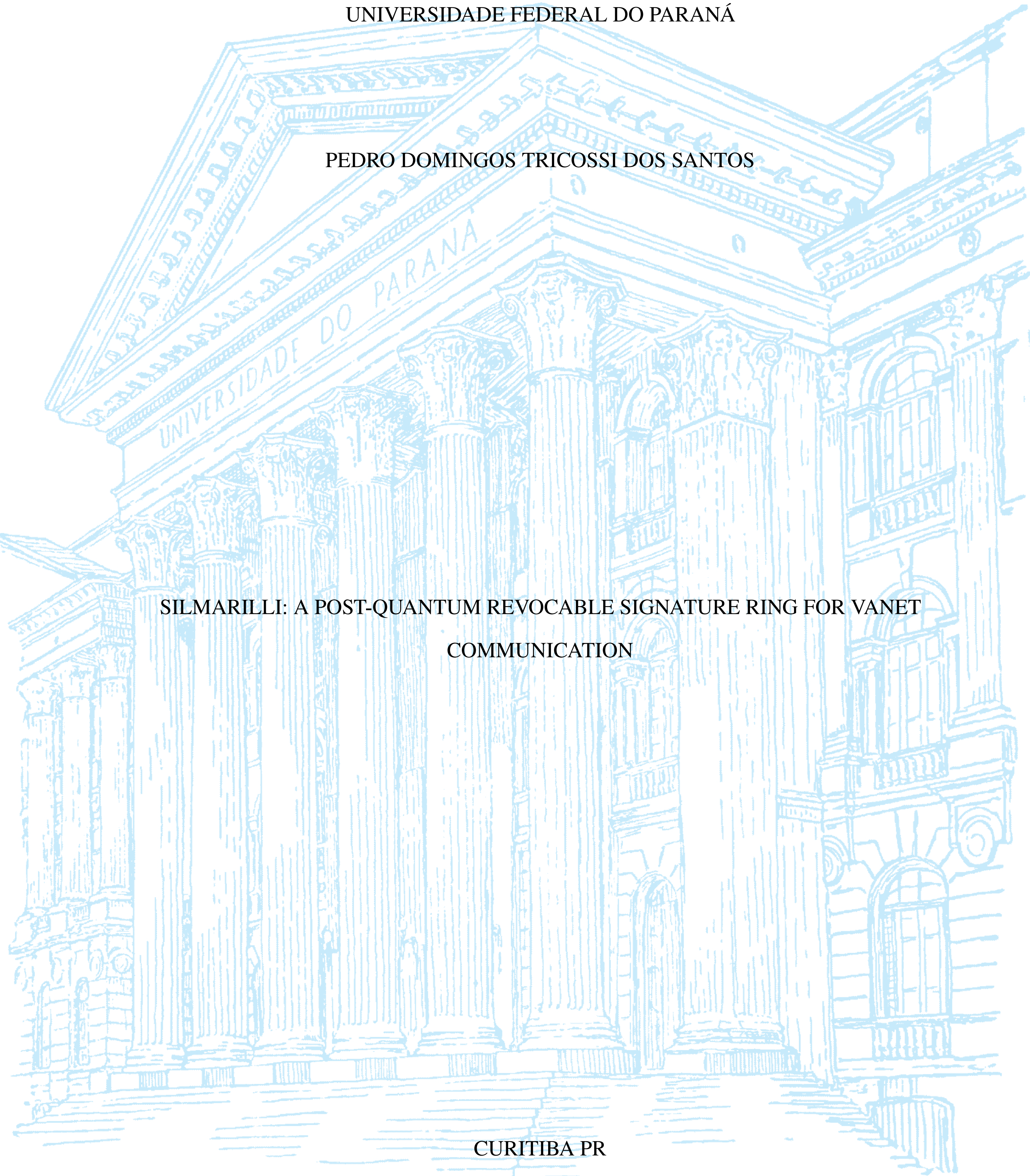
UNIVERSIDADE FEDERAL DO PARANÁ



PEDRO DOMINGOS TRICOSSI DOS SANTOS

SILMARILLI: A POST-QUANTUM REVOCABLE SIGNATURE RING FOR VANET COMMUNICATION

CURITIBA PR

2025

PEDRO DOMINGOS TRICOSSI DOS SANTOS

SILMARILLI: A POST-QUANTUM REVOCABLE SIGNATURE RING FOR VANET COMMUNICATION

Trabalho apresentado como requisito parcial à conclusão do Curso de Bacharelado em Ciência da Computação, Setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Computação*.

Orientador: Luiz Carlos Pessoa Albini.

CURITIBA PR

2025

Dedico esse trabalho aos meus pais, não somente aqueles que me deram a vida, mas também aqueles que me adotaram como filho durante essa essa jornada.
Dedico aos meus irmãos, não somente a de sangue, mas aqueles que mesmo sem laço criaram algo mais forte que sangue.
Dedico a quem acreditou em mim, mesmo nos momentos em que nem eu mesmo acreditava.
E dedico a quem segurou minha mão, aguentou todo o estresse e reclamação advindas da escrita desse trabalho

RESUMO

A crescente integração de sistemas de transporte inteligentes (ITS) à infraestrutura urbana moderna impõe uma necessidade crítica de proteger as comunicações em redes ad hoc veiculares (VANETs), especialmente devido à ameaça iminente da computação quântica aos sistemas de criptografia clássicos. Este trabalho aborda esse desafio apresentando o SILMARILLI, um inovador esquema de criptografia de sigilo em anel revogável pós-quântico projetado especificamente para atender aos rigorosos requisitos de baixa latência, eficiência computacional e escalabilidade do ambiente VANET. O objetivo principal é fornecer um mecanismo que garanta simultaneamente a autenticidade, a confidencialidade, a rastreabilidade de agentes mal-intencionados e a revogabilidade de credenciais comprometidas - propriedades essenciais para a operação segura e confiável de redes veiculares. A metodologia empregada baseia-se na construção de uma primitiva criptográfica sobre os algoritmos baseados em treliça padronizados pelo NIST, CRYSTALS-Dilithium e CRYSTALS-Kyber, garantindo uma resistência robusta contra ataques de computadores clássicos e quânticos. A análise de desempenho do esquema demonstra sua viabilidade prática, alcançando uma latência estimada de ponta a ponta de 15,72 ms para um anel de oito veículos, um valor que está dentro dos limites operacionais dos aplicativos de segurança em tempo real. No entanto, essa eficiência é obtida em troca de um consumo considerável de recursos, principalmente um tamanho de assinatura de aproximadamente 62 KB e um espaço de memória significativo para o armazenamento de dados pré-computados.

Palavras-chave: Criptografia pós-quantica , Revocable Signature Ring, Seguranca em VANET

ABSTRACT

The growing integration of intelligent transportation systems (ITS) into modern urban infrastructure imposes a critical need to secure communications in Vehicular Ad-hoc Networks (VANETs), especially given the imminent threat of quantum computing to classical cryptosystems. This work addresses this challenge by introducing SILMARILLI, an innovative post-quantum revocable ring signcryption scheme specifically designed to meet the stringent requirements of low latency, computational efficiency, and scalability of the VANET environment. The primary objective is to provide a mechanism that simultaneously ensures authenticity, confidentiality, traceability of malicious actors, and the revocability of compromised credentials—properties essential for the safe and reliable operation of vehicular networks. The methodology employed is based on constructing a cryptographic primitive over the NIST-standardized lattice-based algorithms, CRYSTALS-Dilithium and CRYSTALS-Kyber, ensuring robust resilience against attacks from both classical and quantum computers. The scheme's performance analysis demonstrates its practical viability, achieving an estimated end-to-end latency of 15.72 ms for a ring of eight vehicles, a value that falls within the operational limits of real-time safety applications. However, this efficiency is achieved in exchange for considerable resource consumption, notably a signature size of approximately 62 KB and a significant memory footprint for storing pre-computed parameters. It is concluded that SILMARILLI represents a theoretically sound and secure framework for VANET communications in the post-quantum era, while the identified practical challenges, such as communication overhead, motivate clear directions for future research focused on optimization and compression.

Keywords: Post-Quantum Cryptography, Revocable Signature Ring, VANET Security

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ASIC	Application Specific Integrated Circuit
DAA	Direct Anonymous Attestation
FORS	Forest of Random Subsets
IND-CCA2	Indistinguishability under Adaptive Chosen-Ciphertext Attack
ITS	Intelligent Transportation Systems
KGC	Key Generation Center
LaRRS	Lattice-based Revocable Ring Signature
LBCSC	Lattice-based chameleon signcryption scheme
LHS-C2I	lattice-based heterogeneous signcryption scheme
LWE	Learning With Errors
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
MLWE	Module Learning With Errors
MSIS	Module Short Integer Solution
NIST	National Institute of Standards and Technology
NTT	Number Theoretic Transform
OBU	On-Board Units
PQC	Post-Quantum Cryptographic
RAM	Random Access Memory
RCL-PKE	Revocable Certificateless Public Key Encryption
Ring-LWE	Ring-Learning With Errors
Ring-SIS	Ring-Short Integer Solution
RL	Revocation List
RSU	Road-Side Units
SIS	Small Integer Solution
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SUF-CMA	Strong Unforgeability under Chosen-Message Attack
TA	Trusted Authority
TPMS	Trusted Platform Modules
V2I	Vehicle-to-Infrastructure communication
V2V	Vehicle-to-Vehicle communication
V2X	Vehicle-to-Everything communication
VANET	Vehicular Ad-hoc Network
WOTS+	Winternitz One-Time Signatures

LIST OF SYMBOLS

$\mathcal{R}$	A ring
$\mathcal{R}_q$	The polynomial quotient ring $\mathbb{Z}_q[x]/(x^d + 1)$
q	A prime modulus
d	The degree of the polynomial quotient ring
n, m	Integer dimensions for matrices and vectors
$\Lambda(X)$	A lattice generated by the basis matrix X
$\mathbb{Z}_q$	The ring of integers modulo q
S_η	The set of polynomials with coefficients bounded by η
$D_{\Lambda,\delta,y}$	A discrete Gaussian distribution over a lattice Λ
χ	An error distribution over a ring $\mathbb{Z}$
η	A bound for the infinity norm of polynomials in S_η
κ	A parameter related to the challenge set of the hash function
μ	The message to be signed and encrypted
π	The index of the signer in the ring
ρ, ρ'	Seed values used for generating cryptographic parameters
σ	The signature output by the SignCrypt algorithm
ψ, ψ'	Hash values used for message integrity verification
ζ	A random seed value
Ω_i	An intermediate value in the SignCrypt algorithm
A, X	Public matrices in $\mathcal{R}_q^{n\times m}$ used in the scheme
c	The ciphertext component from the Kyber KEM
C_π	The ciphertext generated by the signer π
C_1, C_2	Components of the ciphertext C_π
e, e_1, e_2	Error vectors/polynomials sampled from a distribution
H, H_2	Cryptographic hash functions
id_i	The unique identity of vehicle i
K	A key, either from a hash output or a KEM
L	The set of public keys of the ring members
pk, sk	A public key and secret key pair
s, s_1, s_2	Secret vectors/polynomials used in key generation and signing
t, t_0, t_1	Public vectors/polynomials derived during key generation
T	A timestamp
$\perp$	A symbol representing rejection or an invalid state

CONTENTS

1 INTRODUCTION

One of the pillars of scientific research is improving the quality of human life. In this context, computer science plays a pivotal role by offering tools and methodologies to address complex and multidisciplinary challenges, including those in transportation, healthcare, and cybersecurity.

Among the many fields transformed by computer science, transportation stands out particularly due to the growing demand for intelligent infrastructure and efficient mobility solutions. The integration of computational tools has led to the development of Intelligent Transportation Systems (ITS), which optimize traffic management, enhance safety, and improve overall mobility.

The implementation of ITS in cities such as Zurich and Oslo, has resulted in measurable improvements in traffic management and urban mobility (Papadakis et al., 2024). These systems have led to reduced congestion, improved public transportation efficiency, and enhanced road safety through real-time data integration and predictive traffic modelling (Mohamed, 2019).

The effectiveness of ITS relies on a flawless communication between vehicles and infrastructure, a challenge that intersects multiple computer science subfields, such as computer networks, artificial intelligence, data mining, and cryptography. This communication is primarily conducted through Vehicular Ad-hoc Networks (VANETs), which enable direct, wireless data exchange among vehicles and between vehicles and infrastructure.

In most implementations, VANETs are composed of three main components: On-Board Units (OBUs), Road-Side Units (RSUs) and the Trusted Authority (TA). OBUs are embedded in vehicles and serve as the primary interface for wireless communication. They enable two key modes of communication: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). V2V refers to the direct exchange of information between nearby vehicles, while V2I refers to the interaction between vehicles and fixed infrastructure units such as RSUs. Together, these communication types fall under the broader concept of vehicle-to-everything (V2X), which encompasses all forms of vehicular connectivity within a networked environment. The RSUs, positioned along the roads, act as intermediaries between OBUs and the Trusted Authority. The TA acts as a central entity responsible for key management and ensuring secure communication within the network. A graphical representation of a VANET is provided in figure 4.1.

Vehicular Ad Hoc Networks (VANETs), due to decentralized architecture, high mobility, and frequent topology changes, are exposed to a diverse range of security threats. The reliance on open wireless channels exposes the network to adversarial actions such as:

- Message spoofing, in which an adversary forges messages to impersonate legitimate vehicles, can lead to false alerts or fabricated traffic conditions that compromise situational awareness.

- Sybil attacks, exploit the absence of centralized identity verification, allowing a single node to present multiple false identities, thereby skewing consensus mechanisms and destabilizing routing or traffic control decisions.

- Eavesdropping, enabled by the broadcast nature of vehicular communication, poses a significant threat to user privacy, as attackers may intercept and analyze message contents or vehicle trajectories.

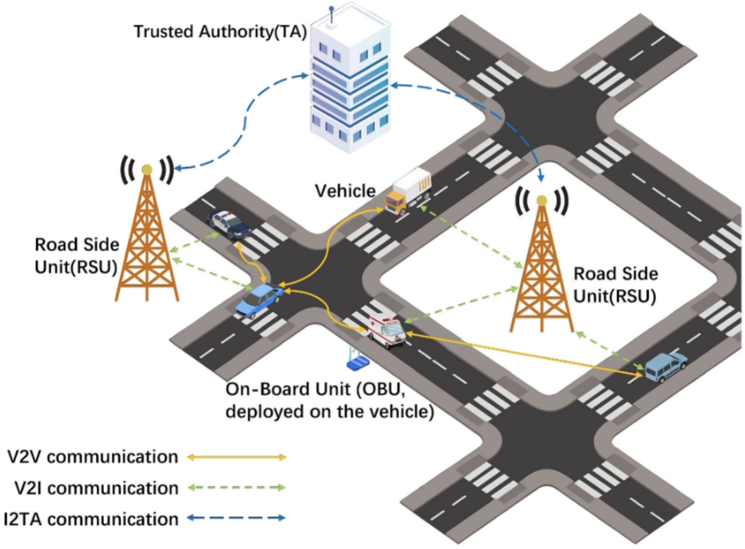


Figure 1.1: VANET communication.

- In general, malicious interference with vehicular messages can disrupt cooperative awareness protocols, mislead autonomous navigation systems, and compromise critical infrastructure coordination.

To address these threats, this work introduces SILMARILLI, a post quantum cryptographic messaging schema tailored to the specific operational constraints of VANETs, such as latency sensitivity, computational efficiency, and scalability. The proposed schema enhances both message integrity and source authentication while ensuring forward secrecy and resilience under adversarial network conditions.

As VANETs become integral to modern transportation, ensuring secure communication remains a critical challenge. Traditional cryptographic methods, while effective against classical threats, face increasing vulnerabilities with advancements in quantum computing. Emerging quantum technologies, such as Shor's algorithm, threaten widely used encryption schemes (Shor, 1999). To address these concerns, cryptographic solutions must transition towards post-quantum security. The proposed schema incorporates two of the most recent standard primitives from National Institute of Standards and Technology (NIST): lattice-based cryptography and hash-based cryptography, ensuring resilience against quantum-enabled attacks. A detailed description of these primitives is provided in chapter 4.

In parallel with advances in cryptography, research in the domain of vehicular networks has established a set of foundational security requirements that any robust VANET communication system must fulfill (Hasrouny et al., 2017). These requirements guide the design of the proposed schema, which aims to ensure the following properties:

- Authentication
- Integrity
- Confidentiality
- Revocability
- Traceability

A more detailed analysis of these security properties, including their relevance and implementation challenges, is presented in Chapter 4 (Hasrouny et al., 2017) (Engoulou et al., 2014) (Mejri et al., 2014).

This work is organized as follows. Chapter 2 provides a comprehensive review of the literature on post-quantum cryptography in the context of VANETs, situating the contribution of the proposed schema within existing research. Chapter 3 defines the mathematical and algorithmic primitives necessary to build post-quantum cryptographic schemas. Chapter 4 introduces the proposed schema, detailing the algorithms, security guarantees, and proofs. Chapter 5 evaluates the schema results, such as keys and signature sizes, and execution time. Finally, Chapter 6 concludes the thesis and outlines directions for future research.

2 RELATED WORK

The security challenges of Vehicular Ad Hoc Networks (VANETs) have been studied in recent years. The increasing capabilities of adversaries, combined with the integration of emerging technologies such as 5G networks and edge computing, rises the necessity of developing robust security protocols. This chapter reviews the state-of-the-art in VANET security, focusing on post-quantum cryptographic approaches and their implications for secure communication protocols (Singh et al., 2021) (Luo et al., 2018) (Boukerche et al., 2008) (Mukhtar et al., 2015) (Mohamed, 2019) (Mundhe et al., 2020) (Jiao and Xiang, 2021) (Chen et al., 2021) (Cao et al., 2022) (Wen et al., 2023) (Cai et al., 2020) (Al-Mekhlafi et al., 2024) (Zhang and Cui, 2024) (Jiao et al., 2025).

Post-quantum cryptographic protocols in VANETs primarily fall into two categories: signature and signcryption schemes. The following sections provide an overview of these approaches, highlighting their relevance to VANET security and limitations.

2.1 POST QUANTUM SIGNATURE SCHEMES

In August 2024, the National Institute of Standards and Technology (NIST) announced the effective standardization of several post-quantum cryptographic (PQC) algorithms designed to provide security against threats posed by future quantum computers. Among the standardized there are two distinct digital signature schemes: CRYSTALS-Dilithium, a Module-Lattice-Based Digital Signature Algorithm (ML-DSA), and SPHINCS+, a Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) (Ducas et al., 2018) (Bernstein et al., 2019).

ML-DSA, derived from the CRYSTALS-Dilithium submission, is a digital signature scheme founded on the principles of lattice-based cryptography. Its security is based on the computational difficulty of specific mathematical problems over module lattices, primarily the Module Learning With Errors (MLWE) and Module Short Integer Solution (MSIS) problems. ML-DSA employs the Fiat-Shamir with aborts paradigm, incorporating rejection sampling, to construct secure signatures and achieve relatively compact signature sizes (Kiltz et al., 2018) (Ducas et al., 2018). This design achieves a positive balance between strong security guarantees and computational efficiency across a wide range of platforms.

In contrast, SLH-DSA, based on the SPHINCS+ submission, is a stateless hash-based signature scheme (Bernstein et al., 2019). Its security assurance is derived directly from the well-established security properties of the underlying cryptographic hash functions, such as SHA-256 or SHAKE-256, offering a highly conservative security posture independent of newer mathematical assumptions. SPHINCS + uses an elegant hypertree structure, which is a hierarchy of Merkle trees, built on Winternitz one-time signatures (WOTS +) and Forest of Random Subsets (FORS) few-time signatures (Lamport, 1979) (Hülsing, 2013) (Bernstein et al., 2019). Although exceptionally robust from a security assumption standpoint, SPHINCS+ generally exhibits larger signature sizes and slower operational speeds compared to ML-DSA (Bernstein et al., 2019).

Both ML-DSA and SLH-DSA have rigorous evaluation as part of NIST's multi-year PQC standardization process. They are engineered to provide resilience against cryptanalytic attacks from both classical and quantum computers.

A critical challenge in the adoption of post-quantum signature schemes is the significant latency introduced by their computational complexity, despite their strong security guarantees. This issue is particularly present in VANETs, as their safety-critical functions depend fundamentally on low-latency communication. In response to this, a significant body of research has focused on developing optimizations to enhance the efficiency of these signature schemes.

Early explorations into post-quantum secure communications for VANETs recognized the utility of ring signatures for preserving vehicle anonymity. (Mundhe et al., 2020) proposed a lattice-based ring signature scheme built upon the hardness of the Small Integer Solution (SIS) problem. Their construction is claimed to offer unconditional anonymity where the signer's identity is computationally hidden within a self-selected ring of public keys and unforgeability, with security formally reduced to the SIS assumption. Similarly, (Jiao and Xiang, 2021) presented an anti-quantum ring signature, also founded on the SIS problem, which distinctively incorporates a bimodal Gaussian distribution to refine rejection sampling and an encoding function to map hash outputs to constant-weight binary vectors. These techniques were introduced with the objective of reducing signature size and accelerating cryptographic operations compared to other contemporary schemes.

However, the strong emphasis on unconditional anonymity in these initial lattice-based ring signature schemes presents a significant operational limitation in the VANET context. Neither scheme inherently supports the traceability of malicious messages back to their originators nor provide a mechanism to remove credentials from compromised or misbehaving vehicles. This lack of accountability is highly problematic for safety-critical VANET applications, where the ability to identify and isolate malicious vehicles is essential to maintain integrity and user trust. Furthermore, while Jiao claims efficiency gains and relatively stable signature sizes with increasing security parameters, the reported absolute signature sizes remain substantial. This emphasis on unconditional anonymity, while offering strong privacy guarantees, ultimately conflicts with the practical need for accountability in safety-critical vehicular networks, suggesting that these early schemes may require substantial augmentation or re-design for secure and scalable deployment.

Addressing some of the limitations of earlier proposals, Chen introduced V-LDAA, a vehicular lattice-based Direct Anonymous Attestation (DAA) scheme that leverages a signature mechanism based on automorphism stability and integrates with vehicle Trusted Platform Modules (TPMs) (Chen et al., 2021). A notable contribution of V-LDAA is its distributed pseudonym update and vehicle revocation mechanism. This distributed approach to revocation promises enhanced scalability, mainly as the authors claim that computation costs for V-LDAA's signing and verification operations are independent of the total number of users in the system. V-LDAA is designed to provide user-controlled anonymity and unlinkability, with its security rooted in the presumed hardness of the Ring-Short Integer Solution (Ring-SIS) and Ring-Learning With Errors (Ring-LWE) problems.

Despite these advancements, V-LDAA faces practical implementation challenges, as highlighted by subsequent analysis (Lesaignoux and Carmona, 2024). A fundamental limitation is that its algebraic structure, particularly the choice of modulus q, is incompatible with Number Theoretic Transform (NTT) optimizations. NTT is a crucial algorithm for accelerating the polynomial arithmetic that forms the backbone of many lattice-based schemes, and its absence in V-LDAA inherently restricts performance. Moreover, V-LDAA signatures and credentials remain very large (e.g., the attestation signature component is approximately 406KB), imposing considerable overhead on VANET communication channels. While signing operations can be efficient, verification operations in V-LDAA are reported to be notably slower than signing and can be much slower than pre-quantum schemes.

A significant development towards achieving practical and accountable anonymity is the Lattice-based Revocable Ring Signature (LaRRS), presented as the first of its kind specifically for VANETs (Wen et al., 2023). LaRRS aims to allow a Trusted Authority (TA) to revoke a vehicle's signing privileges, thereby achieving conditional privacy-preserving authentication. This capability directly addresses the critical lack of accountability in earlier, unconditionally anonymous ring signature schemes. LaRRS is notably structured similarly to the NIST standard CRYSTALS-Dilithium, suggesting a cryptographic foundation in module lattice assumptions (e.g., Module-LWE/SIS) and the Fiat-Shamir with Aborts signature paradigm. Although comprehensive construction details of the LaRRS ring signature's revocation mechanism are not exhaustively available in all reviewed materials, related work on a revocable certificateless Public Key Encryption (RCL-PKE) scheme details a KGC-managed binary tree and an associated revocation list (RL) for managing user status (Wen et al., 2025) (Regev, 2009) (Al-Mekhlafi et al., 2024). This RCL-PKE scheme employs TrapGen for trapdoor generation and SampleLeft/ExtRndLeft algorithms for key derivation processes that are intrinsically tied to this tree structure and revocation status.

The principal strength of LaRRS lies in its explicit revocability feature, which enables TA accountability and the conditional privacy essential for VANET operations. Its architectural alignment with a NIST-selected standard like Dilithium is also advantageous, potentially fostering trust and easing implementation based on well-scrutinized primitives. However, the introduction of TA for the revocation function inherently centralizes trust for this critical aspect of the system. The precise cryptographic mechanisms that link the revocation status to the ring signature's anonymity (for non-revoked members) and unforgeability properties, while allowing the TA to trace signers under defined conditions, require robust security proofs and transparent specification. Furthermore, the scalability of managing revocation information (e.g., updates to a revocation list or tree) in a large, dynamic VANET environment remains a practical concern that must be carefully benchmarked against the scheme's claims of high efficiency.

Table **??** summarizes the main important features of each algorithm schema and compares with the proposed work.

2.2 POST QUANTUM SIGNCRYPTION

Signcryption schemes integrate digital signature and encryption processes into a single cryptographic operation (Chatterjee et al., 2020) (Singh and Vijayan, 2011). This approach typically reduces computational overhead and communication costs compared to traditional sign-then-encrypt methods. These efficiencies are particularly relevant for VANETs, where OBUs in vehicles often have limited processing power and memory, and many applications, especially those related to safety, demand low-latency communication to be effective. By providing essential security services like confidentiality, integrity, and authentication more efficiently, signcryption can be a crucial enabler for deploying comprehensive security in VANETs.

While many signcryption schemes aim to provide fundamental security guarantees such as confidentiality, authentication, and unforgeability, the specific context of VANETs calls for a broader spectrum of protections (Al-Mekhlafi et al., 2024) (Yu et al., 2020). Beyond these core properties, VANETs require robust mechanisms for ensuring anonymity, conditional privacy (where identities can be revealed by a trusted authority under specific legitimate circumstances like accidents or malicious behavior), unlinkability of messages, traceability of malicious actors, and efficient revocation of compromised entities (Nath and Choudhury, 2024) (Wen et al., 2025). Addressing these comprehensive requirements is a key focus in the design of modern security schemes for vehicular communication.

(Cai et al., 2020) proposed a ring-based signcryption scheme for VANETs aimed at conditional privacy, leveraging identity-based cryptosystems and ring signatures to provide anonymity within a group. However, this scheme was built using classical cryptographic methods,

Feature	CRYSTALS-Dilithium	SPHINCS+	Mundhe	Jiao	V-LDAA	LaRRS	SILMARILLI
Post-Quantum Security	✓	✓	✓	✓	✓	✓	✓
Based on NIST PQC Standard	✓	✓	x	x	x	✓	✓
Ring Signature Structure	x	x	✓	✓	x	✓	✓
Anonymity	x	x	✓	✓	✓	✓	✓
Traceability	x	x	x	x	✓	✓	✓
Revocability	x	x	x	x	✓	✓	✓
Integrated Confidentiality	x	x	x	x	x	x	✓

Table 2.1: Feature Comparison of Post-Quantum Signature Schemes for VANETs

making it vulnerable to attacks from quantum computers and thus unsuitable for ensuring long-term security in VANETs. Furthermore, a noted limitation of this approach is that it only supports one-to-one communication, which is restrictive for many VANET scenarios that rely on broadcast messages for safety and traffic information dissemination.

To improve efficiency and adaptability in the post-quantum era, researchers have explored various approaches. (Al-Mekhlafi et al., 2024) proposed a lattice-based anonymous authentication scheme for 5G-assisted vehicular communications that integrates fog computing servers. This architecture leverages 5G connectivity to offload computationally intensive tasks from vehicles to fog servers, aiming to reduce processing costs on OBUs and providing security features such as quantum attack resistance, anonymous authentication, identity privacy, message authentication, unlinkability, and conditional traceability. However, this reliance on fog infrastructure introduces a trade-off, as it can lead to higher transmission costs and create dependencies on the availability and security of the fog servers themselves.

(Zhang and Cui, 2024) introduced a lattice-based chameleon signcryption scheme (LBCSC) designed to provide quantum resistance while incorporating advanced privacy features such as signature non-transferability and signer rejectability. These chameleon properties are particularly valuable as they address potential signature misuse in sensitive VANET applications by allowing only the designated recipient to verify the signature for a specific message, thus preventing them from proving the signature's validity to a third party without revealing their own secret information. The scheme's security, encompassing confidentiality, integrity, and authenticity, is proven in the Standard Model based on the Learning With Errors (LWE) and Small Integer Solution (SIS) problems. While offering robust security and nuanced privacy controls, the practical overheads of implementing these sophisticated chameleon features in resource-constrained VANET devices, along with the inherent complexity of such mechanisms, require careful evaluation for widespread deployment.

More recently, (Jiao et al., 2025) developed an efficient lattice-based heterogeneous signcryption scheme (LHS-C2I), which enables secure communication between entities using different cryptographic frameworks—such as Certificateless Cryptography and Identity-Based Cryptography—an essential feature for interoperability in heterogeneous VANET ecosystems. The scheme adopts an offline/online architecture to minimize computational burden during real-time operations by shifting resource-intensive computations to the offline phase. It is proven to achieve confidentiality (IND-CCA2) and unforgeability (EUF-CMA) under the random oracle model. Although it demonstrates lower computational and communication overhead compared to existing schemes, its reliance on the random oracle model represents a weaker security guarantee than proofs in the Standard Model. Furthermore, the practical challenges of coordinating secure communication across diverse cryptographic domains, as well as the need for empirical validation at scale in dynamic VANET environments, remain open concerns.

Table **??** summarizes the main important features of each algorithm schema and compares with the proposed work.

Feature	**Cai**	**Al-Mekhlafi**	**LBCSC**	**LHS-C2I**	**SILMARILLI**
Post-Quantum Security	x	✓	✓	✓	✓
Confidentiality (IND-CCA2)	x	x	✓	✓	✓
Unforgeability (SUF-CMA)	x	x	✓	✓	✓
Ring-Based Architecture	✓	x	x	x	✓
Conditional Privacy (Anon. + Traceability)	✓	✓	x	x	✓
Explicit Revocation Mechanism	x	x	x	x	✓
Designed for VANET Broadcast	x*	x**	✓	✓	✓

*Supports only one-to-one communication.

**Relies on fog computing infrastructure, introducing external dependencies.

Table 2.2: Feature Comparison of Post-Quantum Signcryption Schemes for VANETs

3 BACKGROUND

his chapter outlines the algebraic and lattice-based foundations of post-quantum cryptography, focusing on structures and problems that support its security. It also presents core algorithms supporting encryption and key management, forming the basis for secure VANET protocols.

3.1 MATHEMATICAL DEFINITION

This section aims to describe the abstract algebraic basis, which will lead to secure construction later used to build the cryptographic schema.

Definition 3.1.1 (Ring) *A ring is a set $\mathcal{R}$ equipped with two operations, which we denote by $(+)$ and $(\cdot)$, that satisfy the following properties:*

With respect to addition, there must exist an additive identity element $0 \in \mathcal{R}$ such that $0 + a = a + 0 = a, \forall a \in \mathcal{R}$. For each element $a \in \mathcal{R}$, there must exist an additive inverse $b \in \mathcal{R}$ such that $a + b = b + a = 0$. Addition must also be associative, meaning $a + (b + c) = (a + b) + c, \forall a, b, c \in \mathcal{R}$, and commutative, meaning $a + b = b + a, \forall a, b \in \mathcal{R}$.

With respect to multiplication, there must exist a multiplicative identity element $1 \in \mathcal{R}$ such that $1 \cdot a = a \cdot 1 = a, \forall a \in \mathcal{R}$. Multiplication must be associative, so that $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall a, b, c \in \mathcal{R}$, and commutative, so that $a \cdot b = b \cdot a, \forall a, b \in \mathcal{R}$. Finally, the two operations are linked by the distributive law, which states that $a \cdot (b + c) = (a \cdot b) + (a \cdot c), \forall a, b, c \in \mathcal{R}$.

Definition 3.1.2 (Quotient Ring) *Let $\mathcal{R}$ be a ring and let $m \in \mathcal{R}$ with $m \neq 0$. For any $a \in \mathcal{R}$, we write a for the set of all $a' \in \mathcal{R}$ such that $a' \equiv a \pmod{m}$. The set a is called the congruence class of a, and we denote the collection of all congruence classes by $\mathcal{R}/(m)$ or $\mathcal{R}/m\mathcal{R}$. Thus,*

$$R/(m) = R/mR = \{\overline{a} : a \in R\}. \tag{3.1}$$

We call $\mathcal{R}/(m)$ the quotient ring of $\mathcal{R}$ by m.

Definition 3.1.3 (Polynomial Quotient Ring) *Let $\mathcal{R}$ be a commutative ring with unity, and let $f(x) \in \mathcal{R}[x]$ be a nonzero polynomial of degree d. Consider the principal ideal $\langle f(x) \rangle \subseteq \mathcal{R}[x]$, consisting of all multiples of $f(x)$. For each $g(x) \in \mathcal{R}[x]$, denote by*

$$\overline{g(x)} = g(x) + \langle f(x) \rangle \tag{3.2}$$

the congruence class (coset) of $g(x)$ modulo $\langle f(x) \rangle$. The set

$$\mathcal{R}[x]/\big(f(x)\big) \;=\; \big\{\, \overline{g(x)} : g(x) \in \mathcal{R}[x] \big\} \tag{3.3}$$

equipped with the operations

$$\overline{g(x)} + \overline{h(x)} = \overline{g(x) + h(x)}, \qquad \overline{g(x)} \cdot \overline{h(x)} = \overline{g(x)\, h(x)}, \tag{3.4}$$

is called the polynomial quotient ring *of $\mathcal{R}[x]$ by $f(x)$.*

Key Properties

Well-Definedness Addition and multiplication on cosets are well-defined because $\langle f(x) \rangle$ is an ideal in $\mathcal{R}[x]$.

Ring Structure $\mathcal{R}[x]/(f(x))$ inherits a commutative ring with unity from $\mathcal{R}[x]$; the coset of 1 serves as the multiplicative identity.

Canonical Representatives Every class $\overline{g(x)}$ contains a unique representative polynomial of degree $< d = \deg(f)$, obtained by Euclidean division by $f(x)$.

Vector-Space Structure (if $\mathcal{R}$ is a field) When $\mathcal{R} = F$ is a field, $F[x]/(f)$ is an F-vector space of dimension d.

Field Criterion If $\mathcal{R} = F$ is a field, then $F[x]/(f)$ is itself a field exactly when $f(x)$ is irreducible over F.

3.2 LATTICE

Lattice is an algebraic structure, defined as a set of periodic points in an n-dimensional space. Lattices are formally defined as:

Definition 3.2.1 (Lattice) *Let* $\mathbf{X} = \begin{pmatrix} \mathbf{x_1}, & \mathbf{x_2}, & \cdots, & \mathbf{x_m} \end{pmatrix} \in \mathbb{Z}_q^{nxm}$*, be a matrix of m linearly independent vectors over the ring of integers, then a* **X***-based lattice* $\Lambda(\mathbf{X})$ *is defined as the set consisting of the linear combinations of the integer coefficients of the set of vector* **X***, that is:*

$$\Lambda(\mathbf{X}) = \left\{ \sum_{i=1}^{m} z_i \cdot \mathbf{x}_i : z_i \in \mathbb{Z} \right\} \tag{3.5}$$

Definition 3.2.2 (q-ary Lattice) *Given a prime number q and a vector* $\eta \in Z_q^n$ *the definition of two types of q-ary lattices are:*

$$\Lambda_q^{\perp}(\mathbf{X}) = \{e \in \mathbb{Z}^m \mid \mathbf{X}e \equiv 0 \pmod{q}\} \tag{3.6}$$

$$\Lambda_q^{\eta}(\mathbf{X}) = \{e \in \mathbb{Z}^m \mid \mathbf{X}e \equiv \eta \pmod{q}\} \tag{3.7}$$

Definition 3.2.3 (Discrete Gaussian Distribution) *Giving* $\mathbf{c} \in \mathbb{R}^m$ *and* $\mathbf{s} \in \mathbb{R}^+$*, where* $m \in \mathbb{Z}$*, a Discrete Gaussian Distribution is defined on a lattice* Λ *centred on in* **y** *with parameters* δ

$$\forall x \in \Lambda, D_{\Lambda,\delta,y} = \frac{\rho_{\delta,y}(x)}{\rho_{\delta,y}(\Lambda)} \tag{3.8}$$

where,

$$\rho_{\delta,y}(x) = \exp\left(-\pi \frac{\|x-y\|^2}{\delta^2}\right) \tag{3.9}$$

3.2.1 Lattices Problems

Definition 3.2.4 (Small Integer Solution Problem, SIS) *Given a prime number q, a matrix* $\mathbf{X} \in \mathbb{Z}_q^{nxm}$ *and a real number* γ*, the problem is to find a non-zero vector* $\mathbf{e} \in \mathbb{Z}^m$*, such that:*

$$\mathbf{X}e \equiv 0 \pmod{q}, 0 < \|e\| \leq \gamma \tag{3.10}$$

Definition 3.2.5 (Learning with Errors Problem, LWE) *Given an integer q, an error distribution χ over a ring $\mathbb{Z}$ (formally defined as $\mathbb{Z}[X]/(f(X))$), the problem is to solve the hidden secret vector $\mathbf{s} \in \mathbb{Z}_q^n$ in*

$$\mathbf{b} = \mathbf{A}^T\mathbf{s} + e \pmod{q} \in \mathbb{Z}^m \tag{3.11}$$

Where $\mathbf{A} \in \mathbb{Z}_q^{nxm}$ and $\mathbf{e} \in \chi$.

3.2.2 Lattices Algorithms

Lattice Trapdoor generation algorithm TrapGen() introduced by (Ajtai, 1996) is defined as follows:

Definition 3.2.6 (Trapdoor) *Given an integer n, a prime $q \geq 3$, and an integer $m \geq 5n \log q$ the algorithm outputs a uniformly distributed matrix $\mathbf{X} \in \mathbb{Z}_q^{nxm}$, a short basis $\mathbf{T}$ for the lattice $\Lambda(\mathbf{X})$ in polynomial time.*

The preimage sampling algorithm SamplePre() introduced by (Gentry et al., 2008) is defined as follows:

Definition 3.2.7 (Preimage Sample) *Input a matrix $\mathbf{X}$ and the short basis $\mathbf{T}$ output by the trapdoor generation algorithm TrapGen(), a security parameter $r \geq \|T\|\omega(\sqrt{\log n})$, and a vector $\mathbf{u} \in \mathbb{Z}_q^n$ uniformly distributed, the algorithm outputs a random vector $\mathbf{e} \in \mathbb{Z}_q^{nxk}$ that follows a Gaussian distribution $D^m_{\Lambda_q^\eta(\mathbf{X}),r}$ in polynomial time, where $\mathbf{Ae} = \mathbf{u} \mod q$*

3.3 HARDNESS DEFINITION

This section aims to define the hardness of solve algorithms SIS and LWE. In his work Ajtai describes the hardness of both problems as follows (Ajtai, 1996):

3.3.1 Small Integer Solution Problem hardness

For any $m = poly(n)$, any $\gamma > 0$, and any sufficiently large $q \geq \gamma * poly(n)$, solving SIS is at least as hard as solving Shortest Vector Problem (SVP) on worst-case n-dimensional lattices with high probability for some approximation factor $\gamma * poly(n)$.

3.3.2 Learning with Errors Problem hardness

For any $m = poly(n)$, any $q \leq 2 * poly(n)$, and any discretized gaussian distribution χ with variance $\alpha q \geq 2\sqrt{n}$, solving the LWE problem is at least as hard as solving Shortest Vector Problem (SVP) on worst-case n-dimensional lattices with high probability for some approximation factor $\frac{n}{\alpha}$.

As presented by Emde Boas and later complemented by Ajtai for the lattice cases, the problem Shortest Vector Problem (SVP) is a NP-complete problem, therefore there is no possible polynomial solution for the given problem. (van Emde Boas, 1981) (Ajtai, 1998)

4 SILMARILLI

This chapter presents the full specification of the proposed cryptographic schema for secure and accountable communication in VANETs. It introduces the core algorithmic framework, outlines the security properties achieved, defines the protocol parameters, and provides formal proofs based on standard cryptographic assumptions.

4.1 CRYPTOGRAPHIC SCHEMA

The Silmarilli cryptographic schema is defined via the following phases: MasterKeyGen, KeyGen, SignCrypt, verifyDecript, Trace, Revoke. The following subsection are responsible to describe in details the functionality of each phase and present its respective algorithm.

All parameters used in the algorithms are listed in Table 4.1

Parameter	**Description**
q	Modulo of $R_q = \mathbb{Z}_q[x]/(x^d+1)$.
d	Degree of $R_q = \mathbb{Z}_q[x]/(x^d+1)$.
$\mathbf{X}$	A matrix $\mathbf{X} \leftarrow R_q^{n\times m}$ in NTT representation. (Liang and Zhao, 2022)
n	The rows of $\mathbf{X}$.
m	The columns of $\mathbf{X}$.
T	The time stamp.
n	The number of public keys in the Signing Ring.
L	The set of ring members' public keys, $L = \{\mathbf{pk}_1, \cdots, \mathbf{pk}_n\}$.
μ	The message to be signed.
$\mathbf{H}, D$	Same as in Dilithium definition, $\mathbf{H} : \{0,1\}^* \to D$. $\mathbf{H}$ is a hash function in the family of SHAKE algorithms, where $D = \{d \in R_q \mid \|d\|_\infty \le 1, \|d\|_1 \le \kappa\}$.
κ	In challenge set D of Hash function $\mathbf{H}$.
S_η, η	S_η includes all $f \in R = \mathbb{Z}[x]/(x^d+1)$, s.t. $\|f\|_\infty \le \eta$.
γ	r_i, t_i coefficient range.

Table 4.1: Description of parameters

4.1.1 MasterKeyGen

MasterKeyGen is an offline initialization phase executed by TA, in which a master key pair (pk, sk) is generated using modified version of CRYTALS key generation algorithm. In addition to the key pair, the TA derives and publishes system-wide public parameters $\mathbf{X}$, which serve as the foundational inputs for all subsequent cryptographic operations. These parameters are chosen to ensure the hardness assumptions.

The MasterKeyGen operation performed as follows:

1. **Seed Generation:** A uniformly random 256-bit seed ζ is sampled from $\{0,1\}^{256}$ to serve as the entropy source.

2. **Hash Expansion:** The seed ζ is processed using a cryptographic hash function $\mathbf{H}(\cdot)$ to derive three values, (ρ, ρ', K), where ρ is used for matrix expansion, ρ' for secret vector sampling, and K is an auxiliary secret key.

3. **Matrix Generation:** The public matrix $\mathbf{X} \in \mathbb{R}_q^{n\times m}$ is deterministically generated using the seed ρ via $\text{ExpandA}(\rho)$. This matrix is shared by all entities in the system.

4. **Secret Vectors Sampling:** Two secret vectors $\mathbf{s}_1 \in S_\eta^m$ and $\mathbf{s}_2 \in S_\eta^n$ are sampled using ρ' through the function $\text{ExpandS}(\rho')$.

5. **Public Value Computation:** The intermediate public vector $\mathbf{t}$ is computed.

6. **Rounding Step:** The vector $\mathbf{t}$ is decomposed into a coarse and a fine component using the rounding function Power2Round_q.

7. **Key Output:** The public key and secret key are assembled.

A pseudocode visualization of the described algorithm is defined as:

Algorithm 1 $Power2Round_q(r, d)$

```
$r \leftarrow r \bmod {}^{+}q$
$r_0 \leftarrow r \bmod {}^{\pm}2^d$
**return** $\left(\frac{r-r_0}{2^d}, r_0\right)$
```

Algorithm 2 MasterKeyGen

```
$\zeta \xleftarrow{\$} \{0,1\}^{256}$
$(\rho, \rho', K) \in \{0,1\}^{256} \times \{0,1\}^{512} \times \{0,1\}^{256} \leftarrow \mathbf{H}(\zeta)$
$\mathbf{X} \in \mathbb{R}_q^{n\times m} \leftarrow \text{ExpandA}(\rho)$
$(\mathbf{s}_1, \mathbf{s}_2) \in S_\eta^m \times S_\eta^n \leftarrow \text{ExpandS}(\rho')$
$\mathbf{t} \leftarrow \mathbf{X} \cdot \mathbf{s}_1 + \mathbf{s}_2$
$(\mathbf{t}_1, \mathbf{t}_0) \leftarrow \text{Power2Round}_q(\mathbf{t}, d)$
$pk \leftarrow (\rho, \mathbf{t}_1)$
$sk \leftarrow (\rho, K, \mathbf{s}_1, \mathbf{s}_2, \mathbf{t}_0)$
**return** (pk,sk)
```

4.1.2 KeyGen

KeyGen is an offline phase during which each vehicle, using the public parameters established in the MasterKeyGen stage, generates a unique public–private key pair. This procedure ensures that every vehicle possesses a verifiable cryptographic identity. Prior to joining the ring, each vehicle's public key is authenticated and certified by the TA, preventing unauthorized participation and preserving the integrity of the ring-based communication protocol.

The KeyGen operation performed similarly to the MasterKeyGen operation, with the additional step of ID derivation, describe as follows:

1. **Identity Derivation:** A vehicle-specific identity id_i is generated.

A pseudocode visualization of the described algorithm is defined as:

Algorithm 3 KeyGen(**X**)

```
$\zeta \xleftarrow{\$} \{0,1\}^{256}$
$(\rho, \rho', K) \in \{0,1\}^{256} \times \{0,1\}^{512} \times \{0,1\}^{256} \leftarrow \mathbf{H}(\zeta)$
$(\mathbf{s}_1, \mathbf{s}_2) \in S_\eta^m \times S_\eta^n \leftarrow \text{ExpandS}(\rho')$
$\mathbf{t} \leftarrow \mathbf{X} \cdot \mathbf{s}_1 + \mathbf{s}_2$
$(\mathbf{t}_1, \mathbf{t}_0) \leftarrow \text{Power2Round}_q(\mathbf{t}, d)$
$id_i \in \{0,1\}^{256} \leftarrow \mathbf{H}(\rho \parallel \mathbf{t}_1)$
$pk \leftarrow (t_1, id_i)$
$sk \leftarrow (\rho, K, \mathbf{s}_1, \mathbf{s}_2, \mathbf{t}_0)$
return (pk,sk)
```

4.1.3 SignCrypt

SignCrypt phase allows a vehicle π to transmit a confidential and authenticated message μ to all members of the ring. Using a combined signcryption primitive, which integrates signature and encryption functionalities into a single logical step, the vehicle generates a ciphertext that simultaneously ensures confidentiality, integrity, and authenticity. The signcryption scheme is assumed to satisfy standard IND-CCA2 and SUF-CMA security notions, offering robustness against quantum adversaries as well as adaptive chosen-ciphertext and existential forgery attacks within the vehicular network.

The SignCrypt operation performed as follows:

1. **Ephemeral Sampling:**
   - A short ephemeral vector $\mathbf{s} \in \mathbb{S}_\eta^n$ is sampled and two noise terms $(\mathbf{e}_1, \mathbf{e}_2) \in \mathbb{S}_\eta^m \times \mathbb{S}_\eta$ are also sampled.
2. **Commitment Computation:** Generates a cryptographic commitment $\mathbf{C}_\pi$to the message originator π, embedding their identity in a way that supports traceability.
3. **Auxiliary Masking Vectors:** Vectors $\mathbf{u} \in \mathbb{S}_{\gamma-1}^{m+n}$ and $\mathbf{w} \in \mathbb{S}_{\gamma-1}^n$ are sampled for signature masking.
4. **Hash Challenge Initialization:** A challenge value $e_{\pi+1}$ is computed using a hash function H, applied over T, L, μ, and auxiliary commitments.
5. **Ring Iteration:** For each member i in the ring (excluding π), the signer simulates their part of the ring as follows:
   - Sample $\mathbf{r}_i$, $\mathbf{y}_i$, and $\mathbf{v}_i$ from appropriate short distributions.
   - Compute a masking factor $\phi_i = e_i \cdot v_i$.
   - Generate intermediate commitments α_i, Ω_i, and δ_i incorporating ring values and commitments.
   - Derive the next challenge hash $e_{i+1} = \mathsf{H}'(\cdots)$.
6. **Real Signer Completion:** For index π, compute the signature values.
7. **Signature Construction:** The final signature σ includes all commitments, ring indices, and challenge data.

8. **Message Encryption:** The message μ is encrypted using Kyber.CCA.KEM.
9. **Authentication Tag:** A message authentication tag ψ is computed.
10. **Output:** The algorithm returns the tuple (σ, c, K, ψ), which can be broadcast in the VANET for secure and anonymous communication.

    A pseudocode visualization of the described algorithm is defined as:

Algorithm 4 SignCrypt(T, L, μ, X)

```
$\mathbf{s} \xleftarrow{\$} \mathbb{S}_\eta^n$
$(\mathbf{e_1}, \mathbf{e_2}) \xleftarrow{\$} \mathbb{S}_\eta^m \times S_\eta$
$\mathbf{C}_\pi \leftarrow (\mathbf{C}_1, \mathbf{C}_2) \leftarrow \left(\mathbf{X}^T\mathbf{s} + \mathbf{e_1}, \tilde{\mathbf{t_1}}^T \cdot \mathbf{s} + \mathbf{e_2} + \lfloor \frac{q}{2} \rfloor \cdot id_\pi\right)$
$\mathbf{u} \xleftarrow{\$} \mathbb{S}_{\gamma-1}^{m+n}$
$\mathbf{w} \xleftarrow{\$} \mathbb{S}_{\gamma-1}^{n}$
$e_{\pi+1} = \mathsf{H}(T, L, \mu, \bar{X}\mathbf{u}, X^T\mathbf{w}, \tilde{\mathbf{t_1}}^T \cdot \mathbf{w})$
for all $i = \pi + 1 ... \pi - 1$ do
    $\mathbf{r_i} \xleftarrow{\$} \mathbb{S}_{\gamma-1}^{m+n}$
    $\mathbf{y_i} \xleftarrow{\$} \mathbb{S}_{\gamma-1}^{n}$
    $\mathbf{v_i} \xleftarrow{\$} \mathbb{S}_\eta$
    $\phi_\mathbf{i} \leftarrow e_i * v_i$
    $\alpha_i \leftarrow \bar{\mathbf{X}} r_i - e_i \cdot \mathbf{t}_i$
    $\Omega_i \leftarrow \mathbf{X}^T y_i + \epsilon \cdot \phi_i - e_i \cdot \mathbf{C}_1$
    $\delta_i \leftarrow \tilde{\mathbf{y}}^T \cdot y_i + \phi_i - e_i \cdot \left(\mathbf{C}_2 - \lceil \frac{q}{2} \rceil \cdot id_i\right)$
    $e_{i+1} = \mathsf{H}'(T, L, \mu, \alpha_i, \Omega_i, \delta_i)$
end for
$\mathbf{r}_\pi \leftarrow \mathbf{u} + e_\pi \cdot \begin{bmatrix} \mathbf{s_1}_\pi \\ \mathbf{s_2}_\pi \end{bmatrix}$
$\mathbf{y}_\pi \leftarrow \mathbf{w} + e_\pi \cdot \mathbf{s}$
$\phi_\pi \leftarrow e_\pi \cdot e_2$
$\sigma \leftarrow (T, e_1, \mathbf{r}_1, t_1, \rho_1, \ldots, \mathbf{r}_n, t_n, \rho_n, \epsilon, \mathbf{C}_\pi)$
$(c, K) \leftarrow Kyber.CCAKEM.Enc(pk_{\pi+1}, \mu)$
$\psi \leftarrow H_2(\mu, \sigma)$
return $(\sigma$, c, K, $\psi$ )
```

4.1.4 verifyDecript

Upon receiving a ciphertext, the verifyDecript phase performs the inverse operation of signcryption, jointly executing verification and decryption. If the output fails the signature verification or decryption validity check, indicating possible tampering or forgery, a secure reporting mechanism is triggered, notifying the TA to initiate the Trace and Revoke procedures.

After successful signature verification, each vehicle in the ring encrypts the message for the next designated vehicle. This encryption step employs the same algorithm as used in the SignCrypt phase: Kyber.CCAKEM.Enc.

The verifyDecript operation performed as follows:

1. **Message Decryption:** The ciphertext c is decrypted using the recipient's secret key sk via Kyber's CCA-secure KEM.

2. **Tag Recalculation:** A fresh tag ψ' is recomputed using the decrypted message and the received signature.

3. **Authentication Check:** If $\psi' \neq \psi$, the message is rejected as unauthentic or tampered.

4. **Commitment Extraction:** The commitment components $\mathbf{C}_1$ and $\mathbf{C}_2$ are extracted from the ring member π's signature.

5. **Challenge Regeneration Loop:** For all ring members $i = 1, \ldots, n-1$, the verifier recomputes the sequence of challenge hashes.

6. **Final Challenge Check:** The final hash value e'_1 is computed from the last ring member $i = n$, completing the ring.

7. **Final Verification:** The verifier checks whether the ring challenge cycles correctly by verifying if $e_1 = e'_1$. If so, the signcryption is accepted; otherwise, it is rejected.

A pseudocode visualization of the described algorithm is defined as:

Algorithm 5 verifyDecript(σ, c, K, ψ, X)

```
$\mu' \leftarrow Kyber.CCAKEM.Dec(c, sk)$
$\psi' \leftarrow H_2(\mu', \sigma)$
**if** $\psi' \neq \psi$ **then**
    **return** reject
**end if**
$(\mathbf{C}_1, \mathbf{C}_2) \leftarrow \mathbf{C}_\pi$
**for all** $i = 1 \ldots n-1$ **do**
    $e_{i+1} \leftarrow \mathcal{H}(T, L, \mu', \overline{X} r_i - e_i \cdot \tilde{t_1}_i, \quad X^T y_i + \epsilon \cdot \phi_i - e_i \cdot \mathbf{C_1}, \quad \tilde{t_1}^T \cdot y_i + \phi_i - e_i \cdot (\mathbf{C_2} - \lfloor q/2 \rfloor \cdot id_i))$.
**end for**
$e'_1 \leftarrow \mathcal{H}(T, L, \mu', \overline{X} r_n - e_n \cdot \tilde{t_1}_n, \quad X^T y_n + \epsilon \cdot \phi_n - e_n \cdot \mathbf{C_1}, \quad \tilde{t_1}^T \cdot y_n + \phi_n - e_n \cdot (\mathbf{C_2} - \lfloor q/2 \rfloor \cdot id_n))$.
**if** $e_1 = e'_1$ **then**
    **return** accept
**end if**
**return** reject
```

4.1.5 Trace

The Trace phase is an accountability mechanism exclusively executed by the TA. It employs embedded tracing components within the ring signature scheme to deterministically reveal the true identity of the message originator. This functionality enables non-repudiation and supports misbehavior attribution, while preserving the anonymity of compliant participants.

The Trace operation performed as follows:

1. **Validity check:** The algorithm verifies if the message μ is a valid message.

2. **Identity Test:** If the message is not valid TA computesid_π from the message TAG

3. **Return Trace:** the algorithm returns id_π as the source of the message.

A pseudocode visualization of the described algorithm is defined as:

Algorithm 6 Trace($\mathbf{C}_\pi$)

```
if $\mu$ is not valid then
    $(\mathbf{C}_1, \mathbf{C}_2) \leftarrow \mathbf{C}_\pi$
    $id_\pi \leftarrow \mathbf{C}_2 - s_1^T \cdot \mathbf{C_1}$
    return $id_\pi$
end if
return $\perp$
```

4.1.6 Revoke

The Revoke phase enforces dynamic membership control in response to confirmed misbehavior. Upon identification of a malicious vehicle through the Trace mechanism, the TA invalidates its cryptographic credentials, thereby excluding it from future protocol participation. This process is essential for preserving the cryptographic integrity and overall trust framework of the vehicular network.

The Revoke operation performed as follows:

1. **Non-null Check:** The algorithm first verifies that the input identity is not null or undefined. This prevents unintended deletions or logic errors.

2. **Membership Check:** If the identity is valid, the algorithm checks whether $id \in L$.

3. **Revocation:** If both checks pass, the identity is removed from the list. This ensures that the revoked identity can no longer participate in any authenticated VANET operations, such as signcryption or verification.

A pseudocode visualization of the described algorithm is defined as:

Algorithm 7 Revoke(id, L)

```
if $id \neq \perp$ then
    if $id \in L$ then
        $L \leftarrow L - id$
    end if
end if
```

4.1.7 Silmarilli diagram representation

The following diagram illustrates the expected operation of Silmarilli:

4.2 SILMARILLI SECURITY GUARANTEES

The proposed scheme satisfies the following security properties, each critical to the reliability and robustness of VANET communication systems:

4.2.1 Authenticity

The scheme guarantees message authenticity by enabling the recipient to verify both the integrity of the message and the legitimacy of the sender. This ensures that the message has not been altered during transmission and that the sender is a certified vehicle entity within the system (Katz and Lindell, 2007).

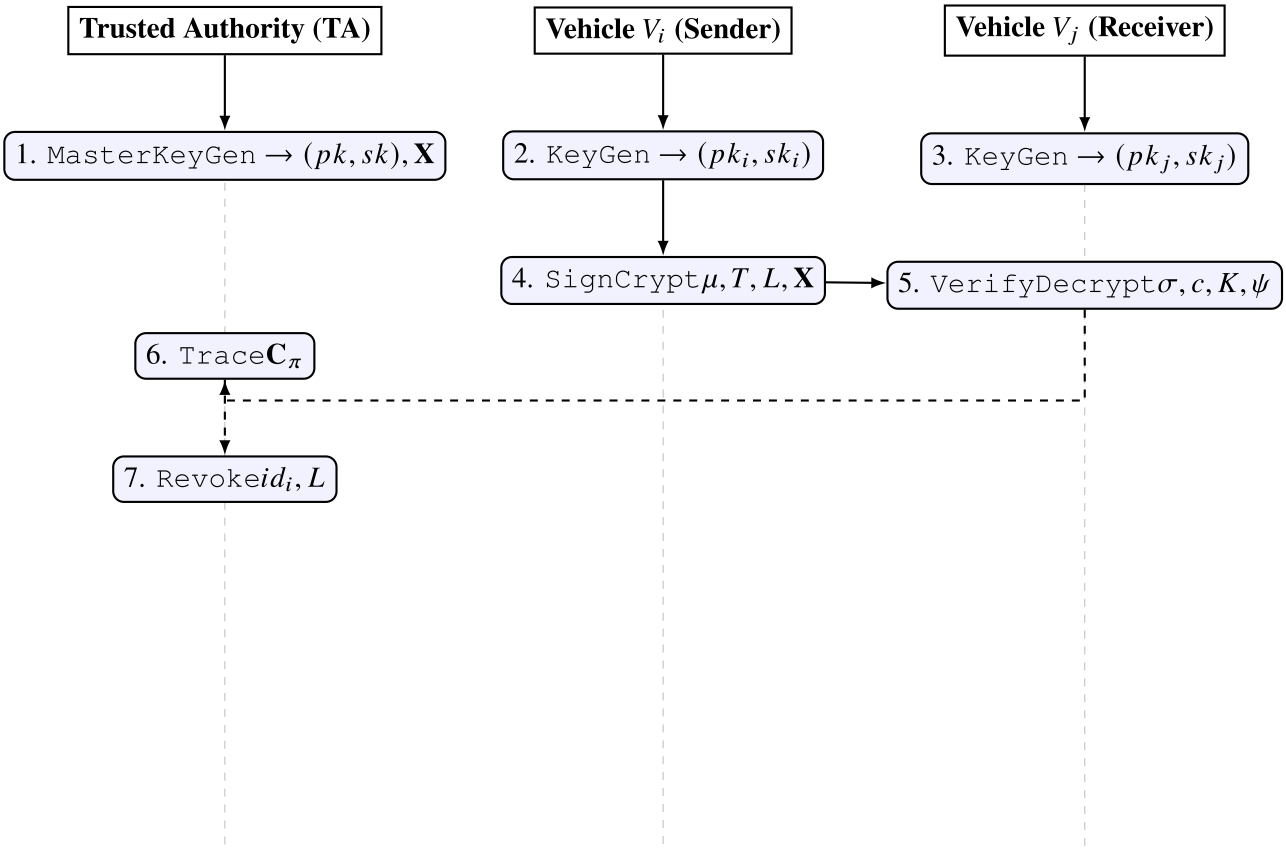

Trusted Authority (TA)
Vehicle V_i (Sender)
Vehicle V_j (Receiver)
1. MasterKeyGen → $(pk, sk), \mathbf{X}$
2. KeyGen → (pk_i, sk_i)
3. KeyGen → (pk_j, sk_j)
4. SignCrypt$\mu, T, L, \mathbf{X}$
5. VerifyDecryptσ, c, K, ψ
6. Trace$\mathbf{C}_\pi$
7. Revokeid_i, L

Figure 4.1: SILLMARILLI communication diagram

Theorem 4.2.1 (Authenticity) *Let H_2 be a collision-resistant one-way hash function. Given a message μ and its signature σ and its generated hash ψ, any changes applied to the message would result in a different hash result, causing the message to be rejected during the **verifyDecript** phase.*

4.2.2 Confidentiality (IND-CCA2)

An adversary cannot gain any partial information about the plaintext from the ciphertext, even with the ability to decrypt other ciphertexts. The confidentiality of the encrypted messages is preserved, making the ciphertext indistinguishable from random data (Katz and Lindell, 2007) (Ferguson et al., 2011).

Theorem 4.2.2 (IND-CCA2 security) *Suppose XOF, H, and G are random oracles. For any classical adversary A that makes at most q_{RO} many queries to random oracles, H and G, there exist adversaries B and C of roughly the same running time as that of A such that:*

$$Adv^{CCA2}_{Kyber}(A) \leq 2Adv^{MLWE}_{n,m,\chi}(B) + Adv^{\mathrm{PRF}}_{prf}(C) \tag{4.1}$$

4.2.3 Strong Unforgeability (SUF-CMA)

An adversary cannot fabricate a valid signcryption ciphertext for any message, regardless of whether the message is new or has been previously signcrypted. An adversary cannot manipulate or alter existing signcryption ciphertexts to produce new, valid ciphertexts for the same messages (Bellare and Namprempre, 2008) (Cremers et al., 2024).

Theorem 4.2.3 (Authenticity) *This proof is based on the CRYSTALS-Dilithium proof, where it is proven that the Dilithium algorithm is SUF-CMA under classical random oracle model attacks, given the hardness to break LWE and SIS problems in a Modular Ring (MLWE and MSIS), and a new introduced problem, SelfTargetMSIS, based on the combined hardness of MSIS and the hash function H (Ducas et al., 2018) (Abdalla et al., 2012) (Alkim et al., 2017).*

The assumptions are defined as follows:

Definition 4.2.4 (The MLWE Problem) *For integers n, m, and a probability distribution $\chi : (R_q) \rightarrow [0, 1]$, we say that the advantage of algorithm A in solving the $MLWE_{n,m,\chi}$ problem over the ring $\mathbb{R}_{\shortparallel}$ is:*

$$\begin{aligned} Adv^{MLWE}_{n,m,\chi} := \big|\Pr[b = 1 \mid \mathbf{X} \leftarrow \mathbb{R}_q^{n\times m}, \mathbf{t} \leftarrow \mathbb{R}_q^n, b \leftarrow \mathcal{A}(\mathbf{X}, \mathbf{t})] \\ - \Pr[b = 1 \mid \mathbf{X} \leftarrow \mathbb{R}_q^{n\times m}, \mathbf{s}_1 \leftarrow D^n, \mathbf{s}_2 \leftarrow D^m, b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{A} \cdot \mathbf{s}_1 + \mathbf{s}_2)]\big|. \end{aligned} \tag{4.2}$$

Definition 4.2.5 (The MSIS Problem) *The MSIS Problem. To an algorithm $\mathcal{A}$ we associate the advantage function $Adv^{MSIS}_{n,m,\gamma}$ to solve the $MSIS_{m,k,\gamma}$ problem over the ring $\mathbb{R}_{\shortparallel}$ as:*

$$Adv^{\text{MSIS}}_{n,m,\gamma}(\mathcal{A}) := \Pr\left[0 < \|\mathbf{y}\|_\infty \leq \gamma \wedge [\mathbf{I} \mid \mathbf{X}] \cdot \mathbf{y} = \mathbf{0} \,\middle|\, \mathbf{X} \leftarrow R_q^{n\times m};\ \mathbf{y} \leftarrow \mathcal{A}(\mathbf{X})\right]. \tag{4.3}$$

Definition 4.2.6 (The SelfTargetMSIS Problem) *Suppose that $H : \{0, 1\}^* \rightarrow B_{60}$ is a cryptographic hash function. To an algorithm A we associate the advantage function:*

$$\begin{aligned} Adv^{\text{SelfTargetMSIS}}_{\mathsf{H},n,m,\gamma}(\mathcal{A}) := \Pr\Big[\ 0 \leq \|\mathbf{y}\|_\infty \leq \gamma \wedge \mathsf{H}([\mathbf{I} \mid \mathbf{X}] \cdot \mathbf{y} \parallel M) = c\ \ \Big| \\ \mathbf{X} \leftarrow R_q^{n\times m};\ \left(\mathbf{y} := \begin{bmatrix}\mathbf{r} \\ c\end{bmatrix}, M\right) \leftarrow \mathcal{A}^{\mathsf{H}(\cdot)}(\mathbf{X}) \end{aligned} \tag{4.4}$$

Therefore, the advantage of an adversary A breaking the SUF-CMA security of the signature scheme is:

$$Adv^{SUF\text{-}CMA}_{Dilithium} \leq Adv^{MLWE}_{n,m,\chi} + Adv^{\text{MSIS}}_{n,m,\gamma}(\mathcal{A}) + Adv^{\text{SelfTargetMSIS}}_{\mathsf{H},n,m,\gamma}(\mathcal{A}) \tag{4.5}$$

for χ a uniform distribution over S_η, and

$$\begin{aligned} \zeta &= \max\{\gamma_1 - \beta,\ 2\gamma_2 + 1 + 2^{d-1} \cdot 60\} \leq 4\gamma_2, \\ \zeta' &= \max\{2(\gamma_1 - \beta),\ 4\gamma_2 + 2\} \leq 4\gamma_2 + 2. \end{aligned} \tag{4.6}$$

Intuitively, the MLWE assumption is needed to protect against key-recovery, the SelfTargetMSIS is the assumption upon which new message forgery is based, and the MSIS assumption is needed for strong unforgeability.

Specific details regarding the details and further discussion of the signature schema can be found in (Kiltz et al., 2018).

4.2.4 Revocability

Revocability is the property by which a TA, and only the TA, can lift a user's anonymity. Concretely, whenever a valid signature is produced, the TA can, using its secret revocation key, run a revocation algorithm to recover the signer's true identity, (Liu et al., 2007).

Following the proof presented on LARRS paper we have the following theorem (Wen et al., 2023):

Theorem 4.2.7 (revocability) *The proposed Ring signcrypt schema have revocability in the random oracle model assuming the MSIS problem. Given an algorithm A, able to obtain a* $sk \in L$ *by querying an oracle* O_C *and generate a valid signature* σ *on a message* μ *such that* $pk_\kappa \leftarrow Revoke(n, L, z, sk_{TA})$*, where* $pk_\kappa \in L\{pk_\pi\}$.

Assume the algorithm A succeeds in executing above with non-negligible probability, in order to close the ring, and generate a valid signature, it can be divided into two cases according to whether A owns the corresponding secret key.

A does not know corresponding secret key but produce a valid signature, that means A breaks the Unforgeability, which derives a solution for the MSIS Problem with non- negligible advantage, contradict!

A knows corresponding secret key, since sk_π *is the unique secret key in L that A knows, we have* μ *was generated by* sk_π*. From the definition of Revoke Algorithm, the output of* $Revoke(id, L)$ *is* $id_\pi(pk_\pi)$*, contradict with* $pk_\kappa \leftarrow Revoke(id, L)$

5 SCHEMA ANALYSIS

5.1 MEMORY CONSUMPTION

5.1.1 Key Sizes

According to the latest CRYSTALS-Dilithium specification, the `KeyGen()` algorithm produces a public key of 1312 bytes and a private key of 2528 bytes, assuming no compression is applied (Ducas et al., 2018). These sizes reflect the parameter set recommended for Dilithium's second security level, Dilithium2 in short, which balances efficiency and post-quantum security guarantees. The relatively large key sizes, particularly for the private key, are a direct consequence of the lattice-based construction and the need to store multiple high-entropy components.

5.1.2 Parameter Storage

CRYSTALS-Dilithium original implementation provides two alternative strategies, differentiated primarily by their memory requirements. The first approach is optimized for resource-constrained environments, such as embedded devices, and stores only a small set of seed values, ζ, from which all other parameters can be deterministically regenerated. The second approach prioritizes performance by retaining additional precomputed elements, including the matrix $\mathbf{A}$, and the randomness sources K, ρ and ρ'.

In the context of VANETs, where reduced cryptographic latency is essential for maintaining communication integrity under real-time constraints, the second implementation is generally preferred. Accordingly, the memory required to store these parameters must be considered. Based on the definitions in the `MasterKeyGen` and `KeyGen` procedures, ρ is a 256-bit (32-byte) value, and ρ' occupies 512 bits (64 bytes). The matrix $\mathbf{A}$ is structured as a 4×4 matrix of polynomials, with each polynomial containing 256 coefficients. Given that Dilithium uses a modulus $q = 8380417$, each coefficient requires a minimum of 23 bits, resulting in a total of approximately 11,776 bytes to store the full matrix. These storage costs are justified by the improved runtime performance observed during the `SignCrypt` and `VerifyDecrypt` operations, where the availability of precomputed parameters significantly reduces online computation(Ducas et al., 2018).

5.1.3 Signature Size

The standard signature produced by CRYSTALS-Dilithium occupies 4654 bytes, reflecting the combination of the compressed polynomial vector, challenge hash, and response vector. However, in schemes that build on Dilithium to enable additional functionality—such as the LaRRS scheme, which incorporates revocation support through a lightweight and traceable ring signature structure—the overall signature size increases substantially. Specifically, LaRRS introduces multiple individual signatures, a revocation tag C, and an accompanying ciphertext. According to the specification in (Wen et al., 2023), the signature size for a ring of 8 vehicles is approximately 62 KB.

The overall size of the transmitted data must also account for the ciphertext generated by the Kyber encryption scheme. Kyber takes a 32-byte message as input and returns a 768-byte ciphertext. Therefore, if a message of size m bytes is partitioned into 32-byte blocks, the total ciphertext size increases proportionally. As a result, the total size of the transmitted package can be estimated using the following expression:

$$S = 62\,\mathrm{KB} + \left(\frac{m}{32}\right) \times 768$$

This formula captures the combined contribution of the extended signature and the ciphertext to the total communication overhead, which is a critical factor in evaluating the protocol's suitability for real-time vehicular networks.

5.2 PREDICTED EXECUTION TIME

As discussed in the previous section, low latency is a critical requirement in VANETs, where time-sensitive message delivery impacts safety and coordination. This section presents the predicted execution times associated with the proposed scheme, incorporating both signing and encryption operations.

According to benchmark results reported in the original specifications, CRYSTALS-Dilithium achieves an average signing time of 0.75 *ms* per signature and a verification time of 0.18 *ms*. For CRYSTALS-Kyber, encryption and decryption require 0.51 *ms* and 0.54 *ms*, respectively. These values are obtained without the use of optimization techniques or hardware acceleration.

Considering a scenario involving a ring of $n = 8$ vehicles, the predicted execution times for both the message sender and the receiving nodes can be modeled as follows:

Sender-side computation: The originating vehicle generates $n = 8$ individual signatures and performs one encryption operation. The total expected time is:

$$t_{\text{total, sender}} = n \cdot t_{\text{sig}} + t_{\text{enc}} = 8 \cdot 0.75 + 0.51 = 6.51\ ms$$

Receiver-side computation: Each receiving vehicle performs a decryption, verifies one signature, and re-encrypts the message for forwarding. The total expected time is:

$$t_{\text{total, receiver}} = t_{\text{dec}} + t_{\text{sig\_verify}} + t_{\text{enc}} = 0.54 + 0.18 + 0.51 = 1.23\ ms$$

End-to-end latency: Assuming negligible communication and propagation delays, the total end-to-end latency can be estimated by summing the sender's processing time with the cumulative computation performed by the other $n - 1 = 7$ vehicles. Each receiver carries out one decryption, one signature verification, and one encryption, for a total of 1.23 *ms* per vehicle. The resulting latency is:

$$t_{\text{end-to-end}} = t_{\text{total, sender}} + (n-1) \cdot t_{\text{total, receiver}} = 6.51 + 7 \cdot 1.23 = 15.72\ ms$$

This value remains within the real-time operational thresholds for VANET systems, validating the scheme's suitability for latency-sensitive applications.

5.3 LIMITATIONS

While the proposed schema satisfies the general latency requirements for VANET safety applications, certain trade-offs emerge when compared to widely deployed classical schemes such as ECDSA (Knežević et al., 2016). The reported end-to-end latency of 15.72 ms for an 8-vehicle ring demonstrates baseline feasibility. However, it does not reflect the significant performance advantage gained from decades of ECDSA optimization. In hardware-accelerated environments, ECDSA signatures can be verified in microseconds using Application-Specific Integrated Circuits (ASICs), a level of efficiency that current post-quantum cryptographic primitives have not yet achieved. Although such a gap is expected during the early stages of PQC adoption, it may limit the applicability of the schema in latency-critical, high-density deployment scenarios.

A primary implementation challenge is the communication overhead introduced by the signature size, which reaches approximately 62 KB for an 8-vehicle ring. This size exceeds the payload capacity of standard vehicular communication protocols, where individual frame sizes are typically restricted to a few kilobytes. As a result, each message must be fragmented into multiple frames, increasing medium access contention and elevating the risk of transmission failure if any fragment is lost. In contrast, classical signatures such as ECDSA, which are generally less than 100 bytes in size, can be transmitted in a single frame with minimal overhead, offering clear advantages under existing communication constraints.

Finally, the schema's dependence on storing precomputed parameters to achieve low latency introduces a notable memory overhead. In resource-constrained On-Board Units (OBUs), which are often designed with limited available memory, this additional demand may compete with other critical system functions such as buffering, control logic, or protocol handling. As a result, implementing the schema may require trade-offs in system design or necessitate the use of higher-specification hardware. These factors could affect the overall cost and scalability of deployment, particularly in settings where lightweight and economically efficient solutions are prioritized.

6 CONCLUSION

This work addresses the critical vulnerability of VANETs to quantum computing threats by introducing SILMARILLI, a post-quantum security framework built on the NIST-standardized lattice-based primitives CRYSTALS-Dilithium and CRYSTALS-Kyber. By integrating revocable ring signcryption, SILMARILLI provides a cohesive solution for conditional anonymity, accountability, and robust communication security, formally proven to achieve strong guarantees like SUF-CMA and IND-CCA2 against both classical and quantum adversaries.

Performance analysis validates SILMARILLI's theoretical viability, demonstrating an estimated end-to-end latency of 15.72 ms for an 8-vehicle ring, which falls within the operational thresholds for real-time vehicular safety applications. This result confirms that the scheme's core architecture is fundamentally sound and highly effective for its intended environment, representing a significant step forward in securing next-generation intelligent transportation systems.

A primary direction for future research is mitigating communication overhead by adapting advanced compression techniques for lattice-based signatures, such as the method proposed by Bai and Galbraith (Bai and Galbraith, 2014). Applying such a technique could significantly reduce signature size, enhancing the scheme's practicality for deployment on existing VANET infrastructure by minimizing message fragmentation. This optimization would, however, require a rigorous re-evaluation of the scheme's security proofs to ensure the compressed signature remains unforgeable.

A second avenue for optimization lies in architectural enhancements to the SignCrypt and verifyDecript primitives. Instead of the current generic "sign-then-encrypt" composition, SILMARILLI could be re-architected to use an interleaved paradigm. In this more integrated approach, the symmetric encryption key is derived directly from the signature components during verification, eliminating the separate overhead of the Kyber ciphertext and potentially reducing computational complexity by reusing polynomial operations. This would require developing a new, unified security proof demonstrating both IND-CCA2 and SUF-CMA properties for the combined primitive.

Finally, to enhance long-term security for vehicles as long-lived assets, future work should focus on integrating forward secrecy. This property ensures that the compromise of a private key in one time period does not affect the security of signatures generated in the past, a critical feature for applications like accident forensics. A promising approach is outlined by Cao, who propose a forward-secure authentication protocol using a lattice-based group signature for VANETs (Cao et al., 2022). Their methodology achieves forward security by employing the Bonsai-tree signature architecture, which functions as a scalable extension of the trapdoor function and reduces algorithmic complexity, making it a highly favorable enhancement for the resource-constrained VANET environment.

REFERENCES

Abdalla, M., Fouque, P.-A., Lyubashevsky, V., and Tibouchi, M. (2012). Tightly-secure signatures from lossy identification schemes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 572–590. Springer.

Ajtai, M. (1996). Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108.

Ajtai, M. (1998). The shortest vector problem in l2 is np-hard for randomized reductions. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 10–19.

Al-Mekhlafi, Z. G., Al-Janabi, H. D. K., Khalil, A., Al-Shareeda, M. A., Mohammed, B. A., Alsadhan, A. A., Alayba, A. M., Saleh, A. M. S., Al-Reshidi, H. A., and Almekhlafi, K. (2024). Lattice-based cryptography and fog computing based efficient anonymous authentication scheme for 5g-assisted vehicular communications. *IEEE Access*.

Alkim, E., Bindel, N., Buchmann, J., Dagdelen, Ö., Eaton, E., Gutoski, G., Krämer, J., and Pawlega, F. (2017). Revisiting tesla in the quantum random oracle model. In *Post-Quantum Cryptography: 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings 8*, pages 143–162. Springer.

Bai, S. and Galbraith, S. D. (2014). An improved compression technique for signatures based on learning with errors. In *Topics in cryptology–CT-RSA 2014: the cryptographer's track at the RSA conference 2014, san francisco, CA, USA, february 25-28, 2014. proceedings*, pages 28–47. Springer.

Bellare, M. and Namprempre, C. (2008). Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *Journal of cryptology*, 21(4):469–491.

Bernstein, D. J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., and Schwabe, P. (2019). The sphincs+ signature framework. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pages 2129–2146.

Boukerche, A., Oliveira, H. A., Nakamura, E. F., and Loureiro, A. A. (2008). Vehicular ad hoc networks: A new challenge for localization-based systems. *Computer communications*, 31(12):2838–2849.

Cai, Y., Zhang, H., and Fang, Y. (2020). A conditional privacy protection scheme based on ring signcryption for vehicular ad hoc networks. *IEEE Internet of Things Journal*, 8(1):647–656.

Cao, Y., Xu, S., Chen, X., He, Y., and Jiang, S. (2022). A forward-secure and efficient authentication protocol through lattice-based group signature in vanets scenarios. *Computer Networks*, 214:109149.

Chatterjee, S., Pandit, T., Puria, S. K. P., and Shah, A. (2020). Signcryption in a quantum world. *Cryptology ePrint Archive*.

Chen, L., Tu, T., Yu, K., Zhao, M., and Wang, Y. (2021). V-ldaa: a new lattice-based direct anonymous attestation scheme for vanets system. *Security and Communication Networks*, 2021(1):4660875.

Cremers, C., Peltonen, A., and Zhao, M. (2024). An extended hierarchy of security notions for threshold signature schemes and automated analysis of protocols that use them. *Cryptology ePrint Archive*.

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and Stehlé, D. (2018). Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 238–268.

Engoulou, R. G., Bellaïche, M., Pierre, S., and Quintero, A. (2014). Vanet security surveys. *Computer Communications*, 44:1–13.

Ferguson, N., Schneier, B., and Kohno, T. (2011). *Cryptography engineering: design principles and practical applications*. John Wiley & Sons.

Gentry, C., Peikert, C., and Vaikuntanathan, V. (2008). Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206.

Hasrouny, H., Samhat, A. E., Bassil, C., and Laouiti, A. (2017). Vanet security challenges and solutions: A survey. *Vehicular Communications*, 7:7–20.

Hülsing, A. (2013). W-ots+–shorter signatures for hash-based signature schemes. In *Progress in Cryptology–AFRICACRYPT 2013: 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22-24, 2013. Proceedings 6*, pages 173–188. Springer.

Jiao, C. and Xiang, X. (2021). Anti-quantum lattice-based ring signature scheme and applications in vanets. *Entropy*, 23(10):1364.

Jiao, J., Guo, L., Yu, W., Yang, S., and Li, S. (2025). An efficient lattice-based heterogeneous signcryption scheme for vanets. *Concurrency and Computation: Practice and Experience*, 37(3):e8384.

Katz, J. and Lindell, Y. (2007). *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC.

Kiltz, E., Lyubashevsky, V., and Schaffner, C. (2018). A concrete treatment of fiat-shamir signatures in the quantum random-oracle model. In *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part III 37*, pages 552–586. Springer.

Knežević, M., Nikov, V., and Rombouts, P. (2016). Low-latency ecdsa signature verification—a road toward safer traffic. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 24(11):3257–3267.

Lamport, L. (1979). Constructing digital signatures from a one way function.

Lesaignoux, D. and Carmona, M. (2024). On the implementation of a lattice-based daa for vanet system. *Cryptology ePrint Archive*.

Liang, Z. and Zhao, Y. (2022). Number theoretic transform and its applications in lattice-based cryptosystems: A survey. *arXiv preprint arXiv:2211.13546*.

Liu, D. Y., Liu, J. K., Mu, Y., Susilo, W., and Wong, D. S. (2007). Revocable ring signature. *Journal of Computer Science and Technology*, 22:785–794.

Luo, G., Yuan, Q., Zhou, H., Cheng, N., Liu, Z., Yang, F., and Shen, X. S. (2018). Cooperative vehicular content distribution in edge computing assisted 5g-vanet. *China communications*, 15(7):1–17.

Mejri, M. N., Ben-Othman, J., and Hamdi, M. (2014). Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66.

Mohamed, S. A. E. (2019). Automatic traffic violation recording and reporting system to limit traffic accidents: based on vehicular ad-hoc networks (vanet). In *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*, pages 254–259. IEEE.

Mukhtar, A., Xia, L., and Tang, T. B. (2015). Vehicle detection techniques for collision avoidance systems: A review. *IEEE transactions on intelligent transportation systems*, 16(5):2318–2338.

Mundhe, P., Yadav, V. K., Verma, S., and Venkatesan, S. (2020). Efficient lattice-based ring signature for message authentication in vanets. *IEEE Systems Journal*, 14(4):5463–5474.

Nath, H. J. and Choudhury, H. (2024). Lbpv: Lattice-based privacy-preserving mutual authentication scheme for vanet. *Computers and Electrical Engineering*, 120:109765.

Papadakis, D. M., Savvides, A., Michael, A., and Michopoulos, A. (2024). Advancing sustainable urban mobility: Insights from best practices and case studies. *Fuel Communications*, 20:100125.

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332.

Singh, R., Saluja, D., and Kumar, S. (2021). 5g enabled vanet: Enhancing the capabilities of vehicular communication network. In *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–5. IEEE.

Singh, S. and Vijayan, R. (2011). Enhanced security for information flow in vanet using signcryption and trust level. *International Journal of Computer Applications*, 16(5):13–18.

van Emde Boas, P. (1981). Another np-complete problem and the complexity of computing short vectors in a lattice. *Tecnical Report, Department of Mathmatics, University of Amsterdam.*

Wen, J., Bai, L., Yang, Z., Zhang, H., Wang, H., and He, D. (2023). Larrs: Lattice-based revocable ring signature and its application for vanets. *IEEE Transactions on Vehicular Technology*, 73(1):739–753.

Wen, J., Susilo, W., Yang, R., Yu, Z., and Zhang, H. (2025). Revocable ring signatures with cca-anonymity from standard lattices. *Computer Standards & Interfaces*, 91:103893.

Yu, H., Bai, L., Hao, M., and Wang, N. (2020). Certificateless signcryption scheme from lattice. *IEEE Systems Journal*, 15(2):2687–2695.

Zhang, J. and Cui, X. (2024). Lbcsc: Lattice-based chameleon signcryption scheme for secure and privacy-preserving vehicular communications. *Transactions on Emerging Telecommunications Technologies*, 35(10):e5040.