






Article

Lattice-Based Lightweight Quantum Resistant Scheme in 5G-Enabled Vehicular Networks

Zeyad Ghaleb Al-Mekhlafi ¹, Mahmood A. Al-Shareeda ^{2,*}, Selvakumar Manickam ^{2,*},
Badia Abdulkarem Mohammed ¹ and Amjad Qtaish ¹

¹ College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia

² National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang 11800, Malaysia

* Correspondence: alshareeda022@usm.my (M.A.A.-S.); selva@usm.my (S.M.)

Abstract: Both security and privacy are central issues and need to be properly handled because communications are shared among vehicles in open channel environments of 5G-enabled vehicular networks. Several researchers have proposed authentication schemes to address these issues. Nevertheless, these schemes are not only vulnerable to quantum attacks but also use heavy operations to generate and verify signatures of messages. Additionally, these schemes need an expensive component RoadSide Unit (RSU)-aided scheme during the joining phase. To address these issues, we propose a lightweight quantum-resistant scheme according to the lattice method in 5G-enabled vehicular networks. Our proposal uses matrix multiplication instead of operations-based bilinear pair cryptography or operations-based elliptic curve cryptography to generate and verify signatures of messages shared among vehicles. Our proposal satisfies a significant reduction in performance, which makes it lightweight enough to handle quantum attacks. Our proposal is based on 5G technology without using any RSU-aided scheme. Security analysis showed that our proposal satisfies privacy and security properties as well as resists quantum attacks. Finally, our proposal also shows favorable performance compared to other related work.

Keywords: vehicular networks based on 5G; quantum attacks; lattice; bilinear pair cryptography; elliptic curve cryptography; security and privacy

MSC: 03G10; 06D05



Citation: Al-Mekhlafi, Z.G.;

Al-Shareeda, M.A.; Manickam, S.;

Mohammed, B.A.; Qtaish, A.

Lattice-Based Lightweight Quantum

Resistant Scheme in 5G-Enabled

Vehicular Networks. *Mathematics*

2023, 11, 399. [https://doi.org/](https://doi.org/10.3390/math11020399)

10.3390/math11020399

Academic Editor: Dmitry Makarov

Received: 7 December 2022

Revised: 30 December 2022

Accepted: 11 January 2023

Published: 12 January 2023



Copyright: © 2023 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article

distributed under the terms and

conditions of the Creative Commons

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

[creativecommons.org/licenses/by/](https://creativecommons.org/licenses/by/4.0/)

4.0/).

1. Introduction

5G-enabled vehicular networks play an important role in Intelligent Transportation Systems (ITSs) by providing safe road environments to drivers and passengers [1–3]. The use and evolution of 5G cellular systems, supported by significant government development in many countries, is the most recent trend in the development of wireless communication technologies [4,5]. Due to the characteristics of 5G, which boosts node information per unit region by 1 k times with a broadcast rate as high as 10 Gbps, a 5G network satisfies a multiple-fold improvement in velocity compared to existing 4G systems [6,7]. Additionally, 5G reduces latency by five times and doubles battery life, which creates a wealth of opportunities for vehicular networks [8,9].

In an intelligent vehicle, a wireless device called an OnBoard Unit (OBU) is installed to generate, broadcast, and obtain information among other participating vehicles. This information includes its speed, direction, traffic status, road condition, etc. Since the message is shared among vehicles in open channel environments of 5G-enabled vehicular networks, both safety and preserving are central issues that need to be properly handled [10–12]. Hence, many researchers have proposed authentication schemes to address these issues. However, their work is not only vulnerable to quantum attacks but also uses heavy operations (e.g., cryptographies of bilinear pairs and elliptic curves) to generate and verify

signatures of the message. Additionally, their work needs an expensive component Road-Side Unit (RSU)-aided scheme during the joining phase [13,14].

To resolve this issue, we propose a lightweight quantum-resistant scheme based on the lattice method in 5G-enabled vehicular networks. Our proposal uses matrix multiplication instead of operations-based bilinear pair cryptography or operations-based elliptic curve cryptography to generate and verify signatures of messages shared among vehicles. The main contributions of our proposal are as follows.

- We propose a lightweight quantum-resistant scheme based on the lattice method in 5G-enabled vehicular networks.
- Our proposal uses matrix multiplication to generate and verify signatures of messages shared among vehicles.
- Without using any RSU-aided scheme, our proposal is based on 5G technology that has the responsibility to connect the TA and vehicles within its wide-range communication domain by using the 5G standard.
- Based on the hardness of SIS/ISIS problems, our proposal achieves strong security against adversaries under the random oracle model.
- Security analysis showed that our proposal satisfies privacy and security properties as well as resisting quantum attacks.
- Our proposal satisfies a significant reduction in the performance, which makes it lightweight enough to handle quantum attacks.

The rest of this paper is arranged as follows. Section 2 highlights the limitations of the previous existing works. Section 3 introduces the preliminaries of this paper. We provide the five phases of our proposal in Section 5, prior to describing the framework and security model in Section 4. The security analysis and performance evaluation are presented in Section 6 and Section 7, respectively. Lastly, we conclude the paper in Section 8.

2. Related Work

In this section, some authentication schemes are proposed to cope with privacy and security properties in a vehicular network. These schemes are established on either cryptography of bilinear pair or elliptic curve to generate and verify signatures of the messages sent among vehicles. Therefore, in the next two sections, we classify the existing schemes based on these cryptography algorithms.

2.1. Bilinear Pair Cryptography Based

Ali et al. [15] combined public key infrastructure-based and certificates cryptosystem-based schemes to propose a conditional privacy-preserving hybrid signcryption scheme for providing communication security in the system. This scheme supports batch signature verification to verify a large number of signatures simultaneously.

To resist impersonation attacks from broadcasting fake messages in the vehicular network, Al-Shareeda et al. [16] presented a secure authentication scheme by frequently updating the vehicle's true identity saved on a tamper proof device (TPD) vehicle.

Bayat et al. [17] presented a privacy-preserving scheme without using a large number of pseudonym-IDs, online RSU, or signer's group in the system.

Pournaghi et al. [18] combined TPD-based and RSU-based schemes to propose an NECPPA scheme by issuing and updating temporary secret keys saved on vehicles.

2.2. Elliptic Curve Cryptography Based

Several researchers [19–28] have proposed schemes based upon elliptic curve cryptography as follows.

Alshudukhi et al. [19] suggested a lightweight authentication with a privacy-preserving scheme by saving the system's master private key in each TPD of RSU instead of the TPD of OBU for satisfying privacy and security properties in the vehicular network.

Cui et al. [24] suggested a content-sharing scheme by downloading demands to speedily filter the adjacent vehicles to select properly proxy vehicles and demand them for communication security in the system.

Zhang et al. [28] designed the concept of edge computing vehicle to propose a fuzzy logic mathematical for satisfying mutual authentication between ordinary vehicles and edge computing.

To prevent insider attacks, Al-Shareeda et al. [20] suggested a privacy-preserving scheme by preloading a pool of pseudonym IDs and the concerned private key from a Trusted Authority (TA) for generating and verifying the signature of messages shared among vehicles.

2.3. Critical Discussion

According to Sections 2.1 and 2.2, these schemes are established by cryptographies of bilinear pair and elliptic curve, respectively, that are proposed to resist security attacks in a vehicular network. However, the operations applied to these algorithms are considered time-consuming and complicated to operate. As a result, these algorithms are not suitable to deploy in the system due to rapid-movement vehicle change topology in the vehicular network. Additionally, these schemes are vulnerable to quantum attacks since these schemes are based on easily solving hard mathematical problems such as elliptic-curve discrete, discrete logarithm, and integer factorization problems by running Shor’s algorithm. Besides, these schemes require an RSU-aided scheme for the mutual authentication process, which is considered an expensive device in the system.

To reduce the overhead of the system and resist quantum attacks, this paper proposes a lightweight quantum-resistant scheme using a lattice (more details in Section 3.3) instead of cryptographies of bilinear pair and elliptic curves. In our proposal, the vehicle applies a metric multiplication based on the lattice to generate and verify signatures of messages shared among vehicles (more details in Section 5). Security analysis not only shows that our proposal satisfies privacy and security properties but also that it resists quantum attacks (more details in Section 7). The operations used based on the lattice are considered lightweight operations (more details in Section 6).

For simplicity, this paper summarizes the comparison of relevant works’ properties of privacy and security in Table 1. These properties should be satisfied on our proposal (more details in Section 3.2) for the 5G-enabled vehicular network. Based on Table 1, we can observe that the existing schemes do not support the mentioned properties of privacy and security in terms of quantum attacks and lightweight operations for vehicular networks. While the schemes in [15,20] need expensive components and an RSU-aided scheme during the joining process, our proposal satisfies a significant reduction in performance, which makes it lightweight enough to handle quantum attacks. Meanwhile, our proposal is based on 5G technology without using any RSU-aided scheme.

Table 1. Comparison of relevant works’ properties of privacy and security.

Property	Ali et al. [15]	Cui et al. [24]	Al-Shareeda et al. [20]	Proposal
Authentication and Integrity	Yes	Yes	Yes	Yes
Identity Privacy-Preserving	Yes	Yes	Yes	Yes
Traceability	Yes	Yes	Yes	Yes
Unlinkability	Yes	Yes	Yes	Yes
Common Security Attack Resistant	Yes	Yes	Yes	Yes
Quantum Attacks	No	No	No	Yes
Lightweight Operations	No	No	No	Yes
No RSU-Aided Scheme	No	Yes	No	Yes

3. Preliminaries

3.1. System Model

As shown in Figure 1, the system model of our proposal consists of three major components, namely a trusted authority (TA), 5G-base station (5G-BS), and onboard unit (OBU) for the 5G-enabled vehicular network. The description of these components is as follows.

- TA: A trusted management to issue system parameters and register vehicles in the system. Additionally, the TA is in charge of carrying out the traceability process.
- 5G-BS: Deployed along the roadside and has the responsibility to connect between the TA and vehicles within its wide-range communication domain by using the 5G standard.
- OBU: Each vehicle contains a wireless device called an OBU that allows it to process, send, and receive messages using the DSRC protocol and 5G standard to communicate with other vehicles and 5G-BS, respectively. Based on our assumption in this paper, each OBU has a very strong TPD device to save the system's master private key that is preserved by the TA during the registration process. Therefore, the third part does not have the ability to reveal the system's saved master private key.

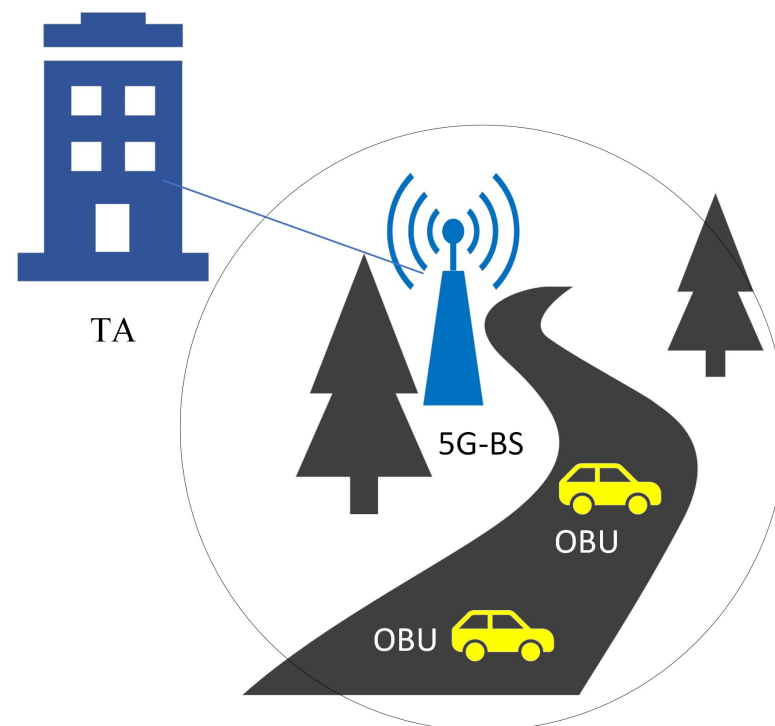


Figure 1. The system model of our proposal.

3.2. Security Design

In this section, we detail the properties of privacy and security that must be supported in our proposal for a vehicular network based on 5G.

- Authentication and integrity: Make sure that message is sent without any modification.
- Identity privacy-preserving: The vehicle's true identity should be hidden.
- Traceability: Only the TA can reveal the vehicle's true identity from the message sent.
- Unlinkability: Adversary tries to link more than two signatures sent from the same sender.
- Security attack resistant:
 - Replay attacks: Adversary tries to replay messages sent from registered vehicles.
 - Modify attacks: Adversary tries to modify/change the content of the message.
 - Forgery attacks: Adversary tries to impersonate a valid signature.
 - Man-in-the-middle attacks: Adversary tries to intercept communication among vehicles.

- Quantum attacks: Adversary tries to easily solve hard mathematical problems such as elliptic-curve discrete, discrete logarithm, and integer factorization problems by running Shor’s algorithm.

3.3. Lattice-Based Cryptography

Ajtai [29] first introduced the lattice-based problem in 1996. Nevertheless, many research [30,31] works in this approach assume the difficulty of the short integer solution (SIS) or independent SIS (ISIS) problems. For these structures, worst-case to average-case hardness-based mathematical security proofs are given. The hard difficulties of finding the short vector in the integer subspace of the m -dimensional Euclidean space R^m serve as the foundation for the cryptographies security.

3.4. Lattice

For some positive integer n , a lattice is a discrete additive subgroup of $R^n(R)$ known as real space. The following is a definition of the lattice [32].

Explanation 1. Assuming that $b_1, b_2, \dots, b_n \in R^m$ are linearly independent vectors, then the discrete set is a lattice \mathcal{L} produced by basis vectors b_1, b_2, \dots, b_n as Equation (1).

$$\mathcal{L}(b_1, b_2, \dots, b_n) = \sum_{i=1}^n j_i b_i : j_i \in Z. \tag{1}$$

The dimension of the provided lattice is an integer α , and its rank is an integer β . The shortest nonzero vector in a particular lattice’s length is the minimum distance³ as Equation (2).

$$D_{min}(\mathcal{L}) = \min \|b\|, \text{ where } b \in \mathcal{L} - 0. \tag{2}$$

Explanation 2. A lattice \mathcal{L} issued by a basis $B \in Z^{\alpha \times \beta}$ is \mathcal{L} . We are aware that premise B is not special. B and BU produce the same lattice $\mathcal{L}(B)$ if $U \in Z^{\alpha \times \beta}$ is a unimodular matrix.

Lemma 1. A discrete additive subgroup of R^m is a lattice if it is a subset of R^m .

Explanation 3 (Short integer solution). Find the shortest nonzero vector $b \in \mathcal{L}$ with b having the lowest norm in the discrete additive subgroup of R^m , given any basis $B \in Z^{\alpha \times \beta}$ of a lattice $\mathcal{L}(B)$.

Explanation 4 (Closest vector problem). Finding $b \in \mathcal{L}$ such that $\|a - b\|$ has the lowest norm is the closest vector problem given a basis $B \in Z^{\alpha \times \beta}$ of a lattice $\mathcal{L}(B)$ and a vector a that is not in \mathcal{L} .

Theorem 1. The following are equal if $B \in R^{\beta \times \alpha}$ and $B^- \in R^{\beta \times \alpha}$ are two complete rank bases.

- $\mathcal{L}(B) = \mathcal{L}(B^-)$.
- $U \in R^{\beta \times \alpha}$ such that $B^- = BU$, where U is unimodular.

Proof. Assume $\mathcal{L}(B) = \mathcal{L}(B^-)$, and there are integer matrices Q and Q' ; then, we demonstrate the unimodularity of Q and Q' . Here, it can be observed that $B^- = BQ = B'(Q'Q)$. Due to B^- being the entire rank matrix, it can be multiplied by B'^{-1} , and result in $QQ' = 1$. Thus, both Q and Q' are non-singular with integer inputs. Lastly, it can be observed from here that either $\det(Q) = \det(Q') = -1$ or $\det(Q) = \det(Q') = 1$. Therefore, Q and Q' are considered unimodularity matrices. □

Contrarily, consider Q to be a unimodular matrix such that $B^- = BQ$. Thus, $\mathcal{L}(Q') \subseteq \mathcal{L}(Q)$, since Q is an integer matrix. Additionally, we can observe that each column of Q' is a linear combination of columns in Q . Here, $Q = Q'U^{-1}$, as u is a unimodular matrix. Thus, $\mathcal{L}(Q) \subseteq \mathcal{L}(Q')$, and it can be concluded that $\mathcal{L}(Q) = \mathcal{L}(Q')$.

3.5. Lattice of q-ary

The term “Lattice of q-ary” refers to an integer lattice \mathcal{L} that includes a q times integer lattice vector and achieves $Z_q^\alpha \subseteq \mathcal{L} \subseteq Z_\beta$ for some integer q . The lattice of q-ary is actually equipment utilized in security proofs that are according to problems based on the lattice.

Definition 1. *M-dimensional q-ary lattices come in two different varieties depending on the matrix modulo $q = \text{poly}(m)$, represented by $E \in Z_q^{\alpha \times \beta}$ as Equation (3).*

$$\begin{aligned} \Lambda_q^t &= \{e \in Z^\beta : Ee = 0(\text{mod}q)\} \\ \Lambda_q &= \{e \in Z^\beta : e = E^t b(\text{mod}q) | b \in Z^\alpha\} \end{aligned} \tag{3}$$

where α, β , and q are integers and $\alpha > \beta$. In order to create cryptographic schemes, these q-ary lattices are applied.

Theorem 2. *In the typical case, approximating the issue GapSV_y [33,34] in an β -dimensional lattice within a factor of $y = \theta O'(\sqrt{\beta})$ is harder than solving SIS problems with a given $\theta = \text{poly}(\alpha) > 0$, where α is the dimension, β is the rank of the lattice, and prime $q \geq \theta \cdot \sqrt{\alpha\beta}$.*

4. Framework and Security Model

In this section, we discuss the framework and security model for our proposal in 5G-enabled vehicular networks.

4.1. Framework

We construct our proposal generically via the following phases: Setup, VehReg, GenSig, SSigVerify, and BSigVerify.

- **Setup:** This phase provides a security parameter 1^k that is used to calculate master private keys s and system parameters $param$ for TA.
- **VehReg:** The vehicle v_i runs this phase that takes $param$ and S_x from the TA after submitting the true identity TID_{v_i} to the system.
- **GenSig:** This phase is carried out by vehicle v_i with the pseudonym-ID PID_i . It takes as inputs $param$, message $M_i \in \{0, 1\}^*$, the system’s private keys S_x , and its private key SK_i , and outputs a signature σ_i and D_i .
- **SSigVerify:** A verifier preforms this phase by taking $param$, single message M_i with the single pseudonym-ID PID_i , single signature σ_i , and D_i from single vehicle v_i and outputs true if σ_i is valid; otherwise it responds false.
- **BSigVerify:** A verifier preforms this phase by taking $param$, batch messages $\{M_1, M_2, \dots, M_n\}$ with the batch pseudonym-IDs $\{PID_1, PID_2, \dots, PID_n\}$, and batch signatures $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ and $\{D_1, D_2, \dots, D_n\}$ from batch vehicles $\{v_1, v_2, \dots, v_n\}$, and outputs true if $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ are valid; otherwise it responds false.

4.2. Security Model

With the use of a game, the components of our proposal’s security model are explained. In the game, a challenger (**C**) and an adversary (**Adv**) are probabilistic polynomial-time (PPT) algorithms that try to undermine the proposed security model. This is a list of PPT questions that an adversary (**Adv**) in the game asks.

- **Setup:** Challenger **C** takes 1^k and issues the system’s parameters. Additionally, **C** sends these parameters to adversary **Adv**.
- **Query (H_1):** In this query, **C** randomly picks the number $d \in Z_q^*$ and issues (M_i, d) . This pair is recorded into a table $List_{h_1}$ and d is sent to **Adv**.
- **Query (H_2):** In this query, **C** randomly picks the number $d \in Z_q^*$ and issues (m, d) . This pair is recorded into a table $List_{h_2}$ and d is sent to **Adv**.

- **Query (H_3):** In this query, **C** randomly picks the number $d \in Z_q^*$ and issues (m, d) . This pair is recorded into a table $List_{h_3}$ and d is sent to **Adv**.
- **Signing Query:** In this query **Adv** sends a message M_i to **C**. In an output, **C** issues and sends $\{M_i, PID_i, T_i, D_i, \delta_i\}$ to **Adv**, who can compromise the authenticity of our proposal if he/she can properly issue a login demand. Consider $Att_{Adv.Auth}^{Proposal}(k)$ be the advantage of **Adv** to compromise our proposal. Our proposal in a 5G-enabled vehicular network satisfies authentication security for any **Adv**,

$$Att_{Adv.Auth}^{Proposal}(k) \leq \epsilon \tag{4}$$

5. Proposed Scheme

This section proposes a lattice-based lightweight quantum-resistant scheme in 5G-enabled vehicular networks. Our proposal has five phases, called setup, VehReg, GenSig, SSigVerify, and BSigVerify, as shown in Figure 2. These phases are proposed as follows.

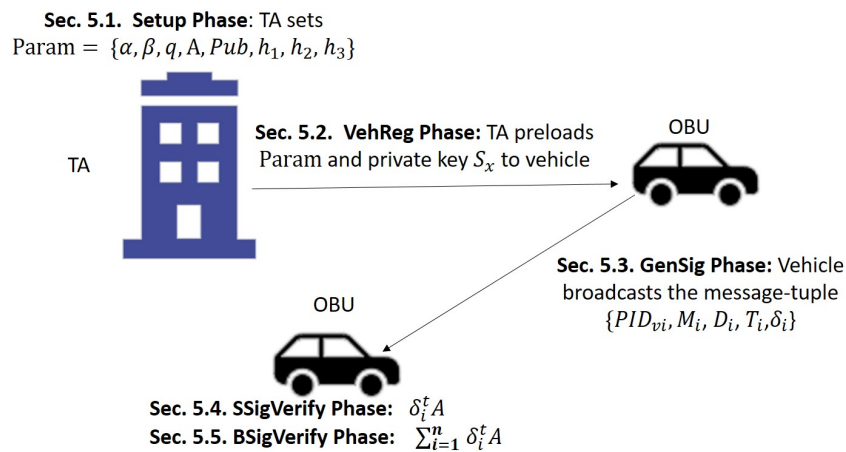


Figure 2. Five phases of our proposal.

5.1. Setup Phase

This phase generates public system parameters by the TA as follows.

- The TA picks a prime q and two positive integers α, β .
- The TA picks a matrix $\mathcal{A} \in Z_q^{\alpha \times \beta}$ with integer entries.
- The TA randomly selects $S_x \in Z_q^\alpha$ as the system’s master private key and then computes the corresponding public key as $Pub = S_x^t \mathcal{A} \in Z_q^{1 \times \beta}$.
- The TA chooses three secure hash functions as $h_1 : Z_q^\alpha \rightarrow Z_q$, $h_2 : \{0, 1\}^* \rightarrow Z_q$, and $h_3 : \{0, 1\}^* \times \{0, 1\}^* \times Z_q^{1 \times \alpha} \times \{0, 1\}^* \rightarrow Z_q$.
- Finally, the TA sets the public system parameters as $param = \{\alpha, \beta, q, \mathcal{A}, Pub, h_1, h_2, h_3\}$.

5.2. VehReg Phase

This phase registries the participating vehicle before leaving the factory as follows.

- A user submits the true identity TID_{v_i} of vehicle v_i to the TA through a secure channel.
- The TA first checks the validity and authenticity of the vehicle’s true identity TID_{v_i} .
- The TA preloads the public system parameters as $param = \{\alpha, \beta, q, \mathcal{A}, Pub, h_1, h_2, h_3\}$ to the OBU of vehicle v_i .
- The TA saves its master private key S_x into TPD of OBU on vehicle v_i . Note that the attacker does not have the ability to reveal any data saved on the TPD, according to the assumption in this paper.

5.3. GenSig Phase

This phase is executed by vehicle v_i as follows.

- Vehicle v_i randomly picks number $r_i \in Z_q^\alpha$ and then calculates pseudonym-IDs PID_{v_i} as Equation (5) by using system's master private key S_x saved on its TPD.

$$\begin{aligned}
 PID_{v_i} &= (PID_{i,1}, PID_{i,2}) \\
 &= (r_i^t \mathcal{A}, TID_{v_i} \oplus h_1(S_x || PID_{i,1}))
 \end{aligned}
 \tag{5}$$

- Vehicle v_i calculates parameter $\eta_i = h_2(PID_{i,1} || T_i)$ private key $SK_i = r_i + S_x \cdot \eta_i$, where T_i is a freshness timestamp.
- Vehicle v_i randomly picks number $d_i \in Z_q^\alpha$ and then computes $D_i = d_i^t \mathcal{A}$, $\sigma_i = h_3(PID_{i,1} || T_i || D_i || M_i)$.
- Vehicle v_i computes the message signature as Equation (6).

$$\delta_i = SK_i + d_i \cdot \sigma_i \in Z_q^\beta
 \tag{6}$$

- Finally, vehicle v_i sends to other vehicles with the message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$.

5.4. SSigVerify Phase

This phase verifies the single message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$ sent from a single source by the verifying recipient v_j at a time as follows.

- Once receiving message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$, verifying recipient v_j checks the freshness timestamp T_i in order to resist a replay attack in our proposal.
- Verifying recipient v_j checks the authenticity and integrity of message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$ by computing Equation (7).

$$\begin{aligned}
 \delta_i^t \mathcal{A} &= (SK_i^t + d_i^t \cdot \sigma_i) \cdot \mathcal{A} \\
 &= (r_i + S_x \cdot \eta_i)^t \cdot \mathcal{A} + d_i^t \cdot \sigma_i \cdot \mathcal{A} \\
 &= r_i^t \mathcal{A} + \eta_i \cdot S_x^t \cdot \mathcal{A} + \sigma_i \cdot d_i^t \cdot \mathcal{A} \\
 &= PID_{i,1} + \eta_i \cdot Pub + \sigma_i \cdot D_i.
 \end{aligned}
 \tag{7}$$

It accepts a message if the verification is successful; otherwise, it refuses.

5.5. BSigVerify Phase

After receiving $\{PID_{v_1}, M_1, D_1, T_1, \delta_1\}, \{PID_{v_2}, M_2, D_2, T_2, \delta_2\}, \dots, \{PID_{v_n}, M_n, D_n, T_n, \delta_n\}$, this phase verifies the large number of message that were sent from a large number of vehicles simultaneously. This process is as follows.

- Once receiving message-tuple $\{PID_{v_n}, M_n, D_n, T_n, \delta_n\}$, verifying recipient v_j checks the freshness timestamp T_n in order to resist a replay attack in our proposal.
- Verifying recipient v_j randomly tests vector $\gamma_i = \{\gamma_1, \gamma_2, \dots, \gamma_n\}$, where $i \in \{1, 2, 3, \dots, n\}$.
- Verifying recipient v_j checks the authenticity and validity of message-tuple $\{PID_{v_n}, M_n, D_n, T_n, \delta_n\}$ by computing Equation (8).

$$\left(\sum_{i=1}^n \gamma_i \delta_i^t \right) \mathcal{A} \stackrel{?}{=} \sum_{i=1}^n \gamma_i PID_{i,1} + \left(\sum_{i=1}^n \gamma_i \eta_i \right) Pub + \left(\sum_{i=1}^n \gamma_i \sigma_i \right) D_i.
 \tag{8}$$

It accepts a the message if verification is successful; otherwise, it refuses.

6. Security Analysis

6.1. Random Oracle Model

The following Random oracle model ensures the security of our proposal in a 5G-enabled vehicular network.

Theorem 3. Under adaptively chosen message attacks in the random oracle model, our proposal satisfies security against a PPT attacker under two problems of ISIS and SIS.

Proof. Assume adversary **Adv** impersonates the valid message $\{M_i, PID_i, T_i, D_i, \delta_i\}$; then, challenger **C** is created in such a way that it can assist **Adv** to compromise the ISIS or SIS problems with a non-negligible advantage to win the game. As a lattice problem with the values $(P, B = S_x^t \mathcal{A})$, challenger **C** responds to **Adv**'s inquiries as follows:

- **Setup:** Challenger **C** assigns $Pub \leftarrow B = S_x^t \mathcal{A}$ and parameters $\{M, q, \mathcal{A}, Pub, h_1, h_2, h_3\}$ are sent to **Adv**.
- **Query (H_1):** **C** maintains a table $List_{h_1}$ with the inputs (ϕ, ν) . At first, this list $List_{h_1}$ is given empty. Then, **Adv** requests a query as query- (H_1) with a message ϕ . In output, **C** tests table $List_{h_1}$ for (ϕ, ν) and, if it exists, transmits $h_1(\phi) = \nu$ to **Adv**; otherwise, **C** selects a random number $\nu \in Z_p^*$, inserts (ϕ, ν) into $List_{h_1}$, and returns $h_1(\phi) = \nu$ to **Adv**.
- **Query (H_2):** **C** maintains a table $List_{h_2}$ with the inputs (PID_i, T_i, ν) . At first, this list $List_{h_2}$ is given empty. Then, **Adv** requests a query as query- (H_2) with a message (PID_i, T_i) . In output, **C** tests table $List_{h_2}$ for (PID_i, T_i, ν) and, if it exists, transmits $h_2(PID_i || T_i) = \nu$ to **Adv**; otherwise, **C** selects a random number $\nu \in Z_p^*$, inserts (PID_i, T_i, ν) into $List_{h_2}$, and returns $h_2(PID_i || T_i) = \nu$ to **Adv**.
- **Query (H_3):** **C** maintains a table $List_{h_3}$ with the inputs $(PID_i, T_i, D_i, M_i, \nu)$. At first, this list $List_{h_3}$ is given empty. Then, **Adv** requests a query as query- (H_3) with a message (PID_i, T_i, D_i, M_i) . In output, **C** tests table $List_{h_3}$ for $(PID_i, T_i, D_i, M_i, \nu)$ and, if it exists, transmits $h_3(PID_i || T_i || D_i || M_i) = \nu$ to **Adv**; otherwise, **C** selects a random number $\nu \in Z_p^*$, inserts $(PID_i, T_i, D_i, M_i, \nu)$ into $List_{h_3}$, and returns $h_3(PID_i || T_i || D_i || M_i) = \nu$ to **Adv**.
- **Signing Query:** In this step, **Adv** transmits a traffic-related M_i to **C**. Then, **C** randomly picks $\delta_i \in Z_q^\alpha$, $\eta_i, \sigma_i \in Z_q^*$, $PID_{i,2}$ and calculates $PID_{i,1} = \delta_i^t \mathcal{A} - \eta_i Pub - \sigma_i D_i$. Lastly, the message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$ is sent to **Adv** by **C**. Meanwhile, we can observe that $\delta_i^t \mathcal{A} = PID_{i,1} + \eta_i Pub + \sigma_i D_i$ holds. Therefore, an input signature creation method performed by **C** is identical to a valid signature scheme performed by registered vehicles.

□

Finally, **Adv** issues a response $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$ and **C** verifies Equation (9).

$$\delta_i^t \mathcal{A} = PID_{i,1} + \eta_i \cdot Pub + \sigma_i \cdot D_i. \tag{9}$$

If Equation (9) does not hold, **C** ends the procedure. If the aforementioned procedure is now repeated with h_2 , **Adv** issues another message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$. Therefore, **C** checks Equation (10).

$$\delta_i'^t \mathcal{A} = PID_{i,1} + \eta_i' \cdot Pub + \sigma_i \cdot D_i. \tag{10}$$

Now, from Equations (9) and (10), Equation (11) can be concluded.

$$\begin{aligned} (\delta_i^t - \delta_i'^t) \mathcal{A} &= PID_{i,1} + \eta_i \cdot Pub + \sigma_i \cdot D_i - PID_{i,1} - \eta_i' \cdot Pub - \sigma_i \cdot D_i \\ &= (PID_{i,1} - PID_{i,1}) + (\sigma_i \cdot D_i - \sigma_i \cdot D_i) + (\eta_i \cdot Pub - \eta_i' \cdot Pub) \\ &= \eta_i \cdot Pub - \eta_i' \cdot Pub \\ &= (\eta_i - \eta_i') \cdot Pub \\ &= (\eta_i - \eta_i') \cdot S_x^t \mathcal{A} \end{aligned} \tag{11}$$

Now, **C** takes the definition of an ISIS or SIS problem as Equation (12).

$$\frac{\delta_i - \delta'_i}{(\eta_i - \eta'_i)} \tag{12}$$

Nevertheless, this definition does not attain the difficulty of ISIS or the SIS problems. Therefore, our proposal achieves strong security against **Adv** under the random oracle model.

6.2. Security Requirements

In this section, our proposal satisfies the privacy and security properties (as mentioned above in Section 3.2) as follows.

- Authentication and integrity: According to Theorem 3, we can observe that PPT-based **Adv** does not have the capability to produce a forgery due to problems of ISIS/SIS. Hence, the validity and safety of message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$ sent by a vehicle are verifiable by testing Equation (7) or Equation (8). Therefore, our proposal for a 5G-enabled vehicular network supports the properties of authentication and integrity.
- Identity privacy-preserving: A vehicle broadcasts message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$ including its true identity TID_{v_i} , where $PID_{v_i} = \{PID_{i,1}, PID_{i,2}\}$. Due to $PID_{i,1} = r_i^t \mathcal{A}$ and $PID_{i,2} = TID_{v_i} \oplus h_1(S_x || PID_{i,1})$, the PPT-based **Adv** must compute $h_1(S_x || PID_{i,1})$ to reveal a vehicle's true identity $TID_{v_i} = PID_{i,2} \oplus h_1(S_x || PID_{i,1})$. Due to the problems of ISIS/SIS, **Adv** does not have the capability to disclose S_x from $Pub = S_x^t \mathcal{A}$ or $PID_{i,2} = TID_{v_i} \oplus h_1(S_x || PID_{i,1})$. Therefore, our proposal for a 5G-enabled vehicular network supports the property of identity privacy-preserving.
- Traceability: The vehicle's true identity TID_{v_i} is traceable by the TA as follows. The pseudonym-ID PID_{v_i} in message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$ is issued by the user with the assistance of true identification TID_{v_i} . This is because $PID_{i,1} = r_i^t \mathcal{A}$, $PID_{i,2} = TID_{v_i} \oplus h_1(S_x || PID_{i,1})$, and $PID_{v_i} = \{PID_{i,1}, PID_{i,2}\}$. The TA utilizes its master private key S_x to calculate $h_1(S_x || PID_{i,1})$ and obtains the true identity as $TID_{v_i} = PID_{i,2} \oplus h_1(S_x || PID_{i,1})$. Therefore, our proposal for a 5G-enabled vehicular network supports the property of traceability.
- Unlinkability: The vehicle randomly picks $r_i \in Z_q^\alpha$ and $d_i \in Z_q^\alpha$ to compute message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$, where $PID_{i,1} = r_i^t \mathcal{A}$, $PID_{i,2} = TID_{v_i} \oplus h_1(S_x || PID_{i,1})$, $PID_{v_i} = \{PID_{i,1}, PID_{i,2}\}$, $D_i = d_i^t \mathcal{A}$ and $\sigma_i = h_3(PID_{i,1} || T_i || D_i || M_i)$. Any **Adv** cannot distinguish two messages of the user due to random values r_i and d_i . Therefore, our proposal for a 5G-enabled vehicular network supports the property of unlinkability.
- Security attack resistant:
 - Replay attacks: In our proposal, the message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$ includes a timestamp T_i . Due to the freshness of T_i , the replay attack cannot be processed.
 - Modify attacks: According to Theorem 3, we can observe that any alteration in the message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$ is easily detectable by testing Equation (7) or Equation (8).
 - Forgery attacks: **Adv** has to generate the message-tuple $\{PID_{v_i}, M_i, D_i, T_i, \delta_i\}$, which holds Equation (7) or Equation (8). Nevertheless, according to Theorem 3, no such **Adv** can be constructed.
 - Man-in-the-middle attacks: Our proposal achieves node authentication and message integrity, and thus the authenticity and validity of the communicating components.

6.3. Quantum Resistant

This section provides security in a quantum environment [35–37]. On the basis of the difficulty in some lattices, the security of our proposal is assumed. This lattice-based technique is according to the worst-to-average-case premise that the SIS and ISIS problems in some lattices are difficult to resolve with appropriate values. The following list contains the key security elements.

- **Resistance to collision:** In some of the lattices, the matrix family $\{\mathcal{A} : C \rightarrow \mathbf{Adv}^\alpha | \mathcal{A} \in \mathcal{A}\}$ has the ability to resist collisions. If there are collisions, then SIS is simple to solve. Let $\mathcal{A}x = \mathcal{A}x'$ for some short vector x and x' be the collision; then, $\mathcal{A}(x - x') = 0$ and $x - x'$ is short.
- **Property of hiding:** (Y, Ω) -hiding for any $\mathcal{A} \in Z_q^{\alpha \times \beta}$, $S_x \in Z_q^\alpha$, $P \in P$; let $\Gamma(S_x, P) = \{S'_x, d', r' : S'_x \mathcal{A} = S_x^t \mathcal{A} \wedge d^t \mathcal{A} = d'^t \mathcal{A} \wedge r^t \mathcal{A}\}$ be the gathering of private keys with corresponding public key $Pub = X_s^t \mathcal{A}$ and signature $d^t \mathcal{A}, r^t \mathcal{A}$. Our proposal has the property of hiding when $Pr_{S_x \in Z_q^\alpha}[\forall P \neq P' | \Gamma(S_x, P) \cap \Gamma(S_x, P')| \leq \epsilon | \Gamma(S_x, P')|] \geq \Omega$.

Lemma 2. Suppose that if a randomized probabilistic polynomial-time adversary **Adv** breaches the authenticity system with probability ω , our proposal has the features of closure and concealing. Then, with probability $\frac{(\omega + \Omega - 1) \cdot (1 - \epsilon)}{2 - \epsilon}$, collision resistance is effectively targeted.

Theorem 4. If an **Adv** has the concealment features, collision resistance, and closing that hold for $\epsilon < 1$ with two hard problems of ISIS and SIS in the associated lattice, then our proposal is quantum-resistant.

Proof. Assume that the adversary with probability ω is the one that compromises the security of our proposal. Here, **Adv** performs the following collision detection using a PPT method as follows.

- Let $\mathcal{A}Z_q^{\alpha \times \beta}$ and private key $S_x \in Z_q^\alpha$, then calculate $Pub = S_x^t \mathcal{A}$.
- Send the system's parameters $\{\mathcal{A}, Pub\}$ to **Adv**.
- Let a query $P \leftarrow \mathbf{Adv}(\mathcal{A}, Pub)$.
- Verify the authenticity of P and transmit $\{P, PID, T, D = d^t \mathcal{A}, \delta = SK + \sigma d\}$ to **Adv**.
- The impersonation obtained is $\{P', PID', T', D', \delta'\} \leftarrow \mathbf{Adv}(\mathcal{A}, Pub, D, \delta, PID)$.
- The result is $\{d^t \mathcal{A}, SK + \sigma d, r^t \mathcal{A}, D', \delta', PID'\}$ as a collision to \mathcal{A} .

□

Consider that in queries of **Adv** with correct P, P', D', δ' , and PID' , if he/she experiences a nontrivial collision as a result, collision will be successful as Equation (13). Note that D^- refers to a query generated through **Adv**.

$$\begin{aligned} d^t \mathcal{A} &\neq D^- \\ SK + \sigma d &\neq \delta' \end{aligned} \tag{13}$$

Attacker **Adv** issues valid message-tuple $\{P', D', \delta', PID'\}$ if $\{P', D', \delta', PID'\} \neq \{P, D, \delta, PID\}$. We can assume that $Pr[\{P', D', \delta', PID'\} \neq \{P, D, \delta, PID\}] = \omega$ and randomly select value $b \in 0, 1$. We assume that $Pr[b = 0] = \frac{1 - \epsilon}{2 - \epsilon}$ and $Pr[b = 1] = \frac{1}{2 - \epsilon}$. Moreover, if $b=0$, then set $S'_x = S_x$, $d = d'$; otherwise select a random value from definitive dissemination $\Gamma(S_x, P)$.

Thus, the amounts $\{d^t \mathcal{A}, SK', \sigma d', r^t \mathcal{A}, D', \delta', PID'\}$ are the result of **Adv**. Additionally, S_x is distributed over $\Gamma(S_x, P)$. From the analysis, we can observe that the amounts $\{d^t \mathcal{A}, SK', \sigma d', r^t \mathcal{A}, D', \delta', PID'\}$ is distributed by the hash function with collision resistance. The following is the probability of a collision:

$$Pr[d^t \mathcal{A} \neq D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t \mathcal{A} \neq PID'] = Pr[(d^t \mathcal{A} D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t \mathcal{A} \neq PID') \wedge P = P'] + Pr[(d^t \mathcal{A} \neq D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t \mathcal{A} \neq PID') \wedge P \neq P' \wedge d^t \mathcal{A} = D \wedge SK + \sigma d = \delta \wedge r^t \mathcal{A} = PID] + Pr[(d^t \mathcal{A} \neq D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t \mathcal{A} \neq PID') \wedge P \neq P' \wedge (d^t \mathcal{A} \neq D' \wedge SK' + \sigma d' \neq \delta' \neq r^t \mathcal{A} \neq PIDA)].$$

Case 1. If $P = P'$ and $\{P', D', \delta', PID'\} \neq \{P, D, \delta, PID \wedge P = P'\}$ holds, $d^t \mathcal{A} \neq D' SK' + \sigma d' \neq \delta' \wedge r^t \mathcal{A} \neq PID'$, and also $P' = P$ holds. Thus, $(d^t \mathcal{A} \neq D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t \mathcal{A} \neq PID') \wedge P = P'$ also holds. Thus, $Pr[d^t \mathcal{A} \neq D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t \mathcal{A} \neq PID'] \wedge P = P'$ also holds. Thus, $Pr[d^t \mathcal{A} \neq D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t \mathcal{A} \neq PID'] \wedge P = P'$ also holds.

$$P = P'] \geq Pr[\{P', D', \delta', PID'\} \neq \{P, D, \delta, PID\} \wedge P = P'] \geq Pr[\{P', D', \delta', PID'\} \neq \{P, D, \delta, PID\} \wedge P = P'] \frac{1-\epsilon}{2-\epsilon}.$$

Case 2. When $P \neq P'$ and $d^t A = D' \wedge SK' + \sigma d = \delta' \wedge r^t A = PID'$, then we have $d^t A \neq D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t A \neq r^t A$. Therefore, $S'_x A = S_x A d^t A \neq d A, SK' + \sigma d' \neq SK + \sigma d$ and $r^t A \neq r^t$ holds if S'_x does not lie in $\Gamma(S_x, P')$. Let $X \subseteq Z_q^\alpha, \Delta \subseteq Z_q^\alpha$ be the set of possible secrets S_x, d and r , respectively, such that $P \neq P' | \Gamma(S_x, P) \cap \Gamma(S_x, P') | \leq \epsilon | \Gamma(S_x, P)$. Based on the concept of hiding, it can be obtained that $Pr[S_x \in x \subseteq Z_q^\alpha, d \in \Delta \subseteq Z_q^\alpha, r \in R \subseteq Z_q^\alpha] \geq \Omega$. Now, we have the following for $b = 1$, using the union bound on probability:

$$Pr[P \neq P' \wedge (d^t A = D' \wedge SK' + \sigma d = \delta' \wedge r^t A = PID') \wedge S_x \in X \wedge d \in \Delta \wedge r \in A \wedge b = 1] = Pr[P \neq P' \wedge (d^t A = D' \wedge SK' + \sigma d = \delta' \wedge r^t A = PID') | S_x \in X \wedge d \in \Delta \wedge r \in A] Pr[b = 1] \geq Pr[P \neq P' \wedge (d^t A = D' \wedge SK' + \sigma d = \delta' \wedge r^t A = PID')] - Pr[X_s \notin X \wedge d \notin \Delta \wedge r \notin A] (2 - \epsilon)^{-1} \geq Pr[\{P', D', \delta', PID'\} \neq \{P, D, \delta, PID\} \wedge P \neq P' \wedge (d^t A = D' \wedge SK' + \sigma d = \delta' \wedge r^t A = PID')] - 1 + \Omega(2 - \epsilon)^{-1}.$$

Likewise, it is possible to see the following:

$$Pr[\{d^t A \neq D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t A \neq PID'\} | \{P \neq P' \wedge d^t A = D' \wedge SK' + \sigma d' = \delta' \wedge r^t A = PID' \wedge S_x \in X \wedge d \in \Delta \wedge r \in A \wedge b = 1\}] \geq 1 - \text{Max}_{S_x \in X \wedge d \in \Delta \wedge r \in A} \frac{|\Gamma(S_x, \alpha) \cap \Gamma(S_x, \alpha')|}{|\Gamma(S_x, \alpha)|} \geq 1 - \epsilon.$$

Consequently, we obtain the following:

$$Pr[(d^t A \neq D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t A \neq PID') \wedge P = P' \wedge (d^t A = D' \wedge SK + \sigma d = \delta' \wedge r^t A = PID') \wedge S_x \in X \wedge d \in \Delta \wedge r \in A] \geq Pr[\{P', D', \delta', PID'\} \neq \{P, D, \delta, PID\} \wedge P = P'] \wedge (d^t A = D' \wedge SK + \sigma d = \delta' \wedge r^t A = PID')] - 1 + \Omega(2 - \epsilon)$$

Case 3. If $P = P'$ and $d^t A \neq D' \wedge SK' + \sigma d \neq \delta' \wedge r^t A \neq PID'$, then it becomes apparent that $P \neq P'$ and $d^t A \neq D' \wedge SK' + \sigma d \neq \delta' \wedge r^t A \neq PID' \wedge b = 0$, implying that $S'_x = S_x$, and $r' = r$.

$$Pr[\{d^t A \neq D' \wedge SK' + \sigma d' \neq \delta' \wedge r^t A \neq PID'\} \wedge P \neq P' \wedge (d^t A \neq D' \wedge SK + \sigma d \neq \delta' \wedge r^t A \neq PID')] \geq Pr[P \neq P' \wedge (d^t A \neq D' \wedge SK + \sigma d \neq \delta' \wedge r^t A \neq PID' \wedge b = 0)] \geq Pr[\{P', D', \delta', PID'\} \neq \{P, D, \delta, PID\}] - 1 + \Omega \frac{1-\epsilon}{2-\epsilon} = (\omega - 1 - \Omega) \frac{1-\epsilon}{2-\epsilon}.$$

According to the calculations above, if ω is very small and Ω is close to 1 with $\epsilon < 1$, then our proposal is resistant to quantum attacks.

7. Performance Evaluation

In this section, we evaluate and compare the performance evaluation of our proposal and recent existing schemes such as those of Ali et al. [15], Cui et al. [24], and Al-Shareeda et al. [20]. Some notations used in this section are as follows.

- T_{bp} : The runtime taken to run a bilinear pairing computation. $T_{bp} = 5.811$ ms.
- M_{bp} : The runtime taken to run a scalar multiplication operation on the bilinear group. $M_{bp} = 1.5654$ ms.
- A_{bp} : The runtime taken to run a point addition operation on the bilinear group. $A_{bp} = 0.0106$ ms.
- h : The runtime taken to run a collision-resistant hash function. $h = 0.001$ ms.
- M_{ecc} : The runtime taken to run a scalar multiplication operation on the elliptic curve. $M_{ecc} = 0.6718$ ms.
- A_{ecc} : The runtime taken to run a point addition operation on the elliptic curve. $A_{ecc} = 0.0031$ ms.
- T_{nm} : The runtime taken to run a number multiplication. $T_{nm} = 1.409$ μ s.
- T_{na} : The runtime taken to run a number addition. $T_{na} = 1.18$ μ s.

Note that we can observe that the overhead of different cryptography operations follows the inequality $h < T_{nm} < M_{ecc} < M_{bp}$. The hardware platform used in this paper operated on a 64-bit Microsoft® Windows™ 10 operating system with a 2.20 GHz processor

and a 16.0 GB RAM-based Intel® Core™ i7-2670QM. The times required for T_{nm} and T_{na} were averaged over 10^5 trials, where the lattice dimension was 251 according to the NTRU standard [32,38]. Table 2 shows each operation over the existing schemes and the proposal in detail.

Table 2. Performance evaluation comparison.

Schemes	Signature Generation (ms)	Signature Generation (ms)	Batch Signature Verification (ms)
Ali et al. [15]	$\{2M_{bp} + A_{bp}\}$	$\{2T_{bp} + 1M_{bp}\}$	$\{2T_{bp} + nM_{bp}\}$
Cui et al. [24]	$\{3M_{ecc} + 3h\}$	$3M_{ecc} + A_{ecc} + 2h$	$(n + 2)M_{ecc} + (n - 1)A_{ecc} + 2nh$
Al-Shareeda et al. [20]	$\{1M_{ecc} + 2h\}$	$2M_{ecc} + A_{ecc} + 1h$	$2M_{ecc} + (n + 1)A_{ecc} + nh$
Our proposal	is $\{\alpha(\beta + 1)T_{nm} + \alpha \cdot T_{na} + \alpha \cdot 3h\}$	$\{\beta(\alpha + 1)(T_{nm}) + \beta \cdot T_{na} + \beta \cdot 2h\}$	$\{nT_{nm} + (2\beta + \alpha)(n - 1)T_{na} + nh\}$

7.1. Signature Generation

This subsection analyzes and evaluates the computation cost of signature generation. Figure 3 summarizes the comparison authentication schemes.

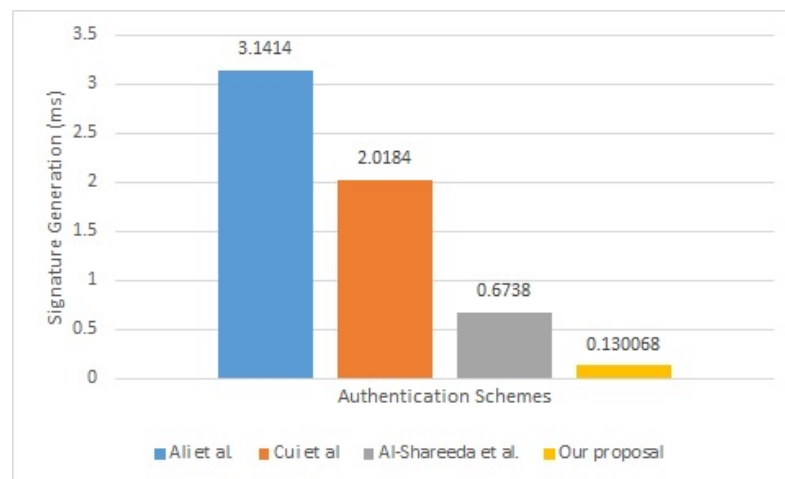


Figure 3. Computation cost of signature generation for authentication schemes.

In the scheme of Ali et al. [15], the user needs two scalar multiplication operations ($2M_{bp}$) on the bilinear group and one point addition operation A_{bp} to generate a signature of the message. Thus, the entire overhead is $\{2M_{bp} + A_{bp}\}$.

In the scheme of Cui et al. [24], the user needs three scalar multiplication operations $3M_{ecc}$ on an elliptic curve and three collision-resistant hash functions $3h$ to generate the signature of the message. Thus, the entire overhead is $\{3M_{ecc} + 3h\}$.

In the scheme of Al-Shareeda et al. [20], the user needs one scalar multiplication operation $1M_{ecc}$ on an elliptic curve and two collision-resistant hash functions $2h$ to generate the signature of the message. Thus, the entire overhead is $\{1M_{ecc} + 2h\}$.

In our proposal, the user needs number multiplication $\{\alpha(\beta + 1)(T_{nm})\}$, number addition $\{\alpha \cdot T_{na}\}$, and collision-resistant hash functions $\{\alpha \cdot 3h\}$ to generate the signature of a message. Thus, the entire overhead is $\{\alpha(\beta + 1)T_{nm} + \alpha \cdot T_{na} + \alpha \cdot 3h\}$.

7.2. Single Signature Verification

This subsection analyzes and evaluates the computation cost of single signature verification. Figure 4 summarizes the comparison authentication schemes.

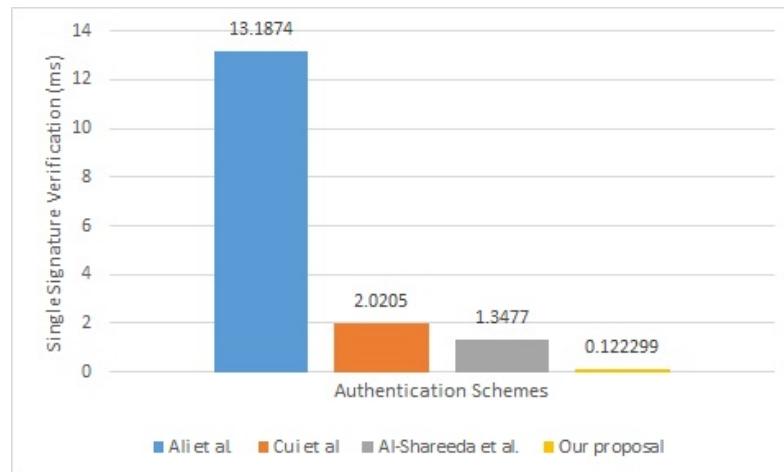


Figure 4. Computation cost of single signature verification for authentication schemes.

In the scheme of Ali et al. [15], the user needs two bilinear pairing operations $2T_{bp}$ and one scalar multiplication operation (M_{bp}) on the bilinear group to verify the single signature verification of message. Thus, the entire overhead is $\{2T_{bp} + 1M_{bp}\}$.

In the scheme of Cui et al. [24], the user needs three scalar multiplication operations $3M_{ecc}$ on an elliptic curve, one point addition operation A_{ecc} , and two collision-resistant hash functions $2h$ to verify the single signature verification of message. Thus, the entire overhead is $3M_{ecc} + A_{ecc} + 2h$.

In the scheme of Al-Shareeda et al. [20], the user needs two scalar multiplication operations $2M_{ecc}$ on an elliptic curve, one point addition operation A_{ecc} , and one collision-resistant hash function $1h$ to verify single signature verification of message. Thus, the entire overhead is $2M_{ecc} + A_{ecc} + 1h$.

In our proposal, the user needs number multiplication $\{\beta(\alpha + 1)(T_{nm})\}$, number addition $\{\beta \cdot T_{na}\}$, and collision-resistant hash functions $\{\beta \cdot 2h\}$ to verify the single signature verification of a message. Thus, the entire overhead is $\{\beta(\alpha + 1)(T_{nm}) + \beta \cdot T_{na} + \beta \cdot 2h\}$.

7.3. Batch Signature Verification

This subsection analyzes and evaluates the computation cost of batch signature verification. Figure 5 summarizes the comparison authentication schemes.

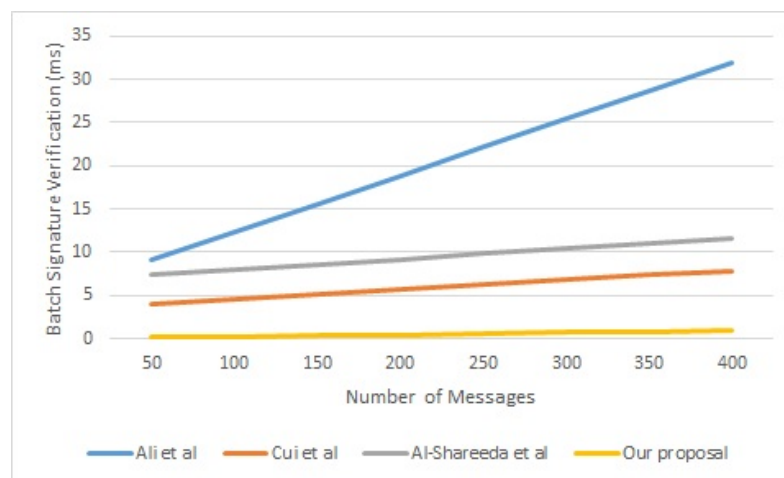


Figure 5. Computation cost of batch signature verification for authentication schemes.

In the scheme of Ali et al. [15], the vehicle needs two operations related to bilinear pairing $2T_{bp}$ and n scalar multiplication operations (nM_{bp}) on a bilinear group to verify the batch signatures verification of messages. Thus, the entire overhead is $\{2T_{bp} + nM_{bp}\}$.

In the scheme of Cui et al. [24], the vehicle requires $(n + 2)$ operations-based scalar multiplication $(n + 2)M_{ecc}$ on an elliptic curve, $(n - 1)$ operations-based point addition $(n - 1)A_{ecc}$, and $(2n)$ collision-resistant hash functions $2nh$ to verify the batch signatures verification of messages. Thus, the entire overhead is $(n + 2)M_{ecc} + (n - 1)A_{ecc} + 2nh$.

In the scheme of Al-Shareeda et al. [20], the vehicle requires two scalar multiplication operations $2M_{ecc}$ on the elliptic curve, $(n+1)$ point addition operations on the $(n + 1)A_{ecc}$, and (n) collision-resistant hash functions nh to verify the batch signatures verification of messages. Thus, the entire overhead is $2M_{ecc} + (n + 1)A_{ecc} + nh$.

In our proposal, the vehicle requires number multiplication $\{nT_{nm}\}$, number addition $\{(2\beta + \alpha)(n - 1)T_{na}\}$, and collision-resistant hash functions $\{nh\}$ to verify the batch signatures verification of messages. Thus, the entire overhead is $\{nT_{nm} + (2\beta + \alpha)(n - 1)T_{na} + nh\}$.

8. Conclusions

This paper has proposed a lattice-based lightweight quantum-resistant scheme in 5G-enabled vehicular networks. Our proposal applies matrix multiplication rather than operations-based cryptographies of the elliptic curve or bilinear pair to generate and verify signatures of messages sent among vehicles. Since these operations-based elliptic curves or bilinear pair are not used to sign and verify messages, our proposal satisfies a significant reduction in the performance, which makes it lightweight enough to handle quantum attacks. Our proposal is based on 5G technology that has the responsibility to connect between the TA and vehicles within its wide-range communication domain by using the 5G standard. Security analysis showed that our proposal satisfies privacy and security properties as well as resisting quantum attacks. Lastly, this work also shows convenient performance compared to most recent schemes.

In future work, we will expand this research by utilizing fog computing to overcome the assumption that the TPD is hard and strong.

Author Contributions: Conceptualization, funding acquisition, visualization, resources, Z.G.A.-M.; Conceptualization, project administration, writing—review and editing, M.A.A.-S.; writing—original draft preparation, investigation, supervision, investigation, S.M.; funding acquisition, software, validation, methodology, B.A.M.; methodology, project administration, funding acquisition, software, A.Q. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been funded by Deputy for Research and Innovation, Ministry of Education, through the Initiative of Institutional Funding at the University of Ha'il, Saudi Arabia, through project number IFP-22 006.

Data Availability Statement: Not Applicable.

Acknowledgments: We would like to acknowledge the Deputy for Research and Innovation, Ministry of Education through the Initiative of Institutional Funding at University of Ha'il, Saudi Arabia, for funding this research.

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

References

1. Khan, A.R.; Jamlos, M.F.; Osman, N.; Ishak, M.I.; Dzaharudin, F.; Yeow, Y.K.; Khairi, K.A. DSRC technology in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) IoT system for Intelligent Transportation System (ITS): A review. In *Recent Trends in Mechatronics Towards Industry 4.0*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 97–106.
2. Al-Shareeda, M.A.; Manickam, S. COVID-19 Vehicle Based on an Efficient Mutual Authentication Scheme for 5G-Enabled Vehicular Fog Computing. *Int. J. Environ. Res. Public Health* **2022**, *19*, 15618. [\[CrossRef\]](#)
3. Jabbar, R.; Dhib, E.; ben Said, A.; Krichen, M.; Fetais, N.; Zaidan, E.; Barkaoui, K. Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review. *IEEE Access* **2022**, *10*, 20995–21031. [\[CrossRef\]](#)
4. Cao, Y.; Xu, S.; Chen, X.; He, Y.; Jiang, S. A forward-secure and efficient authentication protocol through lattice-based group signature in VANETs scenarios. *Comput. Netw.* **2022**, *214*, 109149. [\[CrossRef\]](#)
5. Li, F.; Cui, Y.; Wang, J.; Zhou, H.; Wang, X.; Yang, Q. Lattice-based batch authentication scheme with dynamic identity revocation in VANET. *Int. J. Intell. Syst.* **2022**, *37*, 9442–9460. [\[CrossRef\]](#)

6. Loskot, P. Mobile Networks: 5G and Beyond. In *Emerging Computing Paradigms: Principles, Advances and Applications*; Wiley: Hoboken, NJ, USA, 2022; pp. 161–175.
7. Ali, I.; Lawrence, T.; Omala, A.A.; Li, F. An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 11266–11280. [[CrossRef](#)]
8. Hamdan, M.A.; Maklouf, A.M.; Mnif, H. Review of Authentication with Privacy-preserving Schemes for 5G-enabled Vehicular Networks. In Proceedings of the 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022; pp. 1–6.
9. Ali, I.; Gervais, M.; Ahene, E.; Li, F. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. *J. Syst. Archit.* **2019**, *99*, 101636. [[CrossRef](#)]
10. Marwah, G.P.K.; Jain, A. A hybrid optimization with ensemble learning to ensure VANET network stability based on performance analysis. *Sci. Rep.* **2022**, *12*, 10287. [[CrossRef](#)] [[PubMed](#)]
11. Al-Shareeda, M.A.; Manickam, S.; Laghari, S.A.; Jaisan, A. Replay-Attack Detection and Prevention Mechanism in Industry 4.0 Landscape for Secure SECS/GEM Communications. *Sustainability* **2022**, *14*, 15900. [[CrossRef](#)]
12. Chen, L.; Tu, T.; Yu, K.; Zhao, M.; Wang, Y. V-LDAA: A New Lattice-Based Direct Anonymous Attestation Scheme for VANETs System. *Secur. Commun. Netw.* **2021**, *2021*, 4660875. [[CrossRef](#)]
13. Balen, J.; Tomasic, B.; Semialjac, K.; Varga, H. Survey on using 5G technology in VANETs. In Proceedings of the 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 23–27 May 2022; pp. 442–448.
14. Yang, Y.; Zhang, L.; Zhao, Y.; Choo, K.K.R.; Zhang, Y. Privacy-preserving aggregation-authentication scheme for safety warning system in Fog-Cloud based VANET. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 317–331. [[CrossRef](#)]
15. Ali, I.; Chen, Y.; Ullah, N.; Afzal, M.; Wen, H. Bilinear pairing-based hybrid signcryption for secure heterogeneous vehicular communications. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5974–5989. [[CrossRef](#)]
16. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. SE-CPPA: A Secure and Efficient Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks. *Sensors* **2021**, *21*, 8206. [[CrossRef](#)] [[PubMed](#)]
17. Bayat, M.; Barmshoory, M.; Pournaghi, S.M.; Rahimi, M.; Farjami, Y.; Aref, M.R. A new and efficient authentication scheme for vehicular ad hoc networks. *J. Intell. Transp. Syst.* **2020**, *24*, 171–183. [[CrossRef](#)]
18. Pournaghi, S.M.; Zahednejad, B.; Bayat, M.; Farjami, Y. NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. *Comput. Netw.* **2018**, *134*, 78–92. [[CrossRef](#)]
19. Alshudukhi, J.S.; Mohammed, B.A.; Al-Mekhlafi, Z.G. An efficient conditional privacy-preserving authentication scheme for the prevention of side-channel attacks in vehicular ad hoc networks. *IEEE Access* **2020**, *8*, 226624–226636. [[CrossRef](#)]
20. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. A Secure Pseudonym-Based Conditional Privacy-Preservation Authentication Scheme in Vehicular Ad Hoc Networks. *Sensors* **2022**, *22*, 1696. [[CrossRef](#)]
21. Zhang, J.; Cui, J.; Zhong, H.; Chen, Z.; Liu, L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 722–735. [[CrossRef](#)]
22. Cui, J.; Zhang, X.; Zhong, H.; Ying, Z.; Liu, L. RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks. *IEEE Internet Things J.* **2019**, *6*, 6417–6428. [[CrossRef](#)]
23. Alshudukhi, J.S.; Al-Mekhlafi, Z.G.; Mohammed, B.A. A Lightweight Authentication with Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography. *IEEE Access* **2021**, *9*, 15633–15642. [[CrossRef](#)]
24. Cui, J.; Chen, J.; Zhong, H.; Zhang, J.; Liu, L. Reliable and Efficient Content Sharing for 5G-Enabled Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *23*, 1247–1259. [[CrossRef](#)]
25. Al-Shareeda, M.A.; Anbar, M.; Alazzawi, M.A.; Manickam, S.; Al-Hiti, A.S. LSWBVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network. *IEEE Access* **2020**, *8*, 170507–170518. [[CrossRef](#)]
26. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Yassin, A.A. Vppcs: Vanet-based privacy-preserving communication scheme. *IEEE Access* **2020**, *8*, 150914–150928. [[CrossRef](#)]
27. Cui, J.; Xu, W.; Han, Y.; Zhang, J.; Zhong, H. Secure mutual authentication with privacy preservation in vehicular ad hoc networks. *Veh. Commun.* **2020**, *21*, 100200. [[CrossRef](#)]
28. Zhang, J.; Zhong, H.; Cui, J.; Tian, M.; Xu, Y.; Liu, L. Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 7940–7954. [[CrossRef](#)]
29. Ajtai, M. Generating hard instances of lattice problems. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 99–108.
30. Ajtai, M.; Dwork, C. The first and fourth public-key cryptosystems with worst-case/average-case equivalence. In *Electronic Colloquium on Computational Complexity (ECCC)*; Citeseer: Princeton, NJ, USA, 2007; Volume 14.
31. Hoffstein, J.; Pipher, J.; Silverman, J.H. NSS: An NTRU lattice-based signature scheme. In *International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 211–228.
32. Dharminder, D.; Mishra, D. LCPPA: Lattice-based conditional privacy preserving authentication in vehicular communication. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3810. [[CrossRef](#)]
33. Han, L.; Cao, S.; Yang, X.; Zhang, Z. Privacy protection of VANET based on traceable ring signature on ideal lattice. *IEEE Access* **2020**, *8*, 206581–206591. [[CrossRef](#)]

34. Jiao, C.; Xiang, X. Anti-Quantum Lattice-Based Ring Signature Scheme and Applications in VANETs. *Entropy* **2021**, *23*, 1364. [[CrossRef](#)] [[PubMed](#)]
35. Tzalenchuk, A.; Lara-Avila, S.; Kalaboukhov, A.; Paolillo, S.; Syväjärvi, M.; Yakimova, R.; Kazakova, O.; Janssen, T.; Fal'Ko, V.; Kubatkin, S. Towards a quantum resistance standard based on epitaxial graphene. *Nat. Nanotechnol.* **2010**, *5*, 186–189. [[CrossRef](#)]
36. Hu, J.; Rigosi, A.F.; Kruskopf, M.; Yang, Y.; Wu, B.Y.; Tian, J.; Panna, A.R.; Lee, H.Y.; Payagala, S.U.; Jones, G.R.; et al. Towards epitaxial graphene pn junctions as electrically programmable quantum resistance standards. *Sci. Rep.* **2018**, *8*, 15018. [[CrossRef](#)]
37. Liu, Z.Y.; Tseng, Y.F.; Tso, R.; Mambo, M.; Chen, Y.C. Public-key authenticated encryption with keyword search: A generic construction and its quantum-resistant instantiation. *Comput. J.* **2022**, *65*, 2828–2844. [[CrossRef](#)]
38. Liu, H.; Sun, Y.; Xu, Y.; Xu, R.; Wei, Z. A secure lattice-based anonymous authentication scheme for VANETs. *J. Chin. Inst. Eng.* **2019**, *42*, 66–73. [[CrossRef](#)]

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.