

Article

A Lightweight Double-Ring Hybrid Sparse NTRU (DRH-SNTRU) Scheme for Secure and Real-Time Communication in the Internet of Vehicles (IoV)

Weiqi Wang ¹, Gwo-Chin Ching ²  and Soo Fun Tan ^{3,*} 

¹ Faculty of Computing and Informatics, University Malaysia Sabah (UMS), Kota Kinabalu 88400, Malaysia; wang_weiqi_di21@iluv.ums.edu.my

² Faculty of Engineering, Multimedia University, Cyberjaya 63100, Malaysia; gcchung@mmu.edu.my

³ Cybersecurity Research Lab, Creative Advanced Machine Intelligence Research Centre, Faculty of Computing and Informatics, University Malaysia Sabah (UMS), Kota Kinabalu 88400, Malaysia

* Correspondence: soofun@ums.edu.my

Abstract

The Internet of Vehicles (IoV) is rapidly emerging as a core component of intelligent transportation systems, enabling real-time communication among vehicles, infrastructure, and cloud platforms. However, the increasing interconnectivity of vehicular systems and the advancement of quantum computing introduce significant security challenges to existing cryptographic mechanisms. Conventional schemes such as RSA and Elliptic Curve Cryptography (ECC) are vulnerable to quantum attacks and are computationally inefficient for resource-constrained vehicular environments. To address these limitations, this paper proposes a Double-Ring Hybrid Sparse NTRU (DRH-SNTRU) framework, a lightweight and quantum-resistant cryptographic scheme for secure IoV communication. The proposed framework introduces three key enhancements: (i) controlled-support sparse polynomial structures to reduce polynomial multiplication complexity while improving entropy distribution; (ii) a double-ring algebraic architecture that separates key operations from message processing to enhance structural security and minimize coefficient leakage; and (iii) hybrid ephemeral keys derived from contextual entropy to strengthen forward secrecy and adaptive security. An optional ciphertext evaluation mechanism is further incorporated to detect malformed and replayed ciphertexts prior to decryption. Security analysis demonstrates that the proposed framework achieves IND-CPA security under the hardness assumption of the NTRU lattice problem and can be extended to resist chosen-ciphertext attacks through the integrated validation mechanism. Experimental benchmarking across polynomial dimensions $N = 512$ to 8192 demonstrates that DRH-SNTRU achieves low setup overhead below $3\ \mu\text{s}$, efficient decryption latency of approximately $305.64\ \mu\text{s}$ at $N = 8192$, and compact sparse private key representation of only 117 bytes at higher dimensions. Compared with Standard NTRUEncrypt, NTRU-HRSS, and Ring-LWE Encryption, the proposed framework demonstrates improved decryption efficiency, lightweight storage overhead, and enhanced ciphertext integrity protection while maintaining practical scalability for resource-constrained post-quantum IoV environments.



Academic Editor: Kartik B. Ariyur

Received: 31 March 2026

Revised: 12 May 2026

Accepted: 15 May 2026

Published: 21 May 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons](https://creativecommons.org/licenses/by/4.0/)

[Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Keywords: Internet of Vehicles (IoV); secure vehicular communication; post-quantum cryptography; lattice-based cryptography; NTRU; double-ring structure; sparse polynomial; controlled-support sparsity; context-aware encryption

1. Introduction

The Internet of Vehicles (IoV) is emerging as a critical component of intelligent transportation systems, integrating real-time communication among vehicles, infrastructure, and cloud-based platforms. As the global IoV market is projected to grow at a compound annual growth rate (CAGR) of 21.4% from 2025 to 2034 [1], ensuring the security of these systems becomes increasingly critical. The rise in connected and autonomous vehicles brings heightened risks such as vehicle hijacking, replay attacks, identity spoofing, and unauthorized firmware updates, all of which could compromise both user safety and data integrity [2–4]. Recent studies have identified several critical vulnerabilities, particularly weaknesses in quantum-resistant cryptography algorithms, key distribution mechanisms within VANETs and the absence of encryption protocols that are resilient to future cryptographic threats.

Traditional cryptographic methods like RSA and ECC are no longer sufficient in the face of advancing quantum computing capabilities [5,6]. Post-Quantum Cryptography (PQC), particularly lattice-based schemes such as NTRU, offers a robust alternative with resistance to quantum attacks, low computational overhead, and suitability for resource-constrained vehicular environments [7,8]. Studies [9–12] have demonstrated that PQC enhances secure vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication, providing long-term confidentiality and protection against store-now-decrypt-later threats. Therefore, adopting PQC is essential not only for maintaining present-day security but also for ensuring the resilience of IoV systems in the quantum era.

Among various PQC approaches, lattice-based cryptography has emerged as one of the most practical and efficient candidates due to its strong security foundation, relatively low computational complexity, and resistance against quantum attacks. In particular, NTRU-based cryptosystems are highly suitable for IoV environments because of their efficient polynomial arithmetic, fast encryption and decryption processes, and compatibility with resource-constrained vehicular devices such as On-Board Units (OBUs) and edge nodes. Several recent studies have demonstrated the feasibility of lattice-based cryptographic schemes for vehicular authentication, privacy preservation, and secure V2V/V2I communication. Despite these advantages, existing NTRU and RLWE-based approaches still suffer from several important limitations. Many current schemes rely on computationally expensive polynomial multiplication operations, large parameter sizes, and complex cryptographic structures, which increase processing latency and communication overhead in highly dynamic vehicular environments. In addition, several lightweight lattice-based authentication protocols mainly focus on theoretical security guarantees without sufficiently addressing implementation efficiency, sparse polynomial optimization, or practical deployment suitability in real-time IoV systems. Standard NTRU variants may also experience decryption instability, parameter sensitivity, and increased implementation complexity under constrained vehicular environments. Furthermore, most existing schemes lack adaptive ephemeral key mechanisms and ciphertext evaluation functions to improve robustness against replayed or malformed ciphertext attacks.

Motivated by these limitations, this paper proposes a lightweight and quantum-resistant Double-Ring Hybrid Sparse NTRU (DRH-SNTRU) framework specifically designed for secure IoV communication environments. The proposed scheme introduces a controlled-support sparse polynomial structure combined with a double-ring cryptographic architecture to reduce computational complexity while improving entropy distribution and security robustness. In addition, the framework integrates a context-aware ephemeral key generation mechanism together with an evaluation function to strengthen resistance against replay attacks and ciphertext manipulation in highly dynamic vehicular scenarios. The main objective of this study is to design a lightweight post-quantum cryptographic framework that achieves secure communication, reduced computational overhead, and

practical deployment suitability for resource-constrained IoV systems while maintaining strong resistance against quantum-enabled adversaries. The main contributions of this paper are summarized as follows:

- A Novel DRH-SNTRU Cryptographic Scheme

This paper proposes a Double-Ring Hybrid Sparse NTRU (DRH-SNTRU) scheme, a lightweight lattice-based cryptographic framework specifically designed for secure communication in Internet of Vehicles (IoV) environments.

- Controlled-Support Sparse Polynomial Design

A new controlled-support sparsity model is introduced, which regulates both the number and spatial distribution of non-zero coefficients. This approach reduces computational complexity while enhancing entropy and resistance against structural attacks.

- Double-Ring Cryptographic Architecture

The proposed scheme introduces a double-ring structure that separates key generation and message processing, improving security by minimizing interaction between sensitive key material and plaintext data.

- Hybrid Ephemeral Key Mechanism for IoV

A context-aware ephemeral key generation method is proposed, leveraging dynamic vehicular data (e.g., GPS, timestamps, CAN-bus identifiers) to provide forward secrecy and adaptive security in highly dynamic environments.

- Enhanced Robustness via Evaluation Function

An optional evaluation function is incorporated to detect replayed or malformed ciphertexts, strengthening resistance against adversarial attacks in IoV scenarios.

2. Related Works

The growing interconnectivity within the Internet of Vehicles (IoV) ecosystem demands cryptographic schemes that can support real-time, scalable, and future-proof security under resource-constrained conditions. Recent studies have explored the potential of Post-Quantum Cryptography (PQC) to address these challenges. Alsaadi et al. (2025) [8] proposed a verifiable decryption scheme using lattice-based post-quantum methods for Vehicle-to-Infrastructure (V2I) communication, highlighting its resilience against “store-now-decrypt-later” threats and quantum attacks. While this approach ensures data correctness and scalability, its dependence on certificate authorities and lack of deployment validation under high-mobility environments present gaps in practical IoV adoption. However, they may face challenges such as computational overhead, reliance on trusted infrastructure, and limited real-world validation under dynamic vehicular conditions. Similarly, Karakaya (2025) [13] proposed a lightweight PQC-integrated DAG blockchain for mobile cyber-physical systems, which supports decentralized, low-latency secure communication. The proposed model enhances data integrity and authentication in resource-constrained systems by leveraging quantum-resistant encryption without imposing high computational overhead. Despite its efficiency, the scheme may face scalability and synchronization challenges in highly dynamic vehicular networks due to the structural complexity of DAGs and assumptions about stable node behavior.

Recent works have increasingly focused on NTRU-based schemes due to their promising performance on embedded systems. Lohmiller et al. (2025) [14] evaluated NTRU migration for automotive ECUs, confirming its suitability for constrained vehicular devices due to its efficient implementation and post-quantum security. However, NTRU offers lightweight efficiency but suffers from decryption failures and noise sensitivity, raising

reliability concerns for safety-critical automotive systems. Its integration challenges, closed-source limitations, and risks from improper parameterization further complicate its secure adoption in evolving vehicular environments.

Bhatt et al. (2024) [15] proposed a lattice-based post-quantum identity signature scheme tailored for Vehicular Ad Hoc Networks (VANETs) to ensure secure authentication and prevent impersonation attacks. The proposed scheme achieves anonymity, traceability, and unlinkability, which are critical for preserving driver privacy while enabling authority-level tracking under legitimate conditions. Though it strengthens post-quantum security, the scheme may lack revocation mechanisms and does not address broader routing or data confidentiality issues in VANET environments. While Wang and Tan's NTRU-based protocol [16] offers quantum-resistant security using a lattice-based (likely NTRU) lightweight approach, the study acknowledges potential integration complexity due to cryptographic overhead in constrained autonomous systems. Their solution also relies on frequent updates and precise parameter selection to maintain robustness, which could be impractical for vehicles with long lifecycles and limited maintenance cycles.

Overall, existing literature demonstrates that lattice-based PQC schemes are among the most promising candidates for securing future IoV communication systems due to their quantum resistance and suitability for resource-constrained vehicular environments, as summarized in Table 1. Nevertheless, several significant challenges remain insufficiently addressed. Most existing approaches prioritize theoretical security guarantees while overlooking the lightweight implementation efficiency required for real-time vehicular communication. Many proposed schemes rely on computationally intensive signature mechanisms, large lattice parameters, complex blockchain synchronization processes, or heavyweight cryptographic architectures that are impractical for latency-sensitive IoV environments and constrained On-Board Units (OBUs), as summarized in Table 1.

Table 1. Computational Complexity Comparison of Lattice-Based Encryption Schemes with Classical Polynomial Arithmetic.

Ref.	Scheme/ Approach	Main Contribution	Strengths	Limitations
Alsaadi et al. (2025) [8]	Lattice-based verifiable decryption for V2I	Quantum-resistant V2I communication	Resists store-now-decrypt-later attacks; scalable encryption	Depends on certificate authorities; limited real-world mobility validation
Karakaya (2025) [13]	PQC-integrated DAG blockchain	Lightweight decentralized secure communication	Low-latency authentication; decentralized integrity	DAG synchronization complexity; scalability issues in dynamic IoV
Lohmiller et al. (2025) [14]	NTRU migration for automotive ECUs	Embedded NTRU implementation	Efficient for constrained vehicular hardware	Decryption failures; parameter sensitivity; integration complexity
Bhatt et al. (2024) [15]	Lattice-based VANET identity signature	Anonymous post-quantum authentication	Provides anonymity, traceability, unlinkability	Limited revocation and confidentiality mechanisms
Wang and Tan [16]	NTRU-based lightweight authentication	Lightweight quantum-resistant authentication	Reduced computational complexity	Requires frequent parameter tuning and updates
Standard NTRUEncrypt [17]	Classical NTRU cryptosystem	Efficient lattice-based encryption	Small key sizes; low computational cost	Vulnerable to parameter tuning issues and side-channel attacks
NTRU-HRSS [18,19]	Hardened NTRU variant	Improved security robustness	Stronger post-quantum security guarantees	Increased implementation complexity and computational overhead

In addition, empirical NTRU variants such as standard NTRUEncrypt [17] and NTRU-HRSS [18,19] continue to suffer from important limitations, including decryption instability, noise sensitivity, rigid parameter tuning, ciphertext expansion, and potential vulnerability to side-channel or message recovery attacks when improperly configured. Existing schemes also provide limited optimization of sparse polynomial structures, insufficient adaptive ephemeral key management, and inadequate protection against malformed or replayed ciphertext attacks in highly dynamic vehicular environments.

More importantly, current studies rarely integrate lightweight sparse polynomial optimization, double-ring cryptographic separation, adaptive ephemeral key generation, and ciphertext evaluation mechanisms into a unified post-quantum framework specifically designed for real-time IoV deployment. Consequently, there remains a critical research gap in developing a lightweight, scalable, and practically deployable post-quantum cryptographic framework that simultaneously achieves low computational overhead, strong quantum-resistant security, efficient polynomial operations, and robustness against dynamic vehicular communication threats. To address these limitations, this paper proposes a Double-Ring Hybrid Sparse NTRU (DRH-SNTRU) framework that combines controlled-support sparse polynomial structures, double-ring cryptographic separation, adaptive ephemeral key mechanisms, and enhanced ciphertext evaluation functions to improve computational efficiency, lightweight deployment suitability, and security robustness for next-generation post-quantum IoV communication systems.

3. Preliminaries

This section establishes the fundamental algebraic structures, definitions, and theoretical constructs necessary for constructing the proposed Double-Ring Hybrid Sparse NTRU (DRH-SNTRU) algorithm, used in context-aware, zero-trust vehicular networks.

3.1. Polynomial Rings and Notation

Let $\mathbb{Z}_q$ denote the ring of integers modulo q . For a positive integer N , define the polynomial ring as $R_q = \mathbb{Z}_q[x]/(x^N - 1)$, such that polynomials of degree less than N , with coefficients in $\mathbb{Z}_q$, modulo the cyclotomic polynomial $x^N - 1$. The smaller polynomial rings can be further defined as $R_p = \mathbb{Z}_p[x]/(x^N - 1)$, where $p \ll q$ used for plaintext operations.

3.2. Sparse Polynomials

Sparse polynomials are polynomials with a limited number of non-zero coefficients.

Definition 1. Sparse Polynomials [17,19]: Let $R = \mathbb{Z}_q[x]/(x^N - 1)$, a polynomial $f(x) \in R_q$ is said to be (d_1, d_2) -sparse if it has exactly d_1 coefficients equal to $+1$, d_2 coefficients equal to -1 , and all other coefficients equal to 0.

Lemma 1. Fast Multiplication: If $f \in R$ is sparse with $wt(f) = d$ and $g \in R$ is dense, then: Time Complexity of $f \cdot g \in \mathcal{O}(dN)$. This improves over naive dense multiplication $\mathcal{O}(N^2)$, essential for lightweight cryptography.

3.3. Nth Degree Truncated Polynomial Ring (NTRU) Algorithm

Definition 2. Nth Degree Truncated polynomial ring (NTRU) [19]: Let the security parameter be λ , and let $N = N(\lambda)$ be a positive integer (typically a power of two). Let $p \ll q \in \mathbb{Z}$ be small and large moduli, respectively, such that $\gcd(p, q) = 1$, and define the truncated polynomial ring $R = \mathbb{Z}[x]/(x^N - 1)$. Denote $R_q = R/qR = \mathbb{Z}_q[x]/(x^N - 1)$ and $R_p = \mathbb{Z}_p[x]/(x^N - 1)$. Let the key components consist of two private polynomials $f, g \in R$, where both are sampled with

small coefficients, typically from the set $\{-1, 0, 1\}$. The polynomial f is required to be invertible in both $R_q = \mathbb{Z}_q[x]/(x^N - 1)$ and $R_p = \mathbb{Z}_p[x]/(x^N - 1)$. The public key is then computed as $h = f^{-1} \cdot g \bmod q$, where $h \in R_q$.

- **Encryption:** To encrypt a message $m \in R_p$, the sender samples a random small polynomial $r \in R$, and computes the ciphertext, such that $c = r \cdot h + m \bmod q$, where $c \in R_q$ is the ciphertext polynomial.
- **Decryption:** To decrypt the ciphertext $c \in R_q$, the receiver first computes the intermediate product $a = f \cdot c \bmod q$. The resulting polynomial a is then centre-lifted, meaning its coefficients are mapped to the interval $[-q/2, q/2]$ to ensure correct modular reduction. Finally, the plaintext message is recovered by computing $m = f^{-1} \cdot a \bmod p$, where f^{-1} is the inverse of f in the ring R_p . The result $m \in R_p$ is the original message polynomial.

3.4. Ring Learning with Errors (Ring-LWE)

Definition 3. Ring-Learning With Error, Ring-LWE [20]: Let the security parameter be λ , and let $n = n(\lambda)$ be a power of two. Let $q = q(\lambda) \geq 2$ be an integer modulus and let $R = \mathbb{Z}[x]/(x^n + 1)$ denote the cyclotomic ring of degree n , and define $R_q = R/qR = \mathbb{Z}_q[x]/(x^n + 1)$. Let χ be an error probability distribution over R , such as a discrete Gaussian or binomial distribution. Let the Ring-LWE distribution $A_{s,\chi}$ over $R_q \times R_q$ be defined by choosing $a \in R_q$ uniformly at random, sampling $e \leftarrow \chi$, and compute $(a, b = a \cdot s + e) \in R_q \times R_q$,

where $s \in R_q$ is the secret.

- **Search Ring-LWE Problem:** Given access to a polynomial number of samples $(a_i, b_i = a_i \cdot s + e_i) \in R_q \times R_q$, for $i = 1, 2, \dots, m$, recover the secret polynomial $s \in R_q$. The Search Ring-LWE assumption posits that no efficient (quantum or classical) algorithm can solve this problem with non-negligible probability.
- **Decision Ring-LWE Problem:** Distinguish between two distributions over $R_q \times R_q$: The Ring-LWE distribution $(a_i, b_i = a_i \cdot s + e_i)$, where $a_i \leftarrow R_q$, $e_i \leftarrow \chi$ / The uniform distribution $(a_i, b_i) \leftarrow R_q \times R_q$. The Decision Ring-LWE assumption asserts that it is computationally infeasible to distinguish these two distributions.

4. Proposed Double-Ring Hybrid Sparse NTRU in Securing IoV

The Internet of Vehicles (IoV) operates in a highly dynamic and resource-constrained environment, where security mechanisms must be both robust against emerging threats and efficient enough for real-time communication. Traditional public-key cryptographic schemes, including classical NTRU variants, often struggle to balance post-quantum security, computational efficiency, and long-term deployability in vehicular systems. To address these challenges, we propose a Double-Ring Hybrid Sparse NTRU (DRH-SNTRU) scheme, a lightweight and quantum-resistant encryption framework for securing IoV environments.

4.1. Controlled-Support Sparse Polynomials: Core Optimization for IoV

We introduce a controlled-support sparse polynomial construction, extending classical sparse NTRU designs by explicitly constraining coefficient placement rather than weight alone. Unlike conventional NTRU schemes that primarily control fixed Hamming weight, the proposed method further enforces support-level constraints by regulating both the number and spatial distribution of non-zero coefficients. Specifically, sparse polynomials with ternary or quaternary values are constructed with enforced spacing between active positions, thereby reducing structural leakage while maintaining computational efficiency. This design choice is not merely an efficiency trick; it serves both performance and security

objectives. On the other hand, from a computational perspective, sparsity significantly reduces the cost of polynomial multiplication, enabling faster encryption and decryption on on-board units with limited processing power. Lastly, from a security perspective, controlling the support of non-zero coefficients increases entropy per bit and avoids structural patterns that could otherwise be exploited by statistical or lattice-based attacks. As a result, the sparse construction aligns naturally with the practical constraints of IoV devices while maintaining strong cryptographic properties.

Definition 4. Controlled-Support Sparse Polynomial: Let $R_q = \mathbb{Z}_q[x]/(x^N - 1)$, and let $f(x) \in R_q$ be a sparse polynomial. We define $f(x)$ as a controlled-support sparse polynomial if the following conditions hold:

i. Support Set:

The support of $f(x)$, denoted $\text{Supp}(f) = S_f$, is a subset of indices where the polynomial has non-zero coefficients:

$$S_f \subseteq \{0, 1, \dots, N-1\}, \text{ such that } f(x) = \sum_{i \in S_f} a_i x^i, a_i \in \mathbb{Z}_q \setminus \{0\}$$

ii. Controlled Spacing:

For any distinct $i, j \in S_f$, the indices satisfy a minimum distance constraint:

$$|i - j| \geq \delta, \text{ for some fixed } \delta > 0$$

The proposed controlled spacing constraint ensures improved diffusion properties and enhances resistance against structural or pattern-based attacks by enforcing a controlled distribution of non-zero terms across the polynomial domain.

4.2. Double-Ring Structure: Algebraic Separation for Enhanced Security

Beyond sparsity, DRH-SNTRU introduces a double-ring algebraic structure that explicitly separates key-related operations from message processing with the aim of improving both computational efficiency and cryptographic robustness. Unlike classical NTRU schemes, where encryption, decryption, and key computations are performed within a single polynomial ring, the proposed framework distributes these operations across two algebraically linked rings with different security objectives.

In classical NTRU schemes, all cryptographic operations are performed in the ring:

$$R_q = \mathbb{Z}_q[x]/(x^N - 1)$$

where both keying material and message-related computations coexist. While algebraically convenient, this unified structure may allow unintended interactions between key material and message components. In contrast, the proposed scheme operates across two distinct but algebraically linked rings:

- **Primary Ring:** A primary ring modulo q for public-key computation, and ciphertext formation, such that:

$$R_q = \mathbb{Z}_q[x]/(x^N - 1)$$

- **Message Ring:** A message ring modulo a smaller integer p for message encoding and recovery during decryption, such that:

$$R_p = \mathbb{Z}_p[x] / (x^N - 1)$$

The main rationale behind this separation is to isolate sensitive key operations from plaintext manipulation processes. During encryption, computationally intensive lattice operations are confined to the primary ring, R_q , while lightweight message encoding and recovery are handled independently within R_p . This separation reduces unintended algebraic interactions between secret key coefficients and plaintext data, thereby minimizing coefficient leakage, noise accumulation, and decryption instability. In addition, the double-ring architecture improves implementation flexibility and modularity. Auxiliary security functions, such as entropy masking, ephemeral parameter generation, replay detection, or authentication tagging, can be integrated into one ring without directly affecting the core lattice encryption process in the other ring. This modular separation is particularly beneficial for resource-constrained IoV environments, where lightweight computation, low latency, and operational stability are critical requirements.

Furthermore, the algebraic separation contributes to improved cryptographic hygiene by reducing side-channel exposure during polynomial operations. Since plaintext-related computations are processed independently from security-sensitive lattice operations, the proposed structure reduces the risk of correlated leakage patterns that may arise in traditional single-ring NTRU implementations. Overall, the proposed double-ring architecture enhances lightweight operational efficiency, improves security isolation between key and message processing, and provides greater adaptability for future post-quantum vehicular communication systems.

4.3. Hybrid Ephemeral Keys: Forward Secrecy and Adaptive Security

To further strengthen security in highly dynamic vehicular networks, DRH-SNTRU incorporates hybrid ephemeral keys. These transient keys are generated uniquely for each session or message and are used in conjunction with the long-term private key. The ephemeral key is constructed as a controlled-support sparse polynomial derived from unpredictable contextual entropy, such as timestamps, vehicle state, or location-dependent data.

The introduction of hybrid ephemeral keys serves two critical purposes. First, it provides forward secrecy: even if the long-term private key is compromised at a later time, previously transmitted ciphertexts remain secure because the ephemeral keys used during encryption are never stored or reused. Second, it enables adaptive security, allowing the encryption strength to vary according to operational risk—such as transitioning from low-risk idle states to high-speed or high-density convoy scenarios.

Formally, the public key is generated as

$$h = f^{-1} \cdot g \bmod q,$$

where f and g are sparse polynomials defined in the primary ring. For each encryption instance, an ephemeral sparse polynomial r_{session} is generated using a controlled-support mechanism parameterized by contextual entropy:

$$r = \text{Controlled} - \text{Support} - \text{Sparse}(d, \mathcal{E}(\text{context})).$$

The ciphertext is then computed as

$$c = r \cdot h + m \bmod q,$$

where the message m is encoded in the message ring R_p . After encryption, the ephemeral key r is immediately discarded and never reused. Consequently, even if the long-term secret polynomial f is exposed, an adversary cannot recover past plaintexts, as the ephemeral randomness required for decryption is irretrievable.

By jointly leveraging sparse polynomial optimization, explicit ring separation, and hybrid ephemeral keying, the proposed DRH-SNTRU scheme achieves a balanced combination of post-quantum security, computational efficiency, and forward secrecy. These properties make it particularly well-suited for IoV scenarios, where vehicles must securely exchange data under strict latency constraints, limited computational resources, and evolving threat models. The proposed design thus represents a meaningful advancement over conventional NTRU-based approaches for next-generation vehicular networks

4.4. Proposed Double-Ring Hybrid Sparse NTRU Algorithm

This section presents the proposed Double-Ring Hybrid Sparse NTRU (DRH-SNTRU) algorithm, detailing its key generation, encryption, and decryption procedures. The design explicitly leverages controlled-support sparse polynomials and a double-ring structure to achieve efficient and secure message exchange in Internet of Vehicles (IoV) environments. An optional evaluation function is also introduced to enhance robustness against replay and structural attacks.

- **Setup/Key Generation** (1^λ). Given a security parameter λ , let $N = N(\lambda)$ be the polynomial degree and let $p \ll q$ be positive integers such that $\gcd(p, q) = 1$. Define the polynomial rings $R_q = \mathbb{Z}_q[x]/(x^N - 1)$, $R_p = \mathbb{Z}_p[x]/(x^N - 1)$.

Select two controlled-support sparse polynomials

$$f, g \in R_q,$$

where the number and placement of non-zero coefficients are constrained according to the proposed sparsity rules. The polynomial f is chosen such that it is invertible modulo q and satisfies

$$f \equiv 1 \pmod{p}.$$

Compute the public key polynomial

$$h = f^{-1} \cdot g \pmod{q}.$$

Finally, output:

$$\text{Public key : } PK = h,$$

$$\text{Private key : } SK = (f, f^{-1})$$

- **Encrypt (PK, m, ctx)**. Given the public key $h \in R_q$, a plaintext message $m \in R_p$, and IoV contextual information ctx , proceed as follows. Extract contextual entropy $\mathcal{E}(ctx)$ from sources such as GPS coordinates, timestamps, or CAN-bus identifiers. Using this entropy, generate an ephemeral controlled-support sparse polynomial such that:

$$r \leftarrow \text{SparsePoly}(\mathcal{E}(ctx)) \in R_q,$$

where r is unique for each encryption instance and is never reused. Subsequently, compute the ciphertext such that:

$$c = r \cdot h + m \pmod{q}$$

Output the ciphertext e . The ephemeral polynomial r is discarded immediately after encryption, providing lightweight masking and forward secrecy against passive adversaries.

- **Decrypt(SK, c).** Given the private key (f, f^{-1}) and a ciphertext compute the intermediate polynomial such that:

$$a = f \cdot c \pmod{q}$$

Then recover the plaintext message by reducing modulo p :

$$m = a \pmod{p}.$$

If the system parameters are correctly selected and the noise term induced by $r \cdot h$ remains within the prescribed bounds, the decryption procedure outputs the original plaintext m with overwhelming probability.

- **Evaluation Function(c).** To enhance robustness in adversarial IoV environments, an optional evaluation function may be applied to the ciphertext prior to decryption. Define

$$\text{Eval}(c) = \text{VerifyContext}(c) + \text{PolynomialIntegrity}(c),$$

where $\text{VerifyContext}()$ validates the contextual entropy associated with the ciphertext to prevent replay attacks; subsequently $\text{PolynomialIntegrity}()$ checks compliance with controlled-support sparsity rules and ensures that error bounds are not violated. Only ciphertexts that pass the evaluation function are forwarded to the decryption phase. This optional step enables early rejection of malformed or replayed ciphertexts, improving overall system resilience without introducing significant computational overhead.

5. Security Analysis

This section analyzes the confidentiality of the proposed Double-Ring Hybrid Sparse NTRU algorithm under the notions of indistinguishability under chosen-plaintext attack (IND-CPA). The analysis is based on the hardness of lattice-based problems underlying NTRU-type cryptosystems and the randomness introduced through ephemeral sparse polynomials.

5.1. Security Assumptions

The security of the proposed scheme relies on the following assumptions:

i. The hardness of the NTRU Ring-Lattice Problem

The public key is computed as:

$$h = f^{-1}g \pmod{q}$$

where f and g are short controlled-support sparse polynomials. Recovering the private polynomial f from the public key h is assumed to be computationally infeasible for any probabilistic polynomial-time adversary. This assumption corresponds to the hardness of finding short vectors in the associated NTRU lattice.

ii. Randomness of Ephemeral Sparse Polynomial

For each encryption instance, a fresh polynomial:

$$r \leftarrow \text{SparsePoly}(E(\text{ctx}))$$

is generated from contextual entropy sources such as timestamps, GPS coordinates, or system identifiers. The polynomial r is assumed to be unpredictable and non-reusable.

iii. Correctness of Decryption

The parameters N, p, q are selected such that the noise generated during encryption remains within acceptable bounds. Consequently, the decryption procedure recovers the original message with overwhelming probability.

5.2. IND-CPA Security Analysis

The security of the proposed DRH-SNTRU scheme is constructed based on the hardness of the NTRU lattice problem. This section shows that the proposed scheme is IND-CPA secure under the hardness assumption of the underlying NTRU problem.

Theorem 1. *If there exists a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ that can break the IND-CPA security of the proposed DRH-SNTRU scheme with a non-negligible advantage ϵ , then there exists a PPT algorithm $\mathcal{B}$ that can solve the underlying NTRU lattice problem with an advantage of at least $\epsilon/2$.*

Proof. The proof is constructed using a reduction from the IND-CPA game of the DRH-SNTRU scheme to the hardness of the NTRU problem as below: $\square$

- **Init.** Let $\mathcal{A}$ be an IND-CPA adversary. The challenger generates system parameters using the Setup algorithm and provides the public key

$$h = f^{-1}g(\text{mod } q)$$

to the adversary $\mathcal{A}$.

- **Setup.** The simulator $\mathcal{B}$ receives an instance of the NTRU problem and sets:

$$\text{Public key : } PK = h \in R_q$$

The public parameters are then given to the adversary $\mathcal{A}$.

- **Phase 1.** The adversary $\mathcal{A}$ may issue polynomially many encryption queries. For each query, the simulator $\mathcal{B}$ responds by generating ciphertexts using:

$$e = r \cdot h + m(\text{mod } q)$$

where r is sampled as a fresh controlled-support sparse polynomial.

- **Challenge.** The adversary $\mathcal{A}$ submits two equal-length plaintexts

$$m_0, m_1 \in R_p.$$

The challenger randomly selects a bit $b \in \{0, 1\}$, generates a fresh ephemeral polynomial r^* , and computes the challenge ciphertext:

$$e^* = r^* \cdot h + m_b(\text{mod } q).$$

The ciphertext e^* is returned to $\mathcal{A}$.

- **Phase 2.** The adversary continues to issue encryption queries as in Phase 1, except that it cannot query the challenge ciphertext.
- **Guess.** Finally, the adversary outputs a guess $b' \in \{0, 1\}$. The advantage of $\mathcal{A}$ is defined as:

$$\text{Adv}_{\mathcal{A}}^{\text{IND-CPA}} = | \Pr[b' = b] - \frac{1}{2} |.$$

The security of the scheme relies on the indistinguishability of the masking term:

$$r \cdot h(\text{mod } q)$$

- If the public key h is derived from valid NTRU parameters, then $r \cdot h$ behaves as a structured lattice-based masking term.
- If h is replaced by a uniformly random polynomial in R_q , then $r \cdot h$ is computationally indistinguishable from random.

If an adversary $\mathcal{A}$ can distinguish between encryptions of m_0 and m_1 , then it can distinguish whether h is a valid NTRU public key or a random element in R_q . This implies that $\mathcal{B}$ can use $\mathcal{A}$ to solve the underlying NTRU problem. Thus, if $\mathcal{A}$ has a non-negligible advantage ϵ , then $\mathcal{B}$ can solve the NTRU problem with an advantage of at least $\epsilon/2$:

$$\text{Adv}_{\mathcal{B}} = \frac{1}{2} \cdot \text{Adv}_{\mathcal{A}}$$

Therefore, under the hardness assumption of the NTRU lattice problem and the unpredictability of the controlled-support sparse polynomial r , the proposed DRH-SNTRU scheme is IND-CPA secure.

6. Performance Analysis and Discussion

This section presents a comprehensive performance evaluation of the proposed Double-Ring Hybrid Sparse NTRU (DRH-SNTRU) framework through both theoretical complexity analysis and experimental benchmarking. The proposed scheme is evaluated against Standard NTRUEncrypt [17], NTRU-HRSS [19], and Ring-LWE Encryption [19] schemes to analyze computational efficiency, scalability, ciphertext evaluation overhead, and storage requirements for post-quantum Internet of Vehicles (IoV) communication systems.

To ensure methodological consistency and an unbiased comparative evaluation, all cryptographic schemes were implemented and benchmarked under an identical experimental environment using Python 3.13.5 on a Linux-based platform equipped with 56 logical CPU cores and 4 GB RAM. The evaluation framework measures setup time, key generation time, encryption time, decryption time, ciphertext evaluation overhead, and key/ciphertext storage efficiency across polynomial dimensions $N = 512, 1024, 2048, 4096$, and 8192 . Each experiment was executed repeatedly over multiple iterations to minimize transient system fluctuations, and the reported results correspond to the average execution time measured in nanoseconds (ns). The observed performance variance and error margins across repeated executions remained consistently low, indicating stable benchmarking behavior and reliable computational measurements. This stability is primarily attributed to the deterministic characteristics of lattice-based polynomial arithmetic, modular reduction, and sparse convolution operations employed throughout the evaluated schemes.

6.1. Theoretical and Algorithmic Complexity Analysis

The computational complexity analysis of lattice-based cryptographic schemes primarily depends on the efficiency of polynomial arithmetic operations. Conventional NTRUEncrypt and NTRU-HRSS schemes rely heavily on dense polynomial multiplication and inversion operations within a single polynomial ring. The computational complexity of the proposed DRH-SNTRU scheme can be analyzed according to its four main phases: setup, key generation, encryption, and decryption as summarized in Tables 2 and 3.

Table 2. Computational Complexity Comparison of Lattice-Based Encryption Schemes with Classical Polynomial Arithmetic.

Scheme	Setup	KeyGen	Encrypt	Decrypt
Standard NTRUEncrypt [17]	$O(1)$	$O(N^2)$	$O(N^2)$	$O(N^2)$
NTRU-HRSS [20]	$O(1)$	$O(N^2)$	$O(N^2)$	$O(N^2)$
Ring-LWE PKE [19]	$O(1)$	$O(kN^2)$	$O(kN^2)$	$O(kN^2)$
Proposed DRH-SNTRU	$O(1)$	$O(N^2)$	$O(dN)$	$O(dN)$
Proposed DRH-SNTRU Eval	—	—	$O(N)$	$O(N)$

Table 3. Computational Complexity Comparison of Lattice-Based Encryption Schemes with Fast Polynomial Arithmetic.

Scheme	KeyGen	Encrypt	Decrypt
Standard NTRUEncrypt [17]	$O(N \log N)$	$O(N \log N)$	$O(N \log N)$
NTRU-HRSS [20]	$O(N \log N)$	$O(N \log N)$	$O(N \log N)$
Ring-LWE PKE [19]	$O(kN \log N)$	$O(kN \log N)$	$O(kN \log N)$
Proposed DRH-SNTRU	$O(N \log N)$	$O(dN)$	$O(dN)$

In addition to asymptotic Big-O complexity, the computational cost of the proposed DRH-SNTRU scheme can also be expressed in terms of the number of dominant polynomial operations required in each phase. As polynomial multiplication is the most expensive operation in lattice-based cryptography, the analysis as summarized in Table 4 provides a clearer practical view of algorithm efficiency. Let:

Table 4. Operation Cost Comparison in Terms of Dominant Polynomial Operations.

Scheme	KeyGen	Encrypt	Decrypt	Remarks
Standard NTRUEncrypt [17]	$1I + 1M_s + 1R$	$1I + 1A + 1R$	$1M_s + 2R$	Efficient, but no double-ring separation
NTRU-HRSS [20]	$1I + 1M_s + 1R$	$1I + 1A + 1R$	$1M_s + 2R$	Similar operation profile, better standardized reliability
Ring-LWE PKE [19]	multiple M_d + additions	multiple M_d + additions	multiple M_d + reductions	Higher computational cost due to dense operations
Proposed DRH-SNTRU	$1I + 1M_s + 1R$	$1I + 1A + 1R$	$1M_s + 2R$	Sparse structure and lightweight protocol suitability

- M_s : cost of one sparse–dense polynomial multiplication
- M_d : cost of one dense polynomial multiplication
- I : cost of one polynomial inversion
- A : cost of one polynomial addition
- R : cost of one modular reduction

In terms of dominant polynomial operations, the proposed DRH-SNTRU scheme requires one polynomial inversion and one polynomial multiplication during key generation, one sparse–dense polynomial multiplication during encryption, and one sparse–dense polynomial multiplication during decryption. Specifically, its operation cost can be expressed as $1I + 1M_s + 1R$ for key generation, $1M_s + 1A + 1R$ for encryption, and $1M_s + 2R$ for decryption. Compared with Ring-LWE-based encryption schemes, which typically require multiple dense polynomial multiplications, the proposed scheme is computationally lighter and therefore more suitable for resource-constrained Internet of Vehicles environments.

6.2. Computation Analysis and Scalability Discussion

Practical deployment suitability is a critical requirement for post-quantum IoV cryptographic systems because vehicular communication environments involve highly dynamic network topology, strict latency requirements, and resource-constrained On-Board Units (OBUs). Consequently, cryptographic schemes with excessive computational overhead or large storage requirements may become impractical for real-time vehicular applications. Table 5 presents the detailed computational performance benchmark of the proposed DRH-SNTRU framework across polynomial dimensions ranging from $N = 512$ to $N = 8192$.

Table 5. Computational Performance Benchmark of the Proposed DRH-SNTRU Framework Across Different Polynomial Dimensions.

Polynomial Dimension (N)	Setup Time (ns)	Key Generation Time (ns)	Encryption Time (ns)	Decryption Time (ns)	Ciphertext Evaluation Time (ns)
512	1711.7	1,722,325	110,816.90	29,547.97	3905.52
1024	1695.54	3,761,024	210,545.50	47,534.59	5274.67
2048	2098.18	8,281,560	500,703.10	82,842.01	7603.90
4096	1971.25	17,482,528	1,409,017	150,407.50	11,392.50
8192	2891.65	39,454,356	4,723,823	305,635.50	20,282.07

The evaluation includes setup time, key generation time, encryption time, decryption time, and ciphertext evaluation overhead, providing a comprehensive analysis of the scalability behavior and runtime efficiency of the proposed post-quantum cryptographic architecture. The setup phase demonstrates consistently low initialization overhead across all evaluated dimensions. The setup time remains below 3 μ s even at the highest polynomial dimension ($N = 8192$), increasing only moderately from 1711.7 ns at $N = 512$ to 2891.65 ns at $N = 8192$. This behavior indicates that the initialization complexity of DRH-SNTRU is relatively insensitive to lattice dimension growth. The low setup overhead is primarily attributed to the lightweight sparse polynomial initialization process and efficient parameter generation within the double-ring structure. Such characteristics are highly beneficial for real-time vehicular communication systems, where rapid session initialization and low authentication latency are essential operational requirements. The key generation results reveal the expected scalability trend associated with lattice-based cryptographic systems. As the polynomial dimension increases, the key generation cost rises significantly, growing from approximately 1.72 ms at $N = 512$ to 39.45 ms at $N = 8192$. This increase is mainly caused by the higher computational complexity of polynomial inversion, sparse coefficient generation, and modular arithmetic operations in larger lattice spaces. Nevertheless, the observed growth remains computationally manageable and follows a predictable scaling pattern. The results indicate that the proposed DRH-SNTRU framework preserves stable

key generation behavior even at high security parameters, demonstrating suitability for scalable post-quantum deployment scenarios.

The encryption performance analysis highlights the efficiency of the sparse polynomial structure employed by the proposed framework. At lower polynomial dimensions, DRH-SNTRU achieves highly efficient encryption performance, requiring only 110,816.90 ns at $N = 512$ and 210,545.50 ns at $N = 1024$. The increase in encryption time remains gradual up to $N = 2048$, after which the computational cost becomes more pronounced due to the larger convolution space and additional ciphertext integrity processing within the dual-ring architecture. At the largest evaluated dimension ($N = 8192$), the encryption latency reaches approximately 4.72 ms. Although the encryption cost increases substantially at higher dimensions, the runtime remains practical for secure vehicular communication applications, especially considering the enhanced ciphertext validation and sparse support verification integrated into the framework. The results therefore confirm that the proposed sparse polynomial mapping effectively reduces convolution density and arithmetic complexity during encryption operations. The decryption phase demonstrates one of the most significant strengths of the DRH-SNTRU framework. Across all evaluated dimensions, decryption time remains substantially lower than encryption time, increasing from 29,547.97 ns at $N = 512$ to only 305,635.50 ns at $N = 8192$. This comparatively moderate growth indicates that the sparse polynomial recovery mechanism successfully minimizes modular convolution overhead during ciphertext reconstruction. The separation of polynomial operations within the double-ring structure further reduces redundant arithmetic processing, thereby improving decryption efficiency. From a practical perspective, this characteristic is particularly advantageous for Internet of Vehicles (IoV) environments, where rapid message verification and low response latency are critical for safety-sensitive communication and real-time vehicular decision-making.

An additional feature evaluated in Table 5 is the ciphertext evaluation mechanism integrated into DRH-SNTRU. Unlike conventional lattice-based encryption schemes, the proposed framework incorporates a dedicated ciphertext evaluation stage to detect malformed ciphertexts, replay attempts, and structurally inconsistent polynomial mappings before decryption. The evaluation overhead increases gradually from 3905.52 ns at $N = 512$ to 20,282.07 ns at $N = 8192$. Despite introducing an additional verification phase, the computational cost remains relatively small compared with the total encryption and decryption latency. This demonstrates that enhanced ciphertext validation can be achieved without imposing excessive runtime penalties. The inclusion of this lightweight evaluation mechanism significantly strengthens robustness against active adversarial attacks while preserving practical deployment feasibility.

Overall, the experimental findings presented in Table 5 validate the computational efficiency and scalability of the proposed DRH-SNTRU framework. Although key generation and encryption costs increase with polynomial dimension, the framework maintains low setup overhead, highly efficient decryption performance, and lightweight ciphertext evaluation complexity. The observed performance trends further support the theoretical complexity analysis, where the controlled-support sparse polynomial structure reduces arithmetic density and improves scalability behavior compared with conventional dense polynomial operations. Consequently, the proposed DRH-SNTRU framework demonstrates strong potential for deployment in real-time, resource-constrained, and quantum-resistant communication environments such as IoV, intelligent transportation systems, and vehicular edge computing infrastructures.

Subsequently, we conducted experiments to evaluate the computational behavior and scalability of the proposed DRH-SNTRU scheme across increasing polynomial dimensions $N = 512$ to $N = 8192$. The proposed framework was benchmarked against Standard

NTRUEncrypt, NTRU-HRSS, and Ring-LWE Encryption to evaluate setup overhead, key generation efficiency, encryption performance, decryption scalability, and ciphertext evaluation cost under post-quantum cryptographic environments relevant to Internet of Vehicles (IoV) systems. The setup time analysis shown in Figure 1 demonstrates that the proposed DRH-SNTRU maintains relatively low initialization overhead despite introducing a double-ring algebraic structure and sparse coefficient validation mechanism. At $N = 512$, DRH-SNTRU records a setup cost of approximately 1711.7 ns, increasing moderately to 2891.65 ns at $N = 8192$. Although this overhead is slightly higher than Standard NTRUEncrypt and NTRU-HRSS, which remain below 2600 ns at all dimensions, the difference is computationally negligible in practical deployments because setup operations are executed infrequently. More importantly, DRH-SNTRU exhibits substantially lower setup complexity than Ring-LWE Encryption, which reaches approximately 34,871.45 ns at $N = 8192$. This behavior highlights the efficiency advantage of sparse polynomial initialization compared with dense Ring-LWE parameter generation. The reduced initialization complexity is particularly beneficial for lightweight vehicular devices operating under constrained computational and energy budgets.

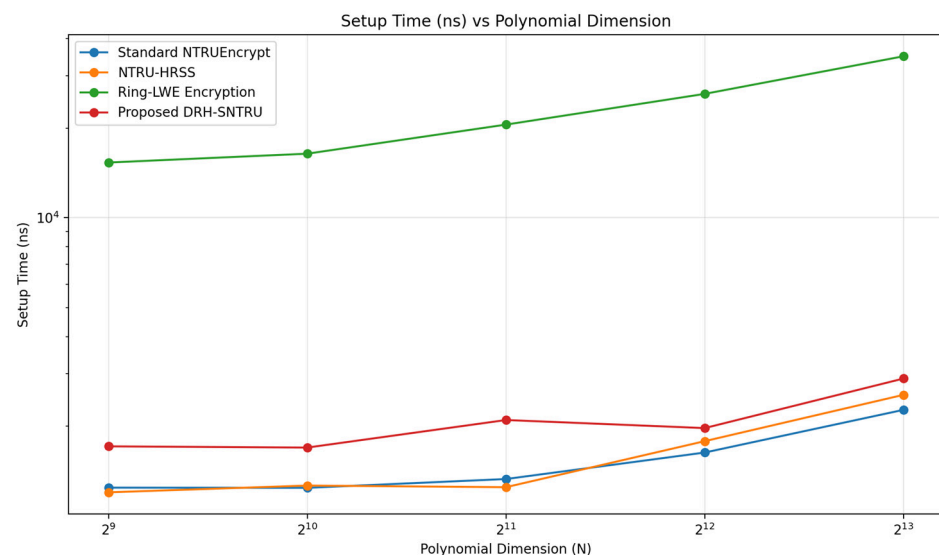


Figure 1. Setup Time Comparison of Lattice-Based Encryption Schemes across Polynomial Dimensions.

The key generation results in Figure 2 reveal that all schemes experience substantial growth in computational cost as the lattice dimension increases. This trend is expected because polynomial inversion and modular arithmetic operations become increasingly expensive in higher-dimensional lattices. Standard NTRUEncrypt increases from approximately 1.73 ms at $N = 512$ to 36.54 ms at $N = 8192$, while NTRU-HRSS follows a nearly identical pattern, reaching 35.86 ms at the largest dimension. The proposed DRH-SNTRU exhibits comparable scalability behavior, increasing from 1.72 ms to 39.45 ms across the same range. The slightly higher key generation overhead observed in DRH-SNTRU originates from the additional entropy filtering, sparse support verification, and dual-ring synchronization mechanisms integrated into the framework. Nevertheless, the increase remains moderate relative to the additional security-oriented functionality introduced by the proposed design. In contrast, Ring-LWE Encryption demonstrates significantly lower key generation latency, remaining below 0.60 ms even at $N = 8192$. However, this computational advantage is accompanied by substantially larger polynomial structures, higher memory consumption, and increased ciphertext overhead, which may reduce practicality in resource-constrained IoV infrastructures.

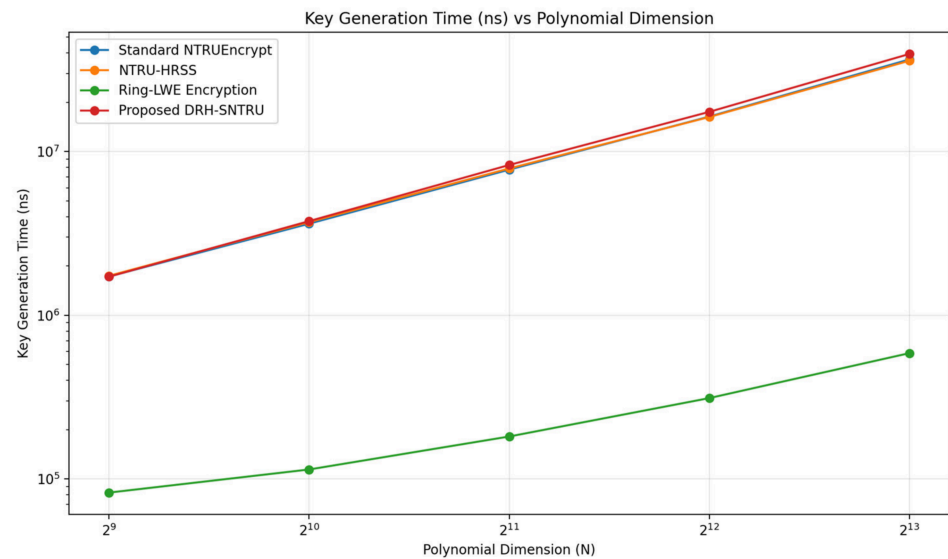


Figure 2. Key Generation Time Comparison across Different Polynomial Dimensions.

The encryption performance illustrated in Figure 3 provides important insight into the runtime scalability of the proposed framework. At smaller dimensions, DRH-SNTRU achieves highly competitive encryption performance due to the use of controlled-support sparse polynomial multiplication. Specifically, DRH-SNTRU records approximately 110,816.92 ns at $N = 512$, outperforming Standard NTRUEncrypt (204,855.96 ns) and NTRU-HRSS (200,490.61 ns). Similar improvements remain visible at $N = 1024$ and $N = 2048$, where the sparse polynomial structure effectively reduces convolution density and coefficient processing complexity. However, as the polynomial dimension increases further, the encryption overhead of DRH-SNTRU rises more rapidly than the conventional NTRU variants.

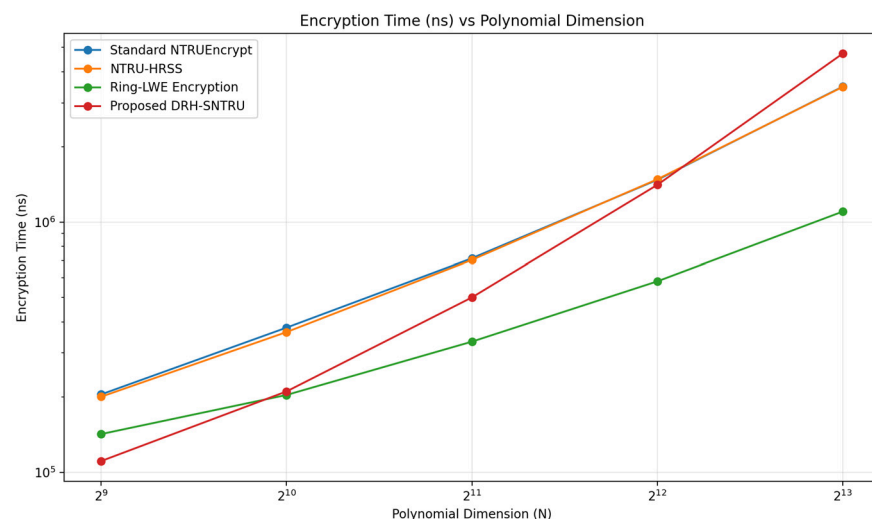


Figure 3. Encryption Time Comparison of Lattice-Based Cryptographic Schemes.

At $N = 8192$, the proposed framework records approximately 4,723,823.45 ns, exceeding both Standard NTRUEncrypt and NTRU-HRSS. This increase is primarily attributed to the additional ciphertext evaluation preparation, double-ring mapping operations, and sparse integrity verification mechanisms incorporated into the encryption pipeline. Despite this increase, the encryption latency remains within the practical range for real-time vehicular communication systems, particularly considering the additional security guarantees

introduced by the proposed architecture. Meanwhile, Ring-LWE Encryption consistently demonstrates the lowest encryption latency across all dimensions, achieving approximately 1,101,360 ns at $N = 8192$. This result confirms the efficiency of optimized Ring-LWE polynomial arithmetic; however, the trade-off appears in larger parameter sizes and denser ciphertext structures.

The decryption analysis shown in Figure 4 represents one of the most significant advantages of the proposed DRH-SNTRU framework. Across all evaluated polynomial dimensions, DRH-SNTRU consistently achieves lower decryption latency than Standard NTRUEncrypt and NTRU-HRSS.

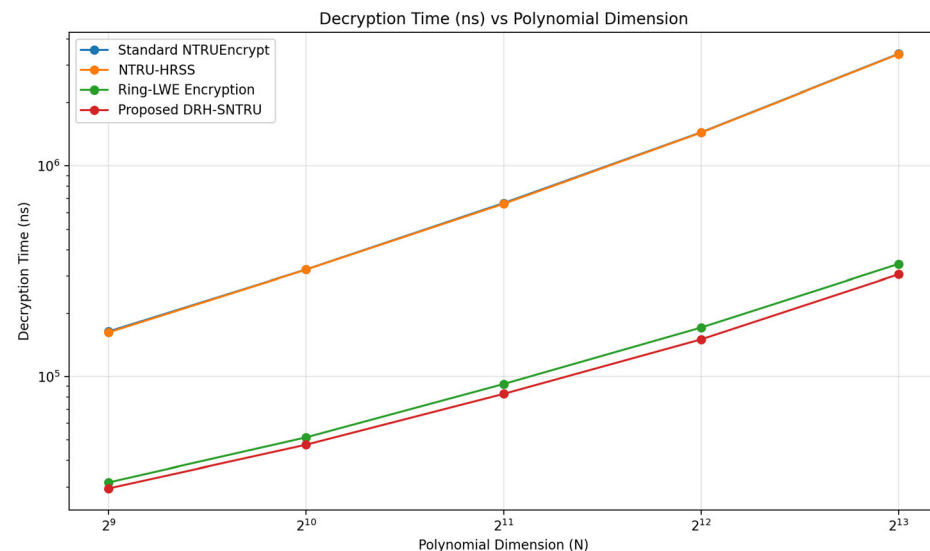


Figure 4. Decryption Time Comparison across Increasing Polynomial Dimensions.

At $N = 512$, DRH-SNTRU records approximately 29,547.97 ns, compared with 164,014.9 ns for Standard NTRUEncrypt and 162,473.4 ns for NTRU-HRSS. This improvement becomes even more pronounced at larger dimensions. At $N = 8192$, the proposed framework achieves approximately 305,635.5 ns, whereas Standard NTRUEncrypt and NTRU-HRSS both exceed 3.3 ms. The substantial reduction in decryption overhead can be attributed to the sparse polynomial recovery process and reduced modular convolution complexity enabled by the controlled-support coefficient structure. Furthermore, the separation of message and key processing within the dual-ring architecture minimizes redundant arithmetic operations during ciphertext reconstruction. In practical IoV deployments where authentication latency and rapid response time are critical for safety-sensitive communication, such decryption efficiency provides a substantial operational advantage. Although Ring-LWE Encryption demonstrates relatively low decryption overhead compared to conventional NTRU schemes, DRH-SNTRU consistently achieves lower latency at all evaluated dimensions.

The ciphertext evaluation results presented in Figure 5 introduce an additional security-performance consideration absent in the benchmark schemes. DRH-SNTRU incorporates a dedicated ciphertext evaluation stage designed to detect malformed ciphertexts, replay attempts, and structurally inconsistent polynomial mappings prior to decryption. As expected, this additional verification mechanism introduces measurable computational overhead. The evaluation latency increases gradually from approximately 3905.52 ns at $N = 512$ to 20,282.07 ns at $N = 8192$. While this overhead is larger than the lightweight evaluation observed in Standard NTRUEncrypt, NTRU-HRSS, and Ring-LWE Encryption, the absolute cost remains relatively small compared with the total encryption and decryption latency. More importantly, the inclusion of a dedicated ciphertext evaluation

mechanism significantly enhances robustness against active adversarial attacks, particularly replay-based and malformed ciphertext injection attacks commonly encountered in highly dynamic vehicular communication environments.

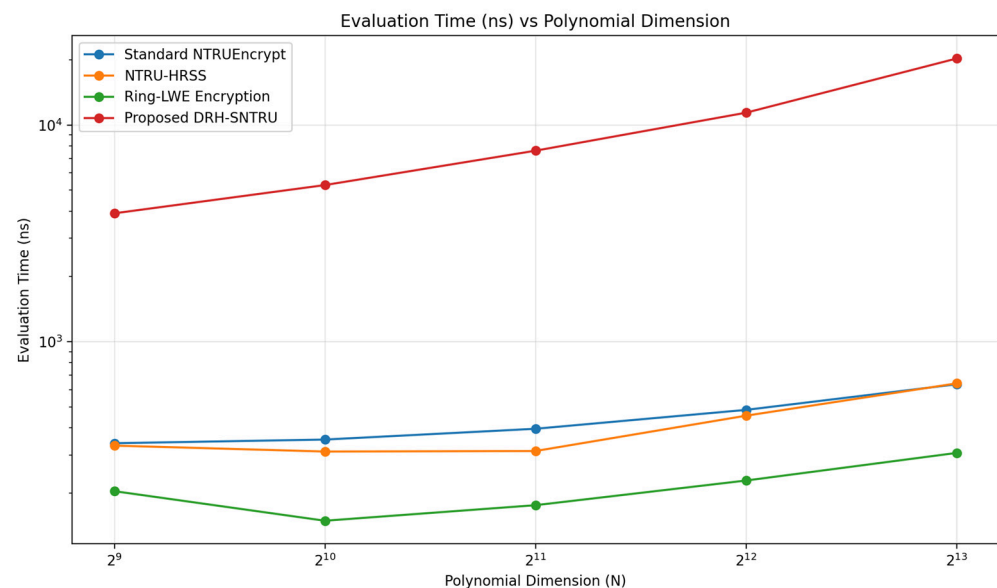


Figure 5. Ciphertext Evaluation Time Comparison across Increasing Polynomial Dimensions.

From a scalability perspective, the experimental findings strongly validate the theoretical complexity analysis presented earlier. Standard NTRUEncrypt and NTRU-HRSS exhibit rapid growth in encryption and decryption overhead due to dense polynomial multiplication complexity approaching $O(N^2)$ under practical implementations. Ring-LWE Encryption demonstrates superior computational efficiency in several operations because of optimized polynomial arithmetic and structured ring operations; however, this benefit is achieved at the expense of larger parameter representations and higher initialization overhead. In contrast, DRH-SNTRU achieves a more balanced computational profile by exploiting sparse polynomial multiplication behavior, approximating $O(dN)$, where $d \ll N$. This allows the framework to maintain highly efficient decryption performance while preserving acceptable encryption scalability and enhanced ciphertext validation capability.

In a nutshell, the results demonstrate that the proposed DRH-SNTRU framework achieves an effective balance between lightweight computation, scalability, ciphertext integrity protection, and post-quantum security robustness. Although the framework introduces moderate overhead during key generation and large-dimensional encryption, these costs are compensated by substantial improvements in decryption efficiency, lower setup complexity compared with Ring-LWE systems, and the integration of additional ciphertext evaluation mechanisms. The findings therefore indicate that DRH-SNTRU is particularly suitable for real-time and resource-constrained post-quantum IoV environments, where low decryption latency, lightweight polynomial operations, and resistance against active ciphertext manipulation are essential requirements.

6.3. Storage Efficiency Analysis and Discussion

We also conducted storage efficiency analysis to provide important insights into the practical deployment feasibility of the proposed DRH-SNTRU framework in comparison with Standard NTRUEncrypt, NTRU-HRSS, and Ring-LWE Encryption. The evaluation focuses on three critical storage-related metrics, namely public key size, private key size, and ciphertext size, across lattice dimensions ranging from $N = 512$ to $N = 8192$. These metrics are particularly important in Internet of Vehicles (IoV) environments because

vehicular communication systems operate under strict bandwidth, memory, and latency constraints. Consequently, schemes with lower storage overhead are generally more suitable for real-time post-quantum communication infrastructures.

The public key size comparison shown in Figure 6 indicates that the proposed DRH-SNTRU maintains nearly identical public key sizes to Standard NTRUEncrypt and NTRU-HRSS across all polynomial dimensions. Specifically, the public key grows linearly from 4096 bytes at $N = 512$ to 65,536 bytes at $N = 8192$. This behavior demonstrates that the introduction of the dual-ring architecture does not significantly inflate the public parameter representation. In contrast, Ring-LWE Encryption consistently produces substantially larger public keys, beginning at 8192 bytes for $N = 512$ and increasing to 131,072 bytes at $N = 8192$. The public key overhead of Ring-LWE is therefore approximately twice that of the NTRU-based schemes at every evaluated dimension. This increase originates from the dense polynomial representation and higher-dimensional coefficient structures required in Ring-LWE constructions. From a deployment perspective, larger public keys directly increase transmission overhead during session establishment and authentication exchanges, which may negatively impact highly dynamic vehicular networks where communication latency and bandwidth efficiency are critical.

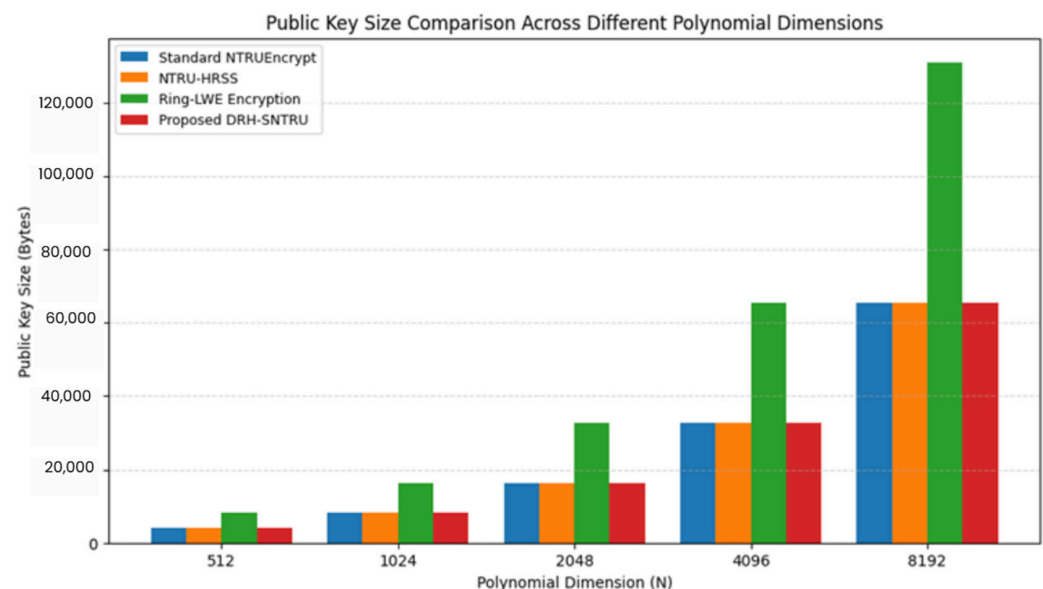


Figure 6. Public Key Efficiency Comparison Across Different Polynomial Dimensions.

The private key storage results illustrated in Figure 7 reveal one of the most important characteristics of the proposed DRH-SNTRU framework. At the smallest dimension ($N = 512$), DRH-SNTRU records a private key size of approximately 7999 bytes, which is nearly identical to Standard NTRUEncrypt (7985 bytes) and NTRU-HRSS (8001 bytes). However, beginning from $N = 1024$, the private key size of DRH-SNTRU collapses to only 117 bytes and remains constant for all larger dimensions. A similar pattern is observed for NTRU-HRSS (119 bytes) and Standard NTRUEncrypt (103 bytes). This dramatic reduction demonstrates the effectiveness of sparse polynomial support representation, where only compact coefficient location information must be stored instead of dense polynomial vectors. The scalability advantage becomes substantially clearer when compared with Ring-LWE Encryption. Unlike the sparse NTRU-based schemes, Ring-LWE private key sizes grow linearly with the polynomial dimension, increasing from 4096 bytes at $N = 512$ to 65,536 bytes at $N = 8192$. Consequently, the proposed DRH-SNTRU achieves several orders of magnitude lower private key storage overhead at large lattice dimensions. This characteristic is highly beneficial for embedded vehicular hardware and resource-constrained

onboard units, where secure storage capacity is limited and low-memory cryptographic deployment is essential. Another important implication of the compact private key structure is reduced memory access overhead during cryptographic operations. Since fewer coefficients participate in secret key reconstruction and sparse convolution processing, DRH-SNTRU benefits not only from lower storage requirements but also from improved decryption efficiency, as demonstrated previously in the computational benchmarking results. This dual optimization effect highlights the synergy between sparse polynomial design and lightweight post-quantum cryptographic implementation.

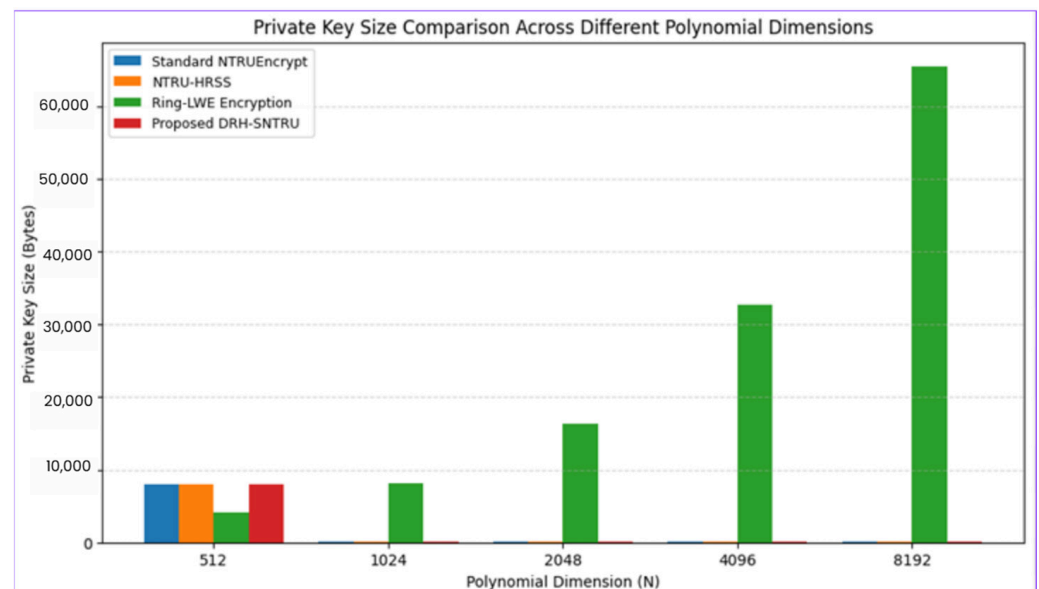


Figure 7. Private Key Efficiency Comparison Across Different Polynomial Dimensions.

The ciphertext size comparison in Figure 8 further reinforces the storage efficiency of the proposed framework. DRH-SNTRU maintains ciphertext sizes identical to Standard NTRUEncrypt and NTRU-HRSS across all polynomial dimensions, increasing linearly from 4096 bytes to 65,536 bytes. This result confirms that the additional double-ring mapping and sparse support validation mechanisms do not introduce ciphertext expansion penalties. Maintaining compact ciphertexts is particularly important in IoV communication because vehicular systems continuously exchange encrypted safety messages, cooperative awareness packets, and authentication tokens under strict latency constraints. In comparison, Ring-LWE Encryption again exhibits significantly larger ciphertext sizes, reaching 131,072 bytes at $N = 8192$, which doubles the communication payload relative to the NTRU-based schemes. Such ciphertext expansion can substantially increase bandwidth consumption, retransmission probability, and communication delay in highly congested vehicular environments. Consequently, although Ring-LWE demonstrates attractive computational characteristics in certain arithmetic operations, its communication overhead may limit practicality for large-scale real-time deployment scenarios.

From a scalability perspective, all schemes demonstrate predictable linear growth in public key and ciphertext sizes as the polynomial dimension increases. However, the proposed DRH-SNTRU maintains a significantly more balanced trade-off between computational complexity and storage overhead. The sparse polynomial representation enables compact key storage while preserving scalable ciphertext behavior and efficient arithmetic operations. This balance becomes increasingly important as future post-quantum security levels demand larger lattice dimensions to resist advanced quantum attacks. Overall, the storage evaluation confirms that the proposed DRH-SNTRU framework achieves strong storage efficiency without sacrificing scalability or structural security robustness.

Compared with Ring-LWE Encryption, DRH-SNTRU significantly reduces public key, private key, and ciphertext overhead while maintaining compact parameter representation equivalent to conventional NTRU-based schemes. The results therefore demonstrate that DRH-SNTRU is highly suitable for real-time post-quantum IoV infrastructures, where lightweight storage, reduced communication overhead, scalable deployment, and efficient cryptographic processing are essential operational requirements.

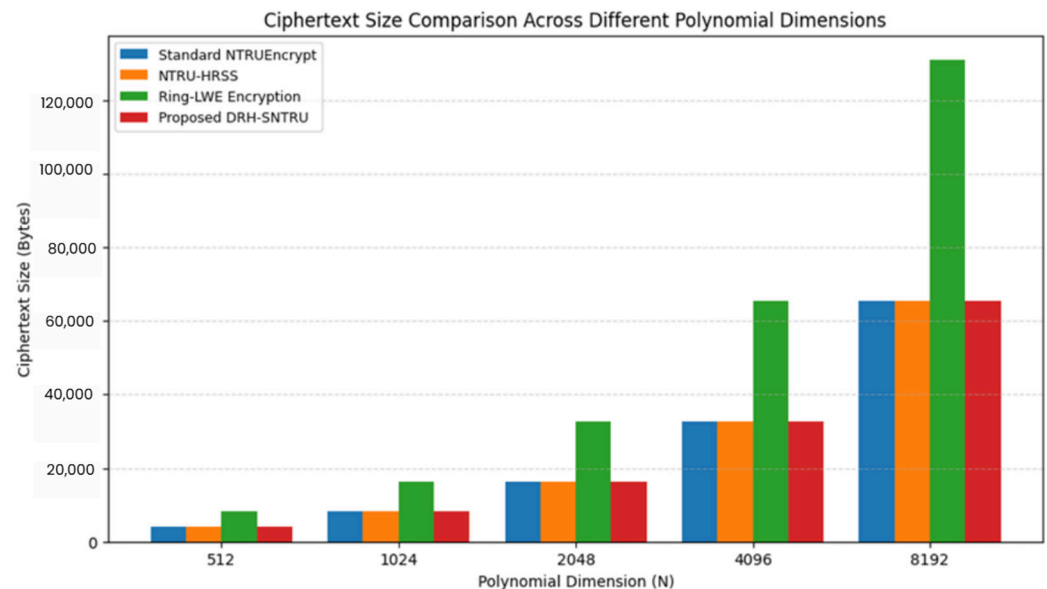


Figure 8. Ciphertext Storage Efficiency Comparison Across Different Polynomial Dimensions.

7. Conclusions

This paper introduced a novel Double-Ring Hybrid Sparse NTRU (DRH-SNTRU) scheme as a lightweight and quantum-resistant solution for securing communication in Internet of Vehicles environments. The design specifically focuses on addressing the practical challenges of vehicular systems, where cryptographic schemes must simultaneously provide strong post-quantum security, low computational overhead, reduced storage complexity, and real-time operational capability. By integrating controlled-support sparse polynomial structures with a dual-ring lattice architecture, the proposed scheme successfully reduces arithmetic complexity while preserving strong randomness and lattice hardness properties.

The introduction of the double-ring structure enables the separation of key-related operations from message-processing functions, thereby improving structural isolation and minimizing potential leakage pathways commonly associated with conventional single-ring lattice constructions. Furthermore, the use of context-driven ephemeral key generation enhances session independence and forward secrecy, ensuring that the compromise of long-term secret keys does not expose previously transmitted ciphertexts. In addition, the optional ciphertext evaluation mechanism strengthens the robustness of the framework against replay attacks, malformed ciphertext injection, and adversarial manipulation by filtering invalid ciphertexts prior to the decryption phase.

From the security perspective, the proposed DRH-SNTRU framework achieves IND-CPA security under the hardness assumption of the NTRU lattice problem, while the integration of the ciphertext validation mechanism provides a practical foundation for extending resistance against adaptive chosen-ciphertext attacks (CCA). The combination of sparse polynomial mapping and hybrid ring separation further increases structural

complexity for adversaries while maintaining lightweight operational behavior suitable for constrained vehicular devices.

Extensive computational benchmarking and storage analysis demonstrate that the proposed scheme achieves a highly balanced trade-off between security robustness and computational efficiency. The experimental results show that DRH-SNTRU maintains low setup overhead, highly efficient decryption performance, compact key and ciphertext representation, and scalable runtime behavior across polynomial dimensions ranging from $N = 512$ to $N = 8192$. Compared with conventional NTRUEncrypt, NTRU-HRSS, and Ring-LWE Encryption schemes, DRH-SNTRU exhibits particularly strong advantages in decryption efficiency, sparse private key representation, and storage scalability, while preserving practical encryption performance for real-time communication environments.

Overall, the proposed DRH-SNTRU framework demonstrates strong potential as a practical lightweight post-quantum cryptographic solution for future intelligent transportation systems, vehicular edge computing, and autonomous V2X communication infrastructures. The findings indicate that sparse lattice-based architectures combined with hybrid ring separation can provide an effective pathway toward scalable, secure, and resource-efficient post-quantum communication systems.

Future work may focus on extending the proposed framework toward full IND-CCA2 secure constructions, hardware-level optimization on embedded vehicular platforms, FPGA and ASIC acceleration, integration with 5G/6G-enabled V2X architectures, and formal resistance analysis against side-channel and fault-injection attacks. In addition, further exploration of adaptive sparse polynomial distributions and hybrid lattice optimization strategies may provide additional improvements in both security strength and computational scalability for next-generation quantum-resistant vehicular communication systems.

Author Contributions: Conceptualization, S.F.T. and W.W.; methodology, S.F.T. and W.W.; validation, S.F.T. and W.W.; formal analysis, S.F.T. and W.W.; investigation, S.F.T. and W.W.; writing—original draft preparation W.W. and S.F.T.; writing—review and editing, W.W. and S.F.T.; visualization, G.-C.C.; supervision, S.F.T.; project administration S.F.T.; funding acquisition, S.F.T., W.W. and G.-C.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to confidentiality restrictions and because they involve proprietary research information of the authors' research group.

Acknowledgments: The authors gratefully acknowledge the reviewers for their insightful comments and constructive suggestions, which have significantly improved the quality of this work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Internet of Vehicles (IoV) Report 2025. Industry to Experience 21.4% CAGR Growth. *Yahoo Finance*. Available online: <https://finance.yahoo.com/news/internet-vehicles-iov-report-2025-132800934.html> (accessed on 7 October 2025).
2. Hakim, S.B.; Adil, M.; Ali, A.; Farouk, A.; Song, H.H. Internet of Vehicles Security Threats, Countermeasures, Open Challenges with Future Research Directions. *IEEE Internet Things J.* 2025, *in press*. [CrossRef]
3. He, C.; Wang, W.; Jiang, W.; He, Z.; Wang, J.; Xie, X. Security for the Internet of Vehicles with Integration of Sensing, Communication, Computing, and Intelligence: A Comprehensive Survey. *Sensors* **2025**, *25*, 5119. [CrossRef] [PubMed]
4. Alalwany, E.; Mahgoub, I. Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions. *Sensors* **2024**, *24*, 368. [CrossRef] [PubMed]
5. Tan, S.F.; Samsudin, A. Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey. *Sensors* **2021**, *21*, 6647. [CrossRef] [PubMed]

6. Xu, S.; Hu, X.; Zhang, X.; Li, K.; Liu, J.; Xie, Q.; Ren, J. Post-Quantum Anonymous, Traceable and Linkable Authentication Scheme Based on Blockchain for Intelligent Vehicular Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 12108–12119. [\[CrossRef\]](#)
7. Zhang, Z.; Cao, Z.; Wang, Y. Forensics System for Internet of Vehicles Based on Post-Quantum Blockchain. *Sensors* **2025**, *25*, 6038. [\[CrossRef\]](#) [\[PubMed\]](#)
8. Alsaadi, M.; Aldawsari, H.; Kasaraneni, B.P.; Alzahrani, A.; Alshamrani, A.; Alghamdi, T. Post-Quantum Verifiable Decryption for Secure and Scalable V2I Communication in Consumer Driven-Intelligent Transportation Systems. *IEEE Trans. Consum. Electron.* **2025**, *71*, 11248–11257. [\[CrossRef\]](#)
9. Shim, K.-A. A Survey on Post-Quantum Public-Key Signature Schemes for Secure Vehicular Communications. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 14025–14042. [\[CrossRef\]](#)
10. Prajapat, S.; Das, A.K.; Park, Y.; Lorenz, P. An Efficient Post-Quantum Lattice-Based Encryption Scheme for Secure Communication in Vehicular Ad-Hoc Networks. *IEEE Trans. Veh. Technol.* **2026**. [\[CrossRef\]](#)
11. Bhuvaneshwari, A.J.; Kaythry, P.; Kishore, R.; MuthuHarish, R. Post-Quantum Enhanced Ascon for Secure Vehicular IoT Data Integrity. *Sci. Rep.* **2025**, *15*, 26591. [\[CrossRef\]](#) [\[PubMed\]](#)
12. Zeydan, E.; Baranda, J.; Mangues-Bafalluy, J. Post-Quantum Blockchain-Based Secure Service Orchestration in Multi-Cloud Networks. *IEEE Access* **2022**, *10*, 129520–129530. [\[CrossRef\]](#)
13. Karakaya, A. A Novel Post-Quantum Lightweight Security Model and Directed Acyclic Graph Based Blockchain Integration for Mobile Cyber-Physical Systems. *Comput. Electr. Eng.* **2025**, *125*, 110415. [\[CrossRef\]](#)
14. Lohmiller, N.; Kaniewski, S.; Menth, M.; Heer, T. A Survey of Post-Quantum Cryptography Migration in Vehicles. *IEEE Access* **2025**, *13*, 10160–10176. [\[CrossRef\]](#)
15. Bhatt, H.; Rana, S.; Mittal, M. Post Quantum Based Identity Signature Scheme with Lattice Assumption for VANETs. In Proceedings of the 2024 IEEE 8th International Conference on Information and Communication Technology (CICT), Prayagraj UP, India, 6–8 December 2024. [\[CrossRef\]](#)
16. Wang, W.; Tan, S.F. Quantum Resistant Authentication and Key Agreement Protocol (AKA) for Autonomous Vehicle. In Proceedings of the 2025 5th International Conference on Neural Networks, Information and Communication Engineering (NNICE), Guangzhou, China, 10–12 January 2025. [\[CrossRef\]](#)
17. Hoffstein, J.; Pipher, J.; Silverman, J.H. NTRU: A Ring-Based Public Key Cryptosystem. In *Algorithmic Number Theory*; Buhler, J.P., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1998; Volume 1423, pp. 267–288. [\[CrossRef\]](#)
18. Bos, J.W.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Kyber and NTRUEncrypt. In *Submission to the NIST Post-Quantum Cryptography Standardization Project*. 2020. Available online: <https://eprint.iacr.org/2017/634.pdf> (accessed on 1 December 2025).
19. Lyubashevsky, V.; Peikert, C.; Regev, O. On Ideal Lattices and Learning with Errors over Rings. *J. ACM* **2013**, *60*, 1–43. [\[CrossRef\]](#)
20. Chen, C.; Danba, O.; Hoffstein, J.; Hülsing, A.; Rijneveld, J.; Schanck, J.; Schwabe, P.; Whyte, W.; Zhang, Z. NTRU Algorithm Specifications and Supporting Documentation. NIST Post-Quantum Cryptography Standardization Project. 2019. Available online: <https://ntru.org/f/ntru-20190330.pdf> (accessed on 1 December 2025).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.