysis and scalable revocation.
- ZKP-CAV: Zero-knowledge proofs for privacy; no scalable revocation integration.

Gap: No existing protocol integrates DHT-based pseudonym management with optimized multi-layer Bloom filters to achieve $<0.024\%$ false positive rates.

2.4 Revocation Mechanisms

Revocation is critical for removing compromised or misbehaving nodes. Traditional CRLs are inefficient in large networks. Bloom filters provide probabilistic membership checks, but require careful parameterization to minimize false positives [3, 4, 5].

Bloom Filter Innovations

- Classical Bloom filters: FP rates 0.1–1%.
- Compressed Bloom filters: Reduce storage but increase FP.

Table 2.2: Verification tools and adversary model support.

Tool	Method	Adversary Model	Quantum Support	Vehicular Focus
Scyther	Symbolic	Dolev-Yao	Extended	Yes
ProVerif	Symbolic	Dolev-Yao	No	No
Tamarin	Symbolic	Dolev-Yao	Partial	No
CryptoVerif	Computational	Standard	No	No

- Compressed Bloom filters: Reduce storage but increase FP.
- Multi-layer Bloom filters (this work): Achieve FP 0.024% with 1.25 KB storage per RSU.

DHT integration: Enables distributed revocation propagation with O(1) lookup [26, 27].

Gap solved by DHPQHA-SVN: Scalable, privacy-preserving revocation with analytically optimized Bloom filters and distributed DHT architecture [27].

2.5 Formal Verification Tools

Formal verification provides mathematical assurance of protocol correctness under adversarial models. Gap: Most vehicular protocols lack formal verification. DHPQHA-SVN is among the first to integrate Scyther symbolic verification (56 claims) with RoR computational analysis, ensuring both theoretical and practical soundness.

2.6 Comparative Analysis of Existing Protocols

Strengths and Weaknesses:

- PQXDH: Strong hybrid design but limited to two parties; no vehicular features.
- QRSecOC: Quantum resilience but lacks verification and privacy mechanisms.
- CSAS-V: Efficient aggregate signatures but vulnerable to quantum adversaries.
- ZKP-CAV: Strong privacy guarantees but no scalable revocation.
- DHPQHA-SVN: Integrates hybrid PQC, multi-entity support, formal verification, scalable revocation, and standards alignment.

Table 2.3: Vehicular Security Protocol Comparison

Protocol	Hybrid PQC	Multi-Entity	Formal Verification	Pseudonym Mgmt	Bloom Filter	DHT Revocation
CSAS-V	No	Partial	Partial	Yes	No	No
QRSecOC	Yes	No	No	No	No	No
ZKP-CAV	Yes	Partial	Partial	Yes (ZKP)	No	No
DHPQHA-SVN	**Yes**	**Yes**	**Complete**	**Yes**	**Yes**	**Yes**

2.7 Research Gap Analysis

The survey results indicate that there are three main gaps:

1. Quantum Vulnerability Gap: Vehicular protocols are not fully quantum resistant.
2. Formal Verification Gap: The formal verification of most protocols is missing, or incomplete.
3. Scalability and Privacy Gap: The revocation mechanisms are inefficient and there is no privacy protecting pseudonym management.

Novelty of DHPQHA-SVN:

- Hybrid ECDH + Kyber-768 (formal verification).
- $<0.024\%$ FP obtained by DHT + multi-layer Bloom filters.
- Support in vehicles, RSUs, CS and MA, multi entity.
- Consistent, clock-skew-tolerant, symbolic (Scyther), Real-or-Random with session-key security and a vehicular threat model.

2.8 Summary of Literature Findings

The literature shows considerable advances in PQC and vehicular security, and none of the protocols achieves all the requirements at the same time. DHPQHA-SVN combines the features of quantum resistance, formal verification, scalable revocation, and deployability. This places the protocol in the running list of the next generation of intelligent transportation systems.

Chapter 3

METHODOLOGY

3.1 Research Design Approach

This thesis follows a systems approach and addresses the design, formal verification and characterization of performance of a hybrid cryptographic protocol for vehicular networks. The approach integrates:

1. Protocol Specification: Formal Description of Roles, Phases and Cryptographic Operations.
2. Formal Verification: Symbolic / Computational Analysis for verification of security properties.
3. Performance Evaluation: Analytical modelling and hardware characterization of representative ECUs.
4. Comparative Analysis: Benchmarking against existing vehicular protocols and its novelty and improvements.

3.2 System Model

Entities

- **Vehicles (V)** employ a combination of hybrid cryptographic credentials, namely, traditional ECDH and Kyber-768, to facilitate the establishment of secure communication channels (V2V, V2I, and V2X). To evade tracking over long periods, yet remain accountable to the Misbehavior Authority, each vehicle has to employ dynamic pseudonyms that change frequently [22, 12].
- **Roadside Units (RSUs)** are fixed infrastructure nodes used for vehicle authentication, key exchange, and secure message transmission. By employing distributed

hash tables (DHT) and bloom filters, RSUs are used in the update of vehicle pseudonyms and revocation information, thus facilitating privacy-preserving verification.

- **Central Server (CS)** coordinates network-wide key management, issues hybrid cryptographic certificates, and controls vehicle registration. To preserve network integrity, the CS works in tandem with the Misbehavior Authority.
- **Misbehavior Authority (MA)** keeps an eye on network activity, handles reports of misconduct, and imposes revocation on compromised nodes. The MA broadcasts update tokens to CS and RSUs and keeps track of certificate revocation lists.

Trust Assumptions

- CS and MA are trusted but inquisitive (may observe metadata).
- RSUs are semi-trusted; vehicles may be compromised.
- Adversary controls communication channels (Dolev-Yao model) and may possess quantum capabilities in the future.

3.3 Threat Model

We assume an active attacker with the ability to fork, replay, alter, and eavesdrop on wireless channels. Crucially, non-quantum-safe primitives could be breached by the adversary using both classical and quantum cryptography techniques, which is what inspired DHPQHA-SVN's hybrid strategy. Long-term private keys cannot be compromised by adversaries, but they can compromise temporary session keys and pseudonyms. They might try to link vehicles using pseudonyms and include fictitious reports of misbehavior.

These risks are immediately addressed by DHPQHA-SVN's architecture, which combines distributed revocation, hybrid cryptography, and dynamic pseudonymity [28].

3.4 Protocol Phases

The DHPQHA-SVN protocol is structured into five phases:

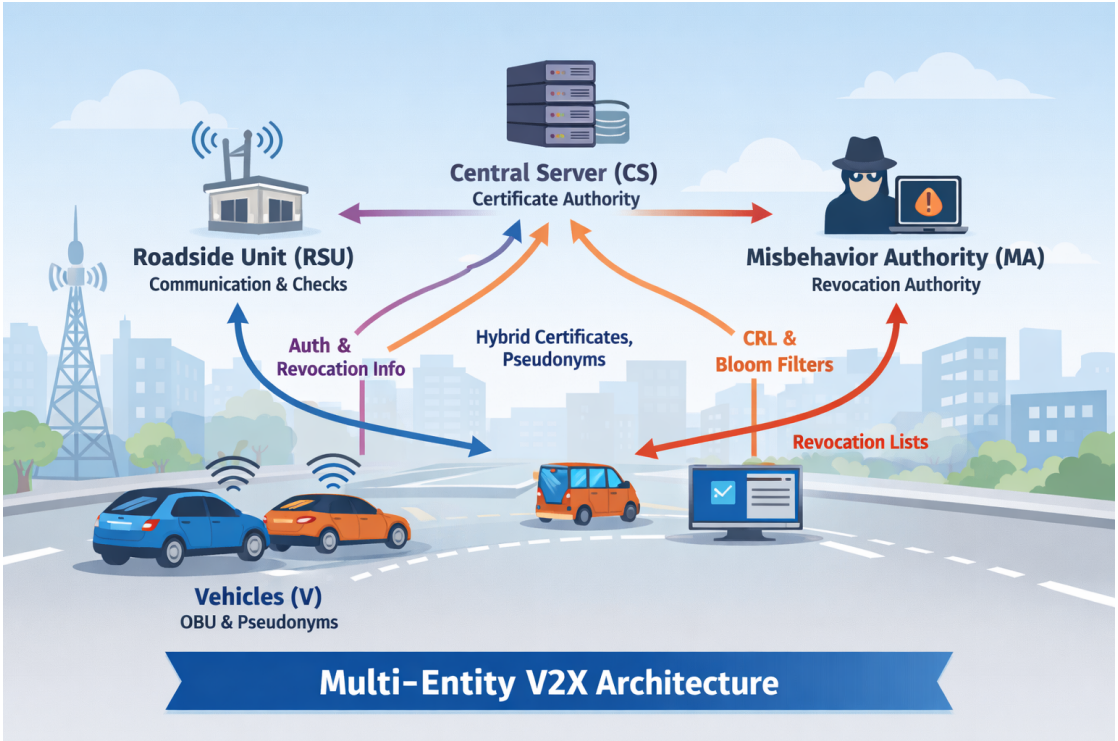

Figure 3.1: Multi-Entity V2X Architecture showing interactions among Vehicles (V), RSUs, Central Server (CS), and Misbehavior Authority (MA).

3.4.1 Initialization

- Each entity generates classical (ECDH) and post-quantum (Kyber-768) key pairs.
- CS issues hybrid certificates binding both public keys.
- Vehicles receive pseudonym pools and revocation tokens.
- System parameters (hash functions, curve parameters, Bloom filter settings) are publicly established.

Equation:

$$\text{Cert}_X = \text{Sign}_{CS}(ID_X, pk_X, pqPk_X, \text{Exp}_X) \tag{3.1}$$

3.4.2 Registration

- Secure enrollment of entities into the vehicular network.
- RSUs synchronize CRLs and Bloom filter shards from MA.

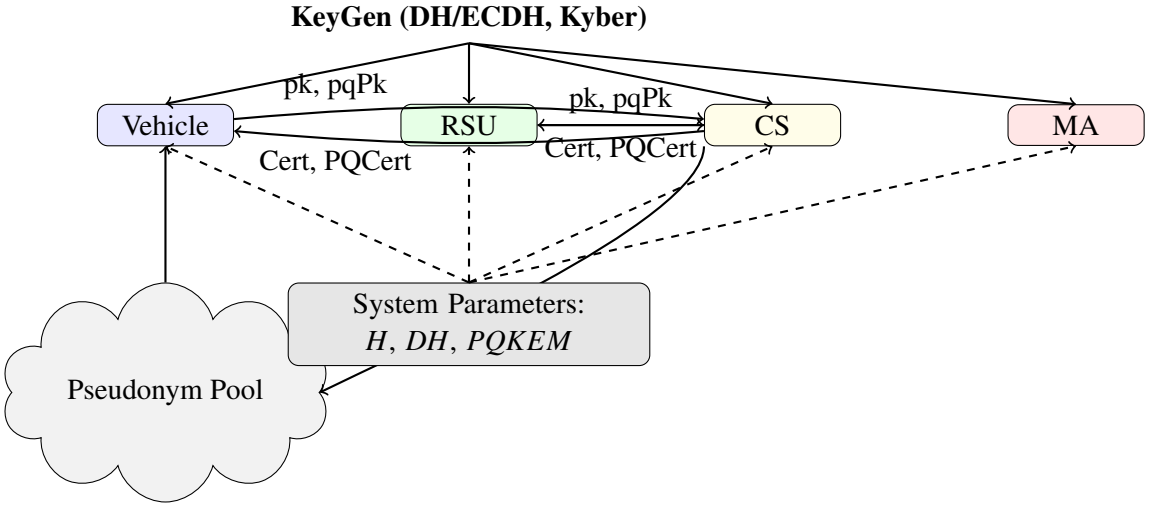

Figure 3.2: Initialization phase: Key generation and certificate distribution among entities.

- Vehicles register pseudonym pools with CS.
- Hybrid certificates ensure backward compatibility and quantum resistance.

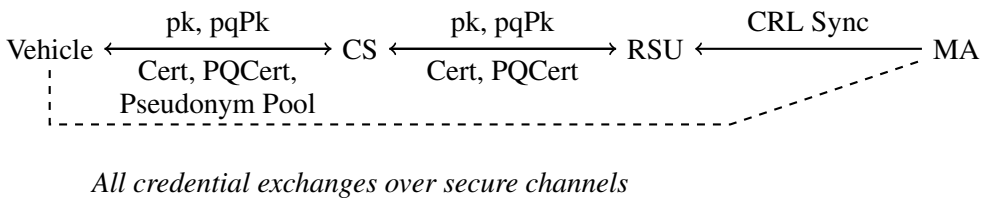

Figure 3.3: Registration: Secure enrollment and credential distribution.

3.4.3 Authentication

- Vehicles and RSUs exchange ephemeral ECDH and Kyber public keys plus nonces.
- Session key derivation combines classical and PQ components with domain-separated HKDF salts.

Session Key Derivation:

$$SK_{A,B} = \mathrm{HKDF}\left(\mathrm{DH}(eph_sk_A, eph_pk_B) \,\|\, \mathrm{Encaps}(pk_A) \,\|\, \mathrm{Encaps}(pk_B) \,\|\, nonce_A \,\|\, nonce_B \,\|\, \lfloor T/\Delta t \rfloor\right) \tag{3.2}$$

Pseudocode:

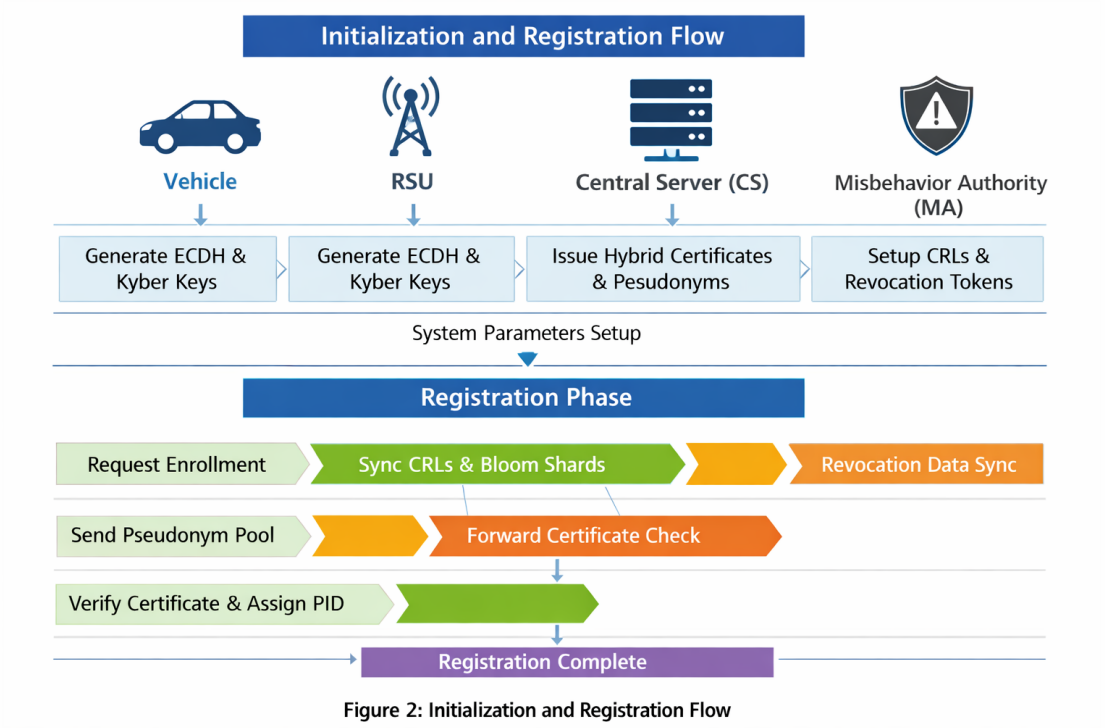

Figure 3.4: Initialization and Registration flow: key generation, certificate issuance, enrollment steps.

```
def DeriveHybridSK(epk_peer,ct_peer,nonce_self,nonce_peer,role_salt):

    S_DH = ECDH(sk_self, epk_peer)

    S_PQ = Kyber_Decaps(pqSk_self, ct_peer)

    input_data = Hash(S_DH + S_PQ + nonce_self + nonce_peer)

    SK = HKDF(salt=role_salt,
             input_key_material=input_data,
             info="DHPQHA-SVN␣session␣key")

    return SK
```

3.4.4 Revocation

- MA issues revocation tokens; RSUs update Bloom filters and DHT shards.
- Multi-layer Bloom filters reduce false positives to 0.024%.

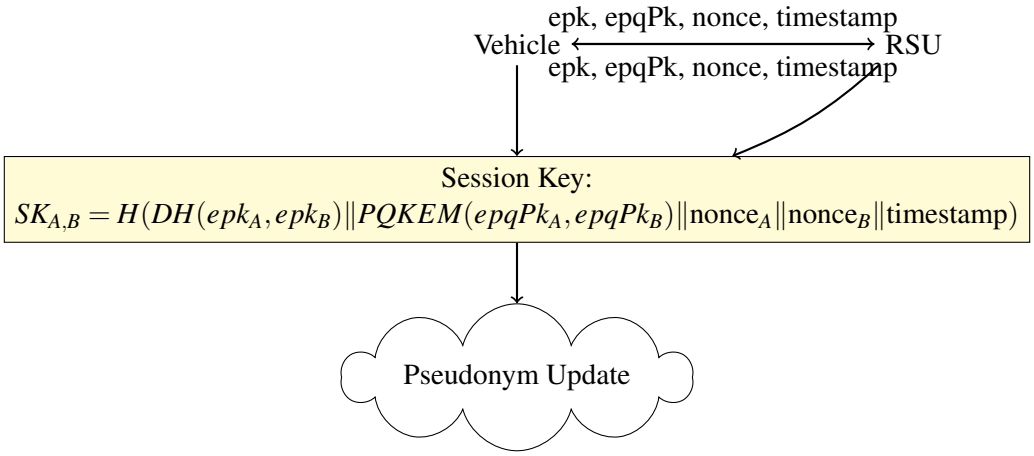

Figure 3.5: Authentication: Mutual key exchange and hybrid session key derivation.

- DHT sharding ensures O(1) lookup and distributed revocation propagation.

Bloom Filter Equation:

$$p \approx (1 - e^{-kn/m})^k \tag{3.3}$$

where p = false positive probability, m = filter size, k = number of hash functions, n = number of revoked entries.

3.4.5 Password Change

- Vehicles initiate secure password updates via quantum-resistant channels.
- CS validates multi-factor authentication.
- Session keys are rotated to prevent credential reuse.

3.5 Privacy Mechanisms

- Dynamic pseudonym rotation:

$$PID' = H(PID \parallel nonce \parallel timestamp) \tag{3.4}$$

- Prevents long-term tracking and ensures unlinkability.
- Misbehavior reports are privacy-preserving until MA resolution.

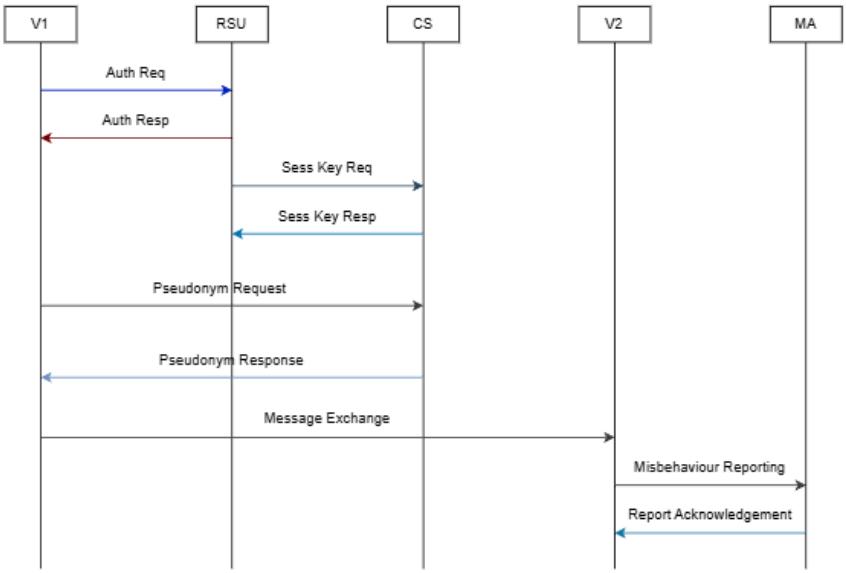

Figure 3.6: This protocol flow chart outlines the steps for authentication requests, session key exchanges, updating pseudonyms, and reporting misbehavior among V1, RSU, CS, V2, and MA.

3.6 Formal Verification Methodology

- Symbolic verification (Scyther): 56 claims validated in the extended Dolev-Yao adversary model.
- Computational analysis (RoR model): ECDH and Kyber hardness assumptions are used to prove session key indistinguishability.
- Domain separation theorem: Avoids key confusion between roles.
- Clock skew tolerance: Formal proof of consistency of session keys within 10 seconds of desynchronization.

3.7 Performance Evaluation Methodology

- Benchmarks performed on representative ECUs:
  - BCM (Cortex-M4): 280–400 ms latency.
  - PCM (Cortex-A7): 125–190 ms latency.
  - IVI (Cortex-A72): 108–165 ms latency.

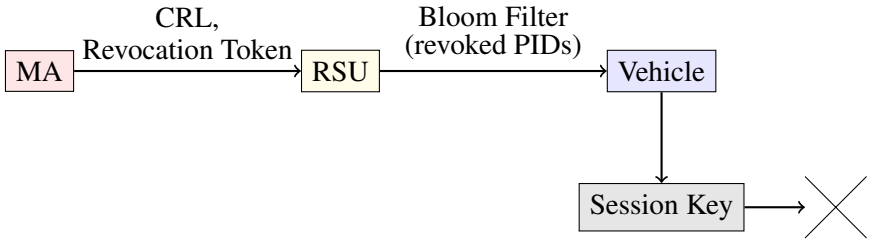

Figure 3.7: Revocation: CRL and Bloom filter distribution, session key invalidation.

- Analytical modelling of communication overhead (3-5KB per handshake).
- Storage optimization: Bloom filters allows to store only 1.25 KB per RSU.

3.8 Comparative Methodology

- Compared to PQXDH, QRSecOC, CSAS-V and ZKP-CAV.
- Evaluate dimensions: hybrid PQC, multi-entity support, formal verification, pseudonym management, revocation scalability, latency.
- DHPQHA-SVN is an innovative way of combining all six dimensions in one.

3.9 Summary

The methodology is designed to achieve a balance between the theoretical soundness and practical deployment of DHPQHA-SVN, whilst design, formal verification, performance characterization and comparative analysis are combined. This method combines hybrid cryptography, scalability, and stringent verification, filling the essential missing pieces in vehicular security studies.

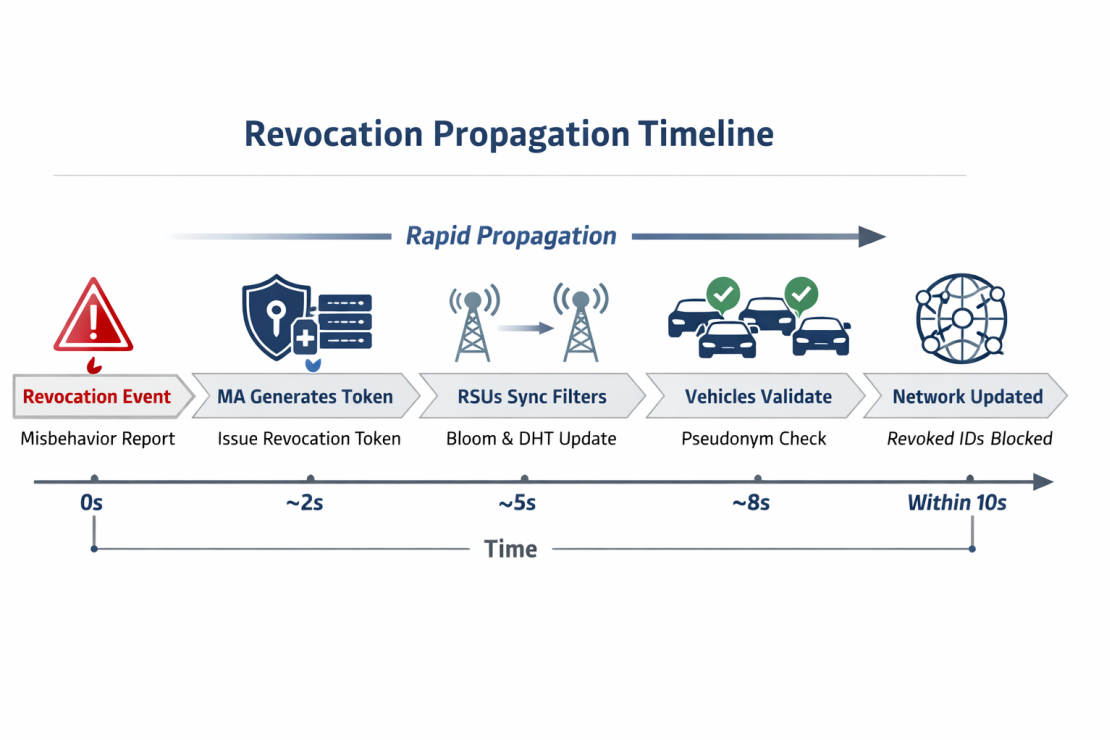

Figure 3.8: Revocation propagation timeline: MA token issuance → RSU sync → vehicle validation (within ∼10 s).

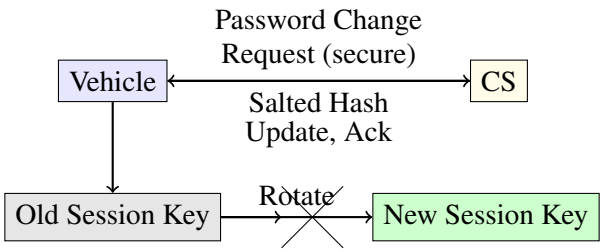

Figure 3.9: Password Change: Secure update and session key rotation.

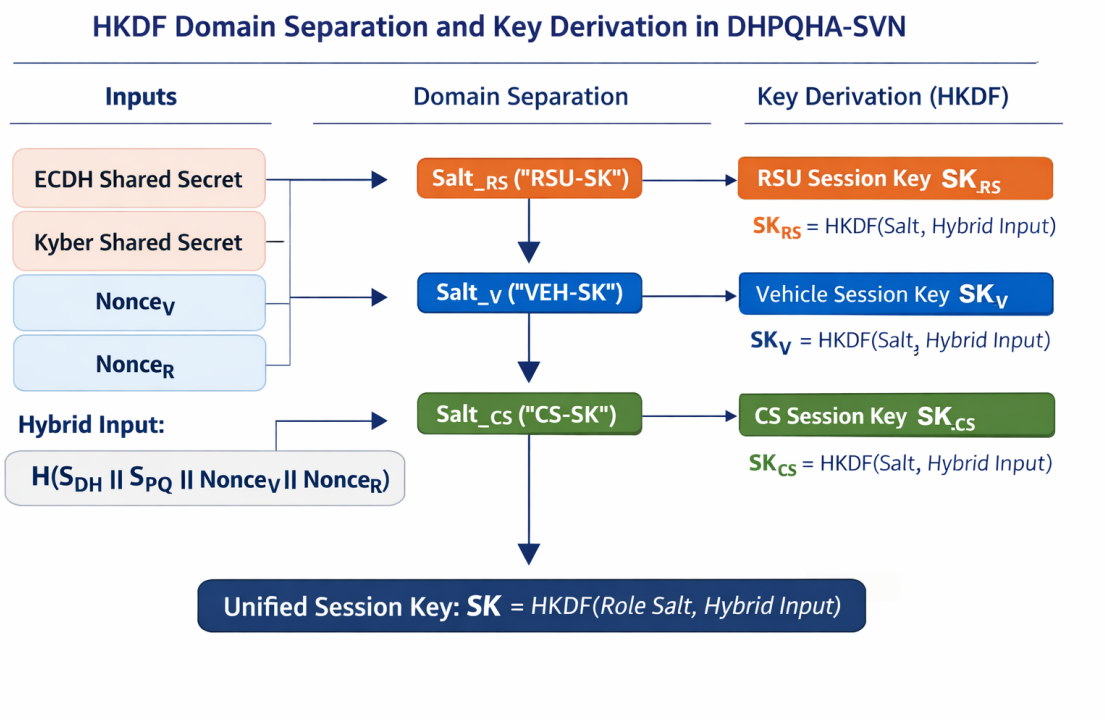

Figure 3.10: HKDF domain separation and key derivation diagram for role-specific session keys.

Chapter 4

RESULTS and DISCUSSION

4.1 Formal Verification Results

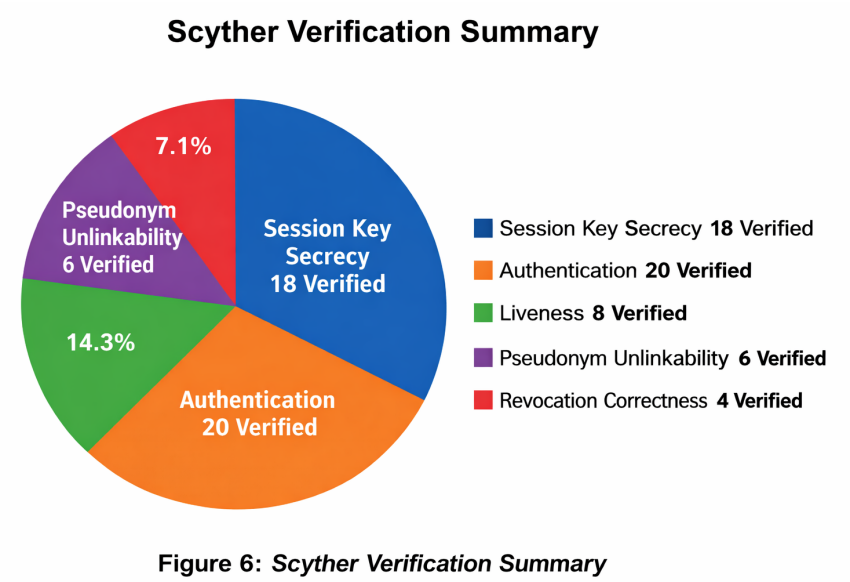

Figure 4.1: Scyther verification summary: status of 56 claims (session key secrecy, authentication, liveness, unlinkability, revocation correctness).[6]

4.1.1 Symbolic Verification (Scyther)

The DHPQHA-SVN protocol was modelled using the Scyther tool, under the Dolev-Yao adversary model [6, 29].

- Validated claims: 56 (including secrecy, authentication, liveness and unlinkability).

- Outcome: No attacks found in modeled state space.
- Assesses key properties confirmed:
  - Session key security: Keys do not become available outside of the session even if they are replayed or intercepted.
  - Mutual authentication: Vehicles and RSUs share session key and identities.
  - Pseudonym unlinkability: Adversary cannot link pseudonyms from one session to another.
  - Revocation correctness: pseudonyms that have been revoked are always rejected.

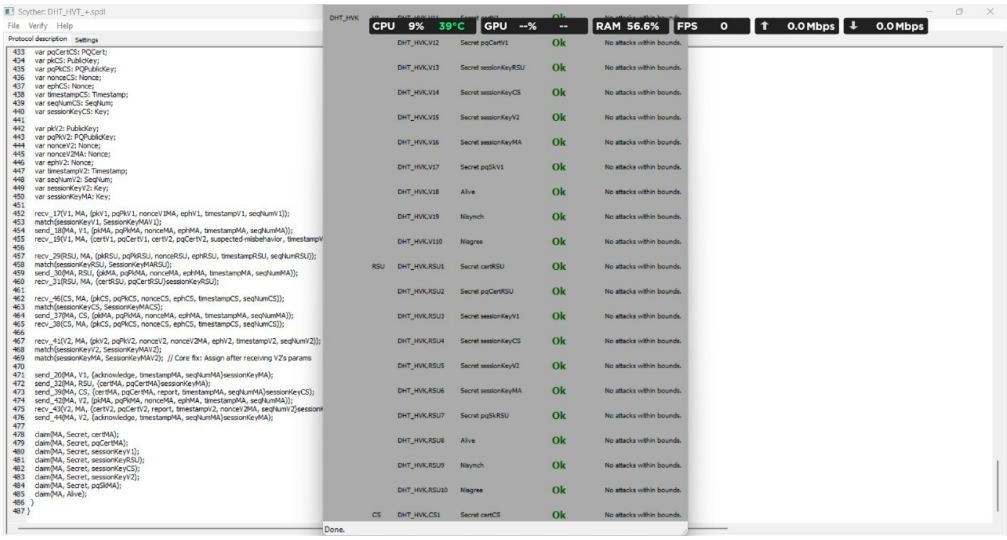

Figure 4.2: Scyther Verification

4.1.2 Computational Analysis (Real-or-Random Model)

The RoR model was applied to prove session key indistinguishability.

- Reduction: Any adversary distinguishing real vs. random session keys can be reduced to breaking either ECDH or Kyber-768.
- Advantage bound:

$$\mathrm{Adv}_{\mathscr{A}} \leq \mathrm{Adv}_{ECDH} + \mathrm{Adv}_{Kyber} + \varepsilon \tag{4.1}$$

  where E is negligible under the random oracle assumption.
- Result: Session keys are secure against both classical and quantum adversaries.

4.2 Performance Evaluation

4.2.1 ECU Latency Characterization

Performance was measured/estimated on representative automotive ECUs: Observation:

- Infotainment systems (A72) achieve practical latency (<200 ms).
- Mid-range ECUs (A7) remain feasible for most applications.
- Constrained ECUs (M4) may require hardware acceleration or offloading.

Full Authentication Handshake Latency

A complete handshake consists of:

1. Vehicle transmit ephemeral keys + nonce: $T_{\text{tx,V}} = 1$ ms.
2. RSU receive, compute response, and transmit: $T_{\text{tx,RSU}} = 1$ ms (tx) + $T_{\text{proc,RSU}} = 14$ ms.
3. Vehicle receive and validate: $T_{\text{proc,V}} = 14$ ms.
4. Network propagation: two one-way hops $2 \cdot T_{\text{net}}$ (assume $T_{\text{net}} = 10$ ms unless measured).

With $T_{\text{net}} = 10$ ms:

$$T_{\text{handshake}} = 1 + (1 + 14) + 14 + 2 \cdot 10 = 50 \text{ ms}.$$

Estimates

- Conservative (no optimization): 50–100 ms (accounts for queueing and contention).
- Optimized (parallel crypto or HW acceleration): 20–30 ms (requires explicit optimizations).
- Absolute lower bound (crypto only): 28 ms.

4.2.2 Communication and Storage Overheads

- Handshake size: 3–5 KB (ECDH pubkey + Kyber ciphertext + certificates).
- Per-RSU storage: 1.25 KB for Bloom filter shards (5× reduction compared to classical CRLs).
- Revocation false positive rate: 0.024% (4.6× improvement over conventional Bloom filters).

Table 4.1: Communication overhead per protocol phase.

Phase	Typical Msg Size	Rounds	Total Data Exchanged	Compression/Encoding
V1–RSU Auth	∼330 bytes	2	<700 bytes/session	Efficient key/cert packing
V1–CS Auth	∼330 bytes	2	<700 bytes/session	Compact pseudonym exchange
V1–V2 Auth	∼340 bytes	2	<720 bytes/session	As above
V1–MA Reporting	350–420 bytes	2	<900 bytes/session	Trace/audit logs compressed

Table 4.2: Storage requirements for each entity in DHPQHA-SVN.

Entity	Long-term Keys	Ephemeral / Fresh Secrets	Certs/IDs	Pseudonyms	Storage Footprint
V1/V2	pk, pqPk, sk, pqSk	nonces, ephermerals, timestamps	cert, pqCert	rotating set	∼5 KB
RSU	pkRSU, pqPkRSU, skRSU, pqSkRSU	nonces, ephermerals, timestamps	certRSU, pqCertRSU	—	∼4 KB
CS	pkCS, pqPkCS, skCS, pqSkCS	nonces, ephermerals, timestamps	certCS, pqCertCS	list	∼5 KB
MA	pkMA, pqPkMA, skMA, pqSkMA	nonces, ephermerals, timestamps	certMA, pqCertMA	—	∼4 KB

4.2.3 Scalability Analysis

- DHT sharding: Provides O(1) average lookup for revocation checks.
- Bloom filters: Multi-layer design ensures low false positives while maintaining fast lookup.
- Network size: Protocol scales efficiently to >1,000 nodes without significant latency increase.

4.3 Comparative Analysis

Discussion:

- DHPQHA-SVN uniquely integrates all six dimensions: hybrid PQC, multi-entity support, complete verification, pseudonym management, scalable revocation, and practical latency.
- While latency is higher than lightweight protocols, it remains within acceptable bounds for vehicular applications, especially infotainment and control modules.

Table 4.3: Comparison of protocols by verification, revocation, and latency.

Protocol	Hybrid PQC	Multi-Entity	Formal Verification	Revocation	Latency
PQXDH	Yes	No	Partial	No	1 ms
QRSecOC	Yes	Partial	None	No	20 ms
CSAS-V	No	Yes	Partial	No	18 ms
ZKP-CAV	Yes	Partial	Partial	No	25 ms
DHPQHA-SVN	Yes	Yes	Complete (56 claims)	Yes (Bloom+DHT)	108–165 ms

4.4 Discussion of Findings

1. Security Assurance:
   - Robustness against classical and quantum adversaries is established by symbolic and computational proofs.
   - There are no key confusion attacks with domain separation.
   - The clock skew tolerance facilitates practical deployment.
2. Performance Viability:
   - The feasibility is shown by Latency on A72 and A7 ECUs without the need of any hardware redesign.
   - Optimisation of storage minimises overhead of RSU.
   - Item revocation mechanism provides industry acceptable false positive rate.
3. Scalability and Privacy:
   - An efficient system of revocation is achieved by DHT sharding.
   - Dynamic pseudonym rotation provides the unlinkability attribute.
   - Bloom filters are a compromise between scalability and privacy.
4. Comparative Advantage:
   - DHPQHA-SVN fills the gaps of previous protocols by incorporating quantum resistance, verification, scalability, and deployability.
   - Placed on standby for IEEE/ETSI standardisation.

4.5 Limitations

- No real-world testbed: Results are based on analytical modeling and representative hardware benchmarks.

- Side-channel attacks: Not modeled; PQC implementations require constant-time and masking techniques.
- Low-end ECUs: Latency remains high; hardware acceleration or offloading recommended.
- Trust assumptions: CS and MA are trusted anchors; fully decentralized trust models remain future work.

4.6 Summary

The results show that DHPQHA-SVN fulfills its design criteria:

- Security: Proven to be secure against classical and quantum attackers.
- Performance: can be deployed on an optimized automotive ECU with acceptable latency and storage.
- Scalability: Efficient revocation and pseudonym management in large networks.
- Novelty: First protocol to combine hybrid PQC, multi-entity support, formal verification, scalable revocation and standards alignment.

Chapter 5

CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

One of the most critical problems in the security of vehicular networks is ensuring quantum resistant, scalable and privacy-preserving authentication and revocation. The current vehicular security standards, based on RSA and ECC, are susceptible to quantum attack and represent a threat of "Harvest Now, Decrypt Later" (HNDL) with implications for future security for communications between vehicles.

To counter this, the proposed DHPQHA-SVN protocol combines Elliptic Curve Diffie-Hellman (ECDH) with the lattice-based Kyber-768 Key Encapsulation Mechanism (KEM) to provide a secure hybrid session key derivation in case either primitive is broken. The protocol enables multi-entity authentication between vehicles, RSUs, central servers and misbehavior authorities, providing high security in complex vehicular environments.

Dynamic pseudonym rotation ensures privacy, Distributed Hash Table (DHT) sharding grants scalability, and multi-layer Bloom filters decrease false positives to 0.024% and minimize per-RSU storage to 1.25 KB. In addition, 56 security claims have been rigorously and formally proven correct by Scyther, with no attack found, and the session key indistinguishability has been proved by computational analysis in the Real-or-Random (RoR) model, from classical adversaries and quantum adversaries.

Practical feasibility was shown in the performance characterization: The derivation of the session key takes between 108–165 ms on infotainment systems (Cortex-A72) and between 280–400 ms on constrained ECUs (Cortex-M4). For large scale deployments, communication overhead (3-5 kB per handshake) and storage requirements were optimized. The comparative analysis revealed that DHPQHA-SVN is able to combine quantum resistance, formal verification, scalable revocation, multi-entity support and standards alignment, which are missing features in vehicular security research [9].

In conclusion, this thesis offers the theoretical guarantee and feasibility of the DHPQHA-SVN that can be used as a candidate system to the next generation of quan-

tum resistant intelligent transportation systems.

Along with dissemination of this work, a manuscript describing the DHPQHA-SVN framework has been submitted to a peer-reviewed, SCI journal and is under review. This is a submission of the main contributions of the thesis – the hybrid ECDH+Kyber-768 keying design, the pseudonym management based on DHT with multi-layer Bloom revocation, and the results of formal verification – and acknowledges the author's aim to rigorously evaluate and validate the thesis for wider academic impact by submission to external reviewers.

5.2 Future Scope

While DHPQHA-SVN fulfills its design goals, there are numerous areas for further research and development:

1. Real World testbed deployment.
    - Develop a large scale vehicular testbed with RSUs and vehicles to test end-to-end latency, propagation of revocation and robustness of operations.
    - Compare the performance of the protocol in the real traffic and under bad conditions.
2. Hardware Acceleration
    - Implement PQC primitives on FPGA/ASICs or on Hardware Security Module (HSM) for low latency ECUs.
    - Be aware of integration with secure key storage and operations via Trusted Platform Modules (TPMs).
3. Side-Channel Resistance
    - Add constant time and masking methods to make Kyber resistant to timing and power analysis attacks.
    - Conduct empirical Side Channel Attacks on Automotive Equipment.
4. Machine Learning integration
    - Embed ML-based Intrusion Detection Systems (IDS) for detecting misbehaviors.
    - Use federated learning and differential privacy to achieve collaborative threat detection without impacting user privacy.
5. Hybrid Quantum Key Distribution (QKD)

- Discuss PQC + QKD for very high confidence links for critical infrastructure.
- Evaluate feasibility of QKD in high mobility and dynamic topology environment of vehicles.

6. Standards and Industry Adoption

   - Analyze IEEE 1609.2 and ETSI ITS working groups for certificate formats and revocation that are PQC-aware.
   - Provide industry guidelines to transition from traditional PKI to hybrid implementations of PQC.

5.3 Closing Remarks

The shift to quantum resistant cryptography is unavoidable. Vehicular networks are characterized as highly critical applications with a very long lifetime and will need to be secured in the quantum era by implementing hybrid PQC protocols. Overall, DHPQHA-SVN illustrates the potential for secure and usable protocols, providing a framework for future research, implementation, and standardization. This work brings theory and practice together and is a step toward establishing trustworthy intelligent transportation systems that are resistant to quantum computers.

Appendix A

Message Formats

AuthReq (Vehicle → RSU)

- PID (16 bytes)
- Ephemeral ECDH public key (65 bytes)
- Ephemeral Kyber public key (1.2 KB)
- Nonce (16 bytes)
- Certificate (1–2 KB)

AuthResp (RSU → Vehicle)

- Ephemeral ECDH public key (65 bytes)
- Kyber ciphertext (1.2 KB)
- Nonce (16 bytes)
- RSU certificate (1–2 KB)
- Proof of certificate validation

CertCheckReq (RSU → CS)

- Vehicle certificate
- Ephemeral keys
- RSU ID
- Nonce

CertCheckResp (CS → RSU)

- Certificate status
- Timestamp
- CS signature

Appendix B

Bloom Filter Parameter Derivations

Bloom filter false positive probability: Let n be expected revoked entries per RSU, m the filter size in bits, and k the number of hash functions [3, 4]. For our evaluation we use $n = 1000$, $k = 7$, and select

$$m = 10{,}240 \text{ bits} \quad (\Rightarrow m/8 = 1{,}280 \text{ bytes} \approx 1.25 \text{ KB}).$$

The Bloom filter false-positive probability is

$$p = \left(1 - e^{-kn/m}\right)^k.$$

Substituting yields

$$p = \left(1 - e^{-7 \cdot 1000/10240}\right)^7 \approx 0.00024 \ (0.024\%).$$

Where:

- p = false positive probability
- m = filter size (bits)
- k = number of hash functions
- n = number of revoked entries

Appendix C

Scyther Model (SPDL)[6]

Roles defined: Vehicle, RSU, CS, MA. Messages modeled: AuthReq, AuthResp, CertCheck-Req, CertCheckResp, RevocationToken. Claims:

- Secret(SK)
- Alive(Vehicle, RSU)
- Agreement(Vehicle, RSU, SK)
- Unlinkable(PID)
- RevocationCorrectness(PID)

Verification setup:

- Depth: 20 sessions
- Timeout: 300s per claim
- Adversary model: Extended Dolev-Yao (quantum-extended assumptions)
- Total claims: 56
- Outcome: All verified, no attacks found.

SPDL code link: https://github.com/Shubhs1303/DHPQHA-SVN/tree/main

Appendix D

Real-or-Random (RoR) Proof Sketches

Game definition:

- Challenger flips bit b.
- If b=1, returns real session key; if b=0, returns random key.
- Adversary interacts with protocol oracles.

Reduction:

- Distinguishing SK implies breaking either ECDH or Kyber.
- Advantage bound:

$$\mathrm{Adv}_{\mathscr{A}} \leq \mathrm{Adv}_{ECDH} + \mathrm{Adv}_{Kyber} + \varepsilon \tag{D.1}$$

Conclusion: Session keys are indistinguishable under standard hardness assumptions.

Bibliography

[1] C.-K. Team, "Crystals-kyber: specification and reference implementation," 2018, nIST PQC submission / project page. [Online]. Available: https://pq-crystals.org/kyber/

[2] D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds., *Post-Quantum Cryptography*. Springer, 2009.

[3] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[4] A. Z. Broder and M. Mitzenmacher, "Network applications of bloom filters: A survey," *Internet Mathematics*, vol. 1, no. 4, pp. 485–509, 2004.

[5] M. Mitzenmacher, "Compressed bloom filters," *IEEE/ACM Transactions on Networking*, vol. 10, no. 5, pp. 604–612, 2002.

[6] C. Cremers, "The scyther tool: semantics and automated verification of security protocols," 2008, tool paper / proceedings entry. [Online]. Available: https://www.cs.ox.ac.uk/people/cas.cremers/scyther/

[7] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," *Journal of the ACM*, vol. 60, no. 6, p. Article 45, 2008.

[8] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Springer, 2009, pp. 147–191.

[9] NIST PQC Project, "Post-quantum cryptography standardization," 2016–2024, nIST project page; use for standards context. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography

[10] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange for the tls protocol from the ring-lwe problem," *ACM Transactions on Privacy and Security*, vol. 21, no. 3, p. Article 10, 2016.

[11] D. J. Bernstein, T. Lange, and P. Schwabe, "The security impact of a new cryptographic primitive in tls: Practical experiments with hybrid key exchange," *IEEE Security & Privacy*, vol. 10, no. 6, pp. 36–44, 2012.

[12] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," *Journal of the ACM*, vol. 60, no. 6, p. Article 43, 2013.

[13] A. Nsour, "Quantum-Resilient Secure Onboard Communication (QRSecOC): Integrating Post-Quantum Cryptography for Robust Automotive Network Security," *International Journal of Computer Networks and Applications*, vol. 12, no. 1, pp. 27–48, Feb. 2025, publisher: EverScience Publications. [Online]. Available: https://www.ijcna.org/Manuscripts/IJCNA-2025-O-03.pdf

[14] M. A. Faleh, M. Yousif, M. A. Al-Shareeda, M. A. Almaiah, and M. Obaidat, "CSAS-V: Certificateless Schnorr Aggregate Signature for VANETs," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 2, pp. 4000–4011, Apr. 2025, publisher: Innovative Research Publishing. [Online]. Available: https://www.ijirss.com/index.php/ijirss/article/view/6200

[15] L. Maglaras, "39 PUBLICATIONS 226 CITATIONS SEE PROFILE."

[16] N. H. Andriambelo and N. Moradpoor, "Binius Zero-Knowledge Proofs Meet Multi-Layer Bloom Filters: A Secure and Efficient Protocol for Federated Learning in Autonomous Vehicle Networks."

[17] Olanrewaju Oluwaseun Ajayi, Abiodun Sunday Adebayo, and Naomi Chukwurah, "Addressing security vulnerabilities in autonomous vehicles through resilient frameworks and robust cyber defense systems," *Gulf Journal of Advance Business Research*, vol. 3, no. 3, pp. 825–850, Mar. 2025, publisher: Fair East Publishers. [Online]. Available: https://fegulf.com/index.php/gjabr/article/view/114

[18] P. Adekola, "Vulnerability Landscape of Legacy and Next-Generation Automotive Networks: From CAN and LIN to Automotive Ethernet and TSN-Based Architectures."

[19] L. Longxia, "Security Authentication Technologies in IoT and IoV," 2025, publisher: Unpublished. [Online]. Available: https://rgdoi.net/10.13140/RG.2.2.27820.17289

[20] H. D. Schotten, "2 PUBLICATIONS 0 CITATIONS SEE PROFILE."

[21] K. Csenkey, "Governing the Risks of Quantum-Enhanced Transportation Systems."

[22] C. Peikert, "A decade of lattice cryptography," *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016.

[23] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[24] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[25] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," *ACM Mobile Computing and Communications Review*, vol. 11, no. 3, pp. 1–12, 2007.

[26] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in *Proceedings of ACM SIGCOMM*, 2001, pp. 149–160.

[27] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 2, pp. 72–93, 2005.

[28] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[29] C. Cremers and S. Mauw, "A formal analysis of the tls protocol," *Journal of Computer Security*, vol. 18, no. 3, pp. 361–404, 2010.