Hindawi
Security and Communication Networks
Volume 2021, Article ID 4660875, 13 pages
https://doi.org/10.1155/2021/4660875

Research Article

V-LDAA: A New Lattice-Based Direct Anonymous Attestation Scheme for VANETs System

Liquan Chen,[1,2] **Tianyang Tu**,[1] **Kunliang Yu**,[1] **Mengnan Zhao**,[1] **and Yingchao Wang**[1]

[1]*School of Cyber Science and Engineering, Southeast University, Nanjing, China*
[2]*Purple Mountain Laboratories for Network Communication and Security, Nanjing, China*

Correspondence should be addressed to Liquan Chen; lqchen@seu.edu.cn

Received 10 June 2021; Accepted 12 August 2021; Published 2 September 2021

Academic Editor: Jinguang Han

Copyright © 2021 Liquan Chen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Privacy protection and message authentication issues in VANETs have received great attention in academia. Many authentication schemes in VANETs have been proposed, but most of them are based on classical difficult problems such as factorization in RSA setting or Elliptic Curve setting and are therefore not quantum resistant. If a quantum computer becomes available in the next few decades, the security of these schemes will be at stake. This paper presents a vehicular lattice-based direct anonymous attestation (V-LDAA) scheme adopting an optimized signature scheme based on automorphism stability which achieves postquantum security. A distributed pseudonym update and vehicle revocation mechanism based on the lattice is introduced in this paper, which means vehicles can update their pseudonyms and revoke the identity certificate by themselves without the need for pseudonym resolutions or CRLs checking. Compared with the existing lattice-based attestation schemes in VANETs, computation costs during signing and verification operations in V-LDAA are no longer related to the number of users, which makes it suitable for large-scale VANETs. Security analysis shows that V-LDAA resists TPM theft attacks and provides users with user-controlled anonymity, user-controlled unlinkability, and unforgeability against quantum adversaries. Experimental results show that V-LDAA reduces the blind signature size by 18%. The speed of blind signing is increased by 30%, and blind verification operation is accelerated 3 times compared with the existing lattice-based direct anonymous attestation (LDAA) scheme.

1. Introduction

The Intelligent Transportation System (ITS) provides vehicles with intelligent and efficient services, such as collision avoidance, traffic condition reports, and entertainment services, etc. Messages are sent to various network nodes through vehicular ad hoc networks (VANETs) [1]. VANET is a key facility of an intelligent transportation system, which is composed of Certification Authority (CA), roadside units (RSUs), and on-board units (OBUs) [2]. Among them, the OBU is responsible for supporting the V2I communication between the roadside units and the vehicle and V2V communication between vehicles. These nodes are connected to each other to form a network, and the communications in the entire network are achieved through the information transferring among adjacent nodes. The key issue that needs to be solved in the implementations for ITS is how to protect the security and privacy of users in VANETs. Vehicle users in ITS need to send information about their location, speed, and other driving conditions, or traffic jams, icy roads, and other surrounding road conditions to adjacent users. If this information is maliciously tracked or tampered with by an adversary, it will cause serious privacy leakage accidents and even threaten the life of the driver. For example, the adversary can obtain the real location information of the vehicle by tracing the navigation route information or modify the traffic information, which may lead to traffic paralysis or even serious traffic accidents. Therefore, an anonymous attestation protocol in VANETs needs to be established to ensure the anonymity of users and the integrity and untraceability of messages.

In addition, with the development of quantum computing technology, the security of traditional public key cryptosystems has received an impact. Most of the existing

authentication protocols in VANETs have their security supported on classic difficult problems such as factorization in RSA setting or Elliptic Curve setting. Under traditional computing conditions, these difficult problems can only be solved in exponential or subexponential time. However, according to Shor's algorithm, quantum computers can efficiently solve these problems, leading to the failure of traditional cryptosystems. Thus, there is a need to introduce quantum-resistant authentication schemes in VANETs.

We have proposed the following major contributions in this paper.

(1) A vehicular lattice-based direct anonymous attestation scheme that achieves postquantum security is proposed in this paper. In this scheme, a lattice-based distributed pseudonym update and certificate revocation mechanism is introduced. By embedding a trusted platform module (TPM) in each vehicle, trust is distributed from Certification Authority (CA), pseudonym provider (PP), Revocation Authority (RA), and other authoritative institutions to each legitimate user, transforming a centralized trust system into a distributed trust system. "Distributed trust" is reflected in the processes of pseudonym update and vehicle revocation. Users can generate pseudonyms by themselves without the need for regular updates and distributions by PP. TPM performs the revocation operation independently, without RA performing pseudonym resolution operations, and there is no need to maintain the certificate revocation lists CRLs. Moreover, the calculation costs in signing operations are no longer related to the number of members. Thus, it is more suitable for large-scale VANETs.

(2) V-LDAA optimizes the signature scheme based on automorphism stability which is used in the *BlindSign* and *BlindVerify* protocols of the original LDAA scheme. The optimized signature scheme reduces the number of automorphisms that need to be proven stable, which simplifies the processes of signing and verification and reduces the signature size. Based on the experimental implementation of the V-LDAA scheme, the high computation and storage efficiency of the proposed scheme is confirmed.

(3) V-LDAA binds TPM and Host to jointly generate an identity certificate in Join protocol to resist TPM theft attacks. This is important in VANETs because it prevents TPM from being transplanted to a new vehicle platform by an adversary and signed with the replaced identity certificate.

The rest of this paper is organized as follows. We first introduce related works, the background knowledge, an optimized signature scheme used in V-LDAA and VANET architectures based on V-LDAA. Then, the construction of the proposed V-LDAA scheme is described. After that, security and performance analysis are detailed. Finally, the conclusion of this paper is presented.

2. Related Works

In recent years, research studies on authentication schemes mainly focused on the following aspects. The first is based on a symmetric key mechanism [2]. The sender uses a shared key to generate the message authentication code (MAC), while the receiver verifies it before accepting the message. However, because both parties need to share the private key, the mechanism based on message authentication code cannot withstand a large number of node tampering attacks in the network. In addition, the adversary can cheat any individual node to obtain the private key, which can be used for message authentication. The second is an identity-based encryption system [3, 4], where the trusted authority is responsible for the generation and distribution of public and private key pairs for legitimate members. However, under this mechanism, the adversary can easily obtain the user's real identity from the signature and track the signature. The third one is an authentication scheme based on vehicle public key infrastructures (VPKIs), which is also the design idea of this paper. CA is responsible for registering and managing long-term identity certificates of members, while members sign messages through short-term pseudonym certificates. The VPKIs scheme can meet the anonymity property and provide a pseudonym mechanism, but there are still many shortcomings. In this scheme, the security risk and computation burden are caused by different pseudonym update strategies. In order to prevent users from being maliciously tracked, CA needs to change pseudonyms for all users regularly [1]. In the case of unconditional security, the pseudonym should be changed every time the signature is signed, which causes a huge computational and storage burden when PP generates new pseudonym certificates and distributes them to every legitimate user periodically. In [5], an optimized pseudonym update scheme is proposed, but its computation costs still burden the vehicle and the Pseudonym Provider (PP). In addition, in order to revoke the identity certificate of an illegal vehicle, the Revocation Authority (RA) needs to resolute the user's long-term identity ID value from the user's pseudonym and save it to certificate revocation lists (CRLs) for all users to query. The update, query, maintenance, and storage of CRLs cause heavy computation and storage costs.

The existing authentication schemes for VANETs which achieve postquantum security are mainly lattice-based ring signature schemes [6–8]. In the lattice-based ring signature scheme, each member needs to use its private key and the public keys of all other members to sign the message, and the members in a ring need to change with the specific driving position of the vehicle. In recent years, several lattice-based direct anonymous attestation (LDAA) schemes are proposed by updating the cryptographic primitives to be quantum resistant in direct anonymous attestation (DAA) [9–11]. The

first LDAA in [9] is based on a lattice-based MAC scheme and a CMA-secure digital signature scheme, but it suffers from high computation costs in signing protocol. LDAA in [10] adopts a noninteractive sigma protocol construction and a modified Boyen's signature scheme, which can improve signing and storage efficiency compared to LDAA in [9]. Among them, the lattice-based direct anonymous attestation in [11] is most suitable for a future quantum-resistant TPM for its high efficiency. LDAA becomes an interesting candidate for the postquantum secure authentication protocol in VANETs because of its balance in authentication and anonymity.

3. Preliminaries

3.1. Notation. Symbols used in this paper are illustrated in Table 1 with their definitions.

3.2. Trapdoor Sampling. Sample two short vectors s_1, s_2 satisfying

$$[\mathbf{a} \mid \mathbf{b} + i[1\sqrt{q}\,]] \cdot \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = u + \mathbf{a}_2 \cdot \mathbf{e}, \tag{1}$$

where i is a nonzero element in $\mathbb{Z}_q$. According to [12], there is a set of basis $\mathbf{S} \in \mathbb{Z}^{4\,d\times 4\,d}$ for $\Lambda^{\perp} = \{x \in \mathscr{R}^4 \mid [\mathbf{a}|\mathbf{b} + i \cdot [1\sqrt{q}\,]] \cdot \mathbf{x} \equiv 0 (\mathrm{mod}\, q)\}$. The Gram–Schmidt orthogonalization of $\mathbf{S} \in \mathbb{Z}^{4\,d\times 4\,d}$ satisfies $\|\tilde{\mathbf{S}}\| \le (s_1(\mathbf{R}+1))\sqrt{\delta^2+1}$ with $\delta = \sqrt{q}$. To sample s_1, s_2, first calculate an arbitrary solution (not necessarily short solutions) that satisfies (1). Then express it in basis $\mathbf{S}$, and use the randomized nearest plane discrete Gaussian sampling algorithm in [13] to get solutions distributed as the discrete Gaussian distribution with $s = 2 \cdot \|\tilde{\mathbf{S}}\| \le 2(3\sqrt{d}+1)\sqrt{\delta^2+1}$. The algorithm is called MP − Sampler.

3.3. Lattice-Based Commitment Scheme. We use the commitment scheme from [14] with M-LWE based hiding property and M-SIS based binding property. Define public parameters $\mathbf{A}_1 \in \mathscr{R}_{q_1}^{1\times k}$, $\mathbf{A}_2 \in \mathscr{R}_{q_2}^{l\times k}$, where $\mathbf{A}_1 = [\,1 \;\; \mathbf{A}_1'\,], \mathbf{A}_1' \xleftarrow{\$}$ and $\mathbf{A}_2 = [\,0^l \;\; \mathbf{I}_l \;\; \mathbf{A}_2'\,], \mathbf{A}_2' \xleftarrow{\$}$. To commit to a message $m \in \mathscr{R}_{q_2}^{l\times l}$, sample $\mathbf{r} \xleftarrow{\$}$ and compute $\mathrm{Com}(m;r) = \begin{bmatrix} \mathbf{t}_1 \\ \mathbf{t}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{bmatrix}\mathbf{r} + \begin{bmatrix} 0 \\ \mathbf{m} \end{bmatrix}$. If there exists $\mathbf{r} \le B_{\mathrm{com}}$ and $c \in \mathscr{R}$ satisfying $c\begin{bmatrix} \mathbf{t}_1 \\ \mathbf{t}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{bmatrix}\mathbf{r} + c\begin{bmatrix} 0 \\ \mathbf{m} \end{bmatrix}$, then the opening $\begin{bmatrix} \mathbf{t}_1 \\ \mathbf{t}_2 \end{bmatrix}$ is valid.

3.4. Lattice-Based Zero-Knowledge Proof. Lattice-based encryption schemes usually include a public A and small coefficient secret value e, which satisfies $Ae = t$. In order to prove that t is a legal ciphertext, a zero-knowledge proof about e needs to be generated, which satisfies $Ae = t$. There are several protocols to achieve zero-knowledge proof about e. The first one is based on a Stern-type protocol to prove a norm bounded e satisfying exactly $Ae = t$, which is the most accurate but also the most expensive protocol. In V-LDAA, this method can be used in the zero-knowledge proof of TPM and Host secret values in the Join phase because each user only needs to perform it once in the entire certificate lifecycle. The second is to use rejection sampling and lattice-based Fiat–Shamir [15], which proves that $Ae\prime = ct$, where $c$is the difference between two challenge values.

4. An Optimized Signature Scheme Based on Automorphism Stability of the Cyclotomic Field

The signature schemes of the LDAA schemes in [9, 10] both use Boyen's signature framework under the standard security model [16]. Although there are studies using polynomial lattices to improve the efficiency of Boyen's signature mechanism [17], the size of its group signature is still around 50 MB [18]. The LDAA framework proposed in [11] uses a selectively secure signature mechanism based on the lattice [19]. The so-called selective security refers to the security of messages that can be fixed in advance (fixed before the attacker communicates with the system). In the case of selectively secure, in order to prove the security of the message to be signed, we have to prove the invertibility of the signed message μ and its stability in a special subset. In [19], a Galois extension of the cyclotomic field was used to prove that μ belongs to a certain subset and is invertible. In this paper, we optimize the selective-secure signature scheme used in [11], reducing the number of automorphisms that need to be proven stable from two to one.

4.1. Galois Group of Cyclotomic Rings. If $T^n - 1$ is separable from K , then $K(\mu_n)$ is the splitting field of $T^n - 1$ on K and $K(\mu_n)/K$ is called a Galois extension. Suppose $K = \mathbb{Q}[X]/(\Phi_m(X))$ is a m^{-th} cyclotomic field of degree $d = \varphi(m)$ with an integer ring$\mathscr{R} = \mathbb{Z}[X]/(\Phi_m(X))$ and its subring $\mathscr{S} \subset \mathscr{R}$. Then, the Galois group G is defined as $G = \mathrm{Gal}(K/\mathbb{Q})$, which consists of all automorphisms of K. The Galois group on the cyclotomic field is isomorphic to $\mathbb{Z}_m^{\times}$, that is $j \mapsto \sigma_j$: $\mathbb{Z}_m^{\times} \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$ where $\sigma_j(X) = X^j$. For the subfield $L \subset K$, there must be a subgroup $H < G$ which is the Galois group K on L, that is $H = \mathrm{Gal}(K/L) = \{\sigma \in G | \sigma(x) = x\, \forall x \in L\}$. According to [19], if $\mu \in \mathscr{R}_q$ satisfies $\sigma(\mu) \equiv \mu (\mathrm{mod}\, q\mathscr{R})$ for all $\sigma \in H$, then μ is in the subfield S_q of $\mathscr{R}_q$. Thus, in order to prove $\mu \in \mathscr{S}_q$, we need to prove the stability of μ by all Galois automorphisms in H. In other words, we need to prove the stability of μ under the generators of H.

4.2. Power-of-Two Cyclotomic Rings. Suppose $K = \mathbb{Q}[X]/(X^d + 1)$ is a power-of-two cyclotomic fields, we get$G = \mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_{2\,d}^{\times} \cong \mathbb{Z}_2 \times \mathbb{Z}_{d/2}$, which is generated by σ_{-1} and σ_5, that is $G = \langle \sigma_{-1}, \sigma_5 \rangle$. Consider a subgroup $H = \langle \sigma_{-1}, \sigma_5^k \rangle$, according to [19], the fixed field L of H is generated by $\alpha = X^{d-(d/2k)} - X^{d/2k}$. Consider the parameter used in [11] when $k = 1$, then $H = G = \langle \sigma_{-1}, \sigma_5 \rangle$ and the corresponding fixed field $L = \mathbb{Q}$ and $\mathscr{S}_q = \mathbb{Z}_q$. For every prime number q,

Table 1: Notation.

Notation	Description
$\mathbb{Z}_q$	Quotient ring Z/qZ
q	The moduli used in the commitment scheme
$K = \mathbb{Q}[X]/(X^d + 1)$	A cyclotomic ring
d	The dimension of ring K
$y \longleftarrow D$	y is drawn according to the distribution D
$G = \mathrm{Gal}(K/\mathbb{Q})$	The Galois group of K over $\mathbb{Q}$
$G = \langle \sigma_{-1}, \sigma_5 \rangle$	Galois group G is generated by σ_{-1} and σ_5
N	The number of users
e	Lowercase bold letters denote a vector of polynomials
A	Capital bold letters denote a matrix whose entities are polynomials

$\mathcal{S}_q$ is a field. In this case, it is enough to prove that the message $\mu \in \mathcal{R}_q$ remains unchanged under σ_{-1} and σ_5. This means that every time the zero-knowledge proof of the identity certificate is performed, similar calculations have to be repeated twice (on σ_{-1} and σ_5), which increases the computational complexity of the protocol and the size of the commitments.

In this paper, we change the subfield to $k = 2$, which means $H = \langle \sigma_{-1}, \sigma_5^2 \rangle$ or $H = \langle \sigma_5 \rangle$. When $H = \langle \sigma_5 \rangle$, the generator of its fixed field L is $\alpha = X^{d/2}$ and the minimal polynomial is $Y^2 + 1$. In this case, only one automorphism stability σ_5 needs to be proved during zero-knowledge proof. We select $\mu \in \mathcal{S}_q$, where $\mathcal{S}_q = \{c_0 + c_1 X^{d/2} \in \mathcal{R}_q | c_0, c_1 \in \mathbb{Z}_q\}$ of size q^2 and $q \equiv 3 \pmod 4$. When TPM chooses its identity value, it computes $\mu = c_0 + c_1\alpha = c_0 + c_1 X^{d/2} \in \mathcal{R}_q$ with arbitrary $c_0, c_1 \in \mathbb{Z}_q$ and proves that μ remains unchanged under $\sigma_5(\mu) = \mu$. The process of signing and verification is shown in Table 2.

5. VANET Architectures Based on V-LDAA

The traditional VPKI is shown in Figure 1, which is composed of a Certification Authority (CA), a pseudonym provider (PP), a vehicle Revocation Authority (RA), and user vehicles. The vehicle registers its identity with CA, and CA signs the long-term identity certificate VID to the vehicle after confirming that the vehicle is in a trustworthy state. After the vehicle shows VID to the pseudonym provider PP, PP generates a pseudonym certificate based on VID and issues it to the vehicle user. During V2V communication, the illegal behavior of the vehicle will be reported to PP, and PP will determine whether to revoke the user certificate. When deciding to revoke the user certificate, RA cooperates with PP and CA to resolute the pseudonymous certificate to obtain the user's real identity ID. The violation ID is updated to the certificate revocation lists (CRLs). Every time before the user verifies the signature, it needs to first check whether the sender is in the CRLs. The main shortcomings of the traditional VPKI architecture are high storage and calculation consumption for updating, maintaining and querying CRLs; pseudonym resolution is required when certificate revocation, computing efficiency, and security issues are brought by PP's regular update of pseudonym certificates, etc.

VANET architecture based on V-LDAA is shown in Figure 2. Compared with the traditional VPKI system, a hardware chip TPM is embedded in each user's vehicle platform. Through the identity certificate, we distribute trust from CA to TPM embedded in each legitimate user, transforming a centralized trust system into a distributed trust system. "Distributed Trust" is reflected in the processes of pseudonym update and vehicle revocation. Users can generate pseudonyms by themselves without the need for regular updates and distribution by PP. During certificate revocation, RA only needs to broadcast the revocation instruction of a certain vehicle, while the target vehicle will check its identity, perform the revocation operation, and return the revocation certificate to RA. The whole process does not involve any pseudonym resolution or operations related to the revocation list CRLs.

6. Proposed V-LDAA Scheme

Based on the LDAA scheme in [11], we propose a V-LDAA scheme in VANETs. The overall V-LDAA scheme includes Setup, Join, Create, Sign/verify, Revoke protocols. The structure of the DAA protocol is redesigned. After the Join phase, each user needs to pass through the Create phase to generate identity credentials $\mathrm{PSCert} = (\mathrm{nym} \| \mathrm{sig}_1 \| \mathrm{sig}_2)$, where *nym* is a pseudonym public key, sig_1 is the certificate used to determine the identity when the certificate is revoked, and sig_2 is a blind signature on VID used to verify the identity of its legitimate users. Users can complete the anonymous authentication of the message and the self-revocation of the certificate by holding *PSCert*. TPM executes the destruction operation of the identity certificate and the pseudonymous certificate, generates the revocation certificate, and returns it to RA. RA verifies the identity certificate and the revocation certificate and confirms that the target vehicle has revoked its identity certificate.

Moreover, we optimize the signature scheme based on automorphism stability of the power-of-two cyclotomic fields. When the user interacts with the CA to generate the VID, the identity ID is selected in the more optimal $k = 2$ cyclotomic field, where $\mathcal{S}_q = \{c_0 + c_1 X^{d/2} \in \mathcal{R}_q | c_0, c_1 \in \mathbb{Z}_q\}$. At this time, it is enough to prove automorphism stability once instead of twice as in [11], which optimizes the computational efficiency and signature size during *Blind-Sign*. Finally, in the Join phase, the platform secret value sent to CA is changed to be generated by TPM and Host together instead of TPM alone. This is very important in VANETs, because the TPM chip embedded in the vehicle may be in an unmanned environment, and the adversary can directly steal

Table 2: An optimized signature scheme based on automorphism stability of the cyclotomic field.

Signer			Verifier	
	Message: $M \in \{0,1\}^*$ Public: $\mathbf{t}, \sigma_5$ Private: $\mathbf{r}$			Message: $M \in \{0,1\}^*$ Public: $\mathbf{t}, \sigma_5$
$y, y_5 \longleftarrow D_\xi^3$ $\mathbf{W}_1 = \mathbf{a}_1^T \mathbf{y}$ $\mathbf{W}_{1,5} = \sigma_5^{-1}(\mathbf{a}_1^T)\mathbf{y}_5$ $\mathbf{W}_{2,5} = \mathbf{a}_2^T \mathbf{y} - \sigma_5^{-1}(\mathbf{a}_2^T)\mathbf{y}_5$ $c = \mathbf{H}(\mathbf{t}, \sigma_5, \mathbf{W}_1, \mathbf{W}_{1,5}\mathbf{W}_{2,5}, M)$ $\mathbf{z} = \mathbf{r}c + \mathbf{y}$ $\mathbf{z}_5 = \sigma_5^{-1}(\mathbf{r})c + \mathbf{y}_5$ if rej$([\mathbf{z}\|\mathbf{z}_5], [\mathbf{r}c\|\sigma_5^{-1}c], \xi) = 1$, abort		$\xrightarrow{z, z_5}$		$\mathbf{W}_1' = \mathbf{a}_1^T \mathbf{z} - t_1 c$ $\mathbf{W}_{1,5}' = \sigma_5^{-1}(\mathbf{a}_1^T)\mathbf{z}_5 - \sigma_5^{-1}(t_1)c$ $\mathbf{W}_{2,5}{}' = \mathbf{a}_2^T \mathbf{z} - \sigma_5^{-1}(\mathbf{a}_2^T)\mathbf{z}_5$ if $\|z\|, \|z_5\| \le \beta_z$ and $c = \mathbf{H}(\mathbf{t}, \sigma_5, \mathbf{W}_1', \mathbf{W}_{1,5}'\mathbf{W}_{2,5}', M)$ Output 1 else Output 0

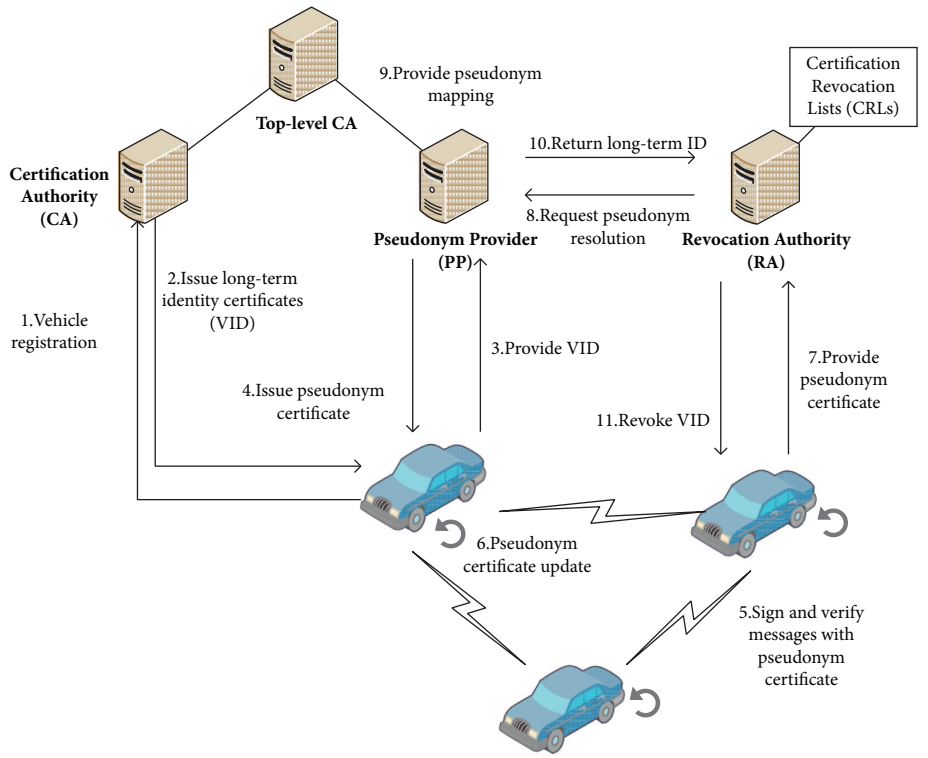

Figure 1: Traditional VPKI architectures.

the TPM chip and transplant it to another Host platform to cheat the verifier.

6.1. Setup. We consider a cyclotomic ring $\mathcal{R} = \mathbb{Z}[X]/(X^d + 1)$, $k = 2$ and identity ID in VID $i \in \mathcal{S}_q = \{c_0 + c_1 X^{d/2} \in \mathcal{R}_q | c_0, c_1 \in \mathbb{Z}_q\}$, which keeps stable under σ_5. Randomly choose $\mathbf{a}_t = [a_1 \ a_2]$ as TPM public parameters, $\mathbf{a}_h = [a_3 \ a_4]$ as Host public parameters and $u \leftarrow R_q$ as CA public parameter. The private key of CA is a trapdoor $\mathbf{R} \leftarrow R^{2\times 2}$ while the public key is $a \leftarrow R_q$, $\mathbf{b} = [a \ 1]\mathbf{R}$. By Ring-LWE assumption, $(a, \mathbf{b})$ is indistinguishable from uniform. Thus, we write CA public key as $[\mathbf{a}|\mathbf{b}]$, where $\mathbf{a} = [a \ 1]$.

6.2. Join. TPM randomly select a secret value $\mathbf{e} = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} \leftarrow R_3^2$ and a private key $sk \in \{0,1\}^{256}$. Compute $u_t = \mathbf{a} \cdot \mathbf{e} = a_1 e_1 + a_2 e_2$ and send u_t to the Host. Similarly, the Host chooses its secret $\mathbf{e}' = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} \leftarrow R_3^2$ and computes $u_h = a_3 e_3 + a_4 e_4$. Then,

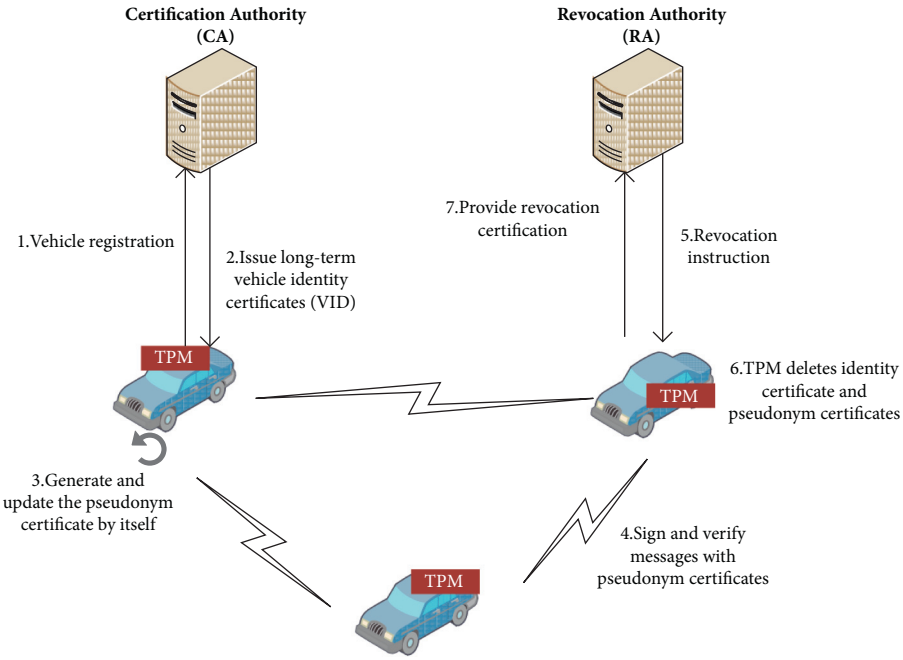

Figure 2: VANET architecture based on V-LDAA.

the Host adds u_t and u_h to generate u_1. TPM and Host jointly give a zero-knowledge proof π_1 of short $\mathbf{e}$ and e'. (u_1, π_1) is sent by Host to CA. Because the Join protocol only needs to be executed once, the calculation of zero-knowledge proof has little effect on the efficiency of the entire protocol. We can choose the "Stern-type" protocol with the largest amount of calculation but the most accurate. CA first confirms the zero-knowledge proof and then uses MP – sampleralgorithm to sample $s = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$ satisfying $[\mathbf{a}|\mathbf{b} + i \cdot [1|\sqrt{q}]] \cdot \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = u + u_1$. Note that $i \in \mathcal{S}_q = \{c_0 + c_1 X^{d/2} \in \mathcal{R}_q | c_0, c_1 \in \mathbb{Z}_q\}$ instead of an arbitrary $i \in R_q$. Finally, CA sends the generated identity certificate (s, i) to the Host and the Host saves it as VID.

6.3. Create. The Create protocol generates *PScert* for vehicles to send and receive messages in VANETs, including pseudonym key pairs, identity certificate sig_1 in revocation, and legal member certificates sig_2. To generate pseudonym key pairs, TPM picks a basename *bsn* and creates a value $d = H_{R_q}(\text{bsn})$ as well as the pseudonym private key (e_1, e'), where e_1 is a part of the TPM secret value and $e' = H_{R_3}(\text{sk}, \text{bsn})$. TPM outputs $\text{nym} = de_1 + e' \in R_q$ as pseudonym public key and creates $\text{sig}_1 = H_{R_q}(\text{nym}, \mathbf{e})$.

Using the *BlindSign* protocol in Table 3, TPM and Host jointly sign the message "certified" with TPM private key $\mathbf{e}$ and the pseudonymous private key (e_1, e') to generate a legal identity certificate sig_2. *BlindSign* is a zero-knowledge proof of VID (s, i) completed by the Host and TPM interaction. That is, to prove that the Host has (s, i) satisfying $[\mathbf{a}|\mathbf{b} + i \cdot [1|\sqrt{q}]] \cdot \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = u + \mathbf{a}_2 \cdot \mathbf{e}$. However, the verifier needs to know the value of $\mathbf{a}|\mathbf{b} + i \cdot [1|\sqrt{q}]$ in the scheme, among which $[\mathbf{a}, \mathbf{b}, [1|\sqrt{q}]]$ are all public parameters, so the identity can be easily deduced, and the user's identity will be leaked. Therefore, the zero-knowledge proof is not directly performed on i, but the commitment value about i is first generated, and the zero-knowledge proof is generated by replacing i with the commitment value. Bring the commitment value into the trapdoor function to get the following:

$$\left[\mathbf{a}^T|\mathbf{b}^T + [t_2 t_2']|\mathbf{a}_2^T\right] \begin{bmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \\ \mathbf{e} - [\mathbf{r}\,\mathbf{r}']\mathbf{s}_2 \end{bmatrix} = u, \tag{2}$$

where $\mathbf{t} = \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} = \text{Com}(i, \mathbf{r})$ and $\mathbf{t}' = \begin{bmatrix} t_{1'} \\ t_{2'} \end{bmatrix} = \text{Com}(i\delta, r')$. Suppose $\mathbf{v}^T = [\mathbf{a}^T|\mathbf{b}^T + [t_2 t_2']|\mathbf{a}_2^T]$ and $s' = \begin{bmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \\ \mathbf{e} - [\mathbf{r}\,\mathbf{r}']\mathbf{s}_2 \end{bmatrix}$, then (2) can be expressed as $\mathbf{v}^T s' = u$.

In summary, the Host needs to generate three zero-knowledge proofs in parallel, that is,

π_1': prove t, t' open to messages m, m' satisfying $m' = \delta m$

π_2': prove t opens to message m satisfying $m = \sigma_5(m)$

π_3': prove s' satisfying $\mathbf{v}^T s' = u$

Table 3: BlindSign.

TPM		Host
Public: $\mathbf{nym}, \mathbf{d}$ Private: $e', \mathbf{e}_1$		Message: μ Public: $\sigma_5, \delta, \mathbf{v}^T, \mathbf{t}, \mathbf{t}'$ Private: $\mathbf{r}, \mathbf{r}', i$
$\mathbf{y}_{e_1}, \mathbf{y}_{e'} \longleftarrow D_\xi$ $\mathbf{t} = \mathbf{d}\mathbf{y}_{e_1} + \mathbf{y}_{e'}$	$\xrightarrow{t}$	$y, y', y_5 \leftarrow D_\xi^3$ $y_{s_1} \leftarrow D_{\xi_1}^4$ $y_{s_2} \leftarrow D_{\xi_1}^2$ $y_s = (y_{s_1}, y_{s_2})$ $\pi_{1'}$: $\mathbf{W}_1 = \mathbf{a}_1^T \mathbf{y}$ $\mathbf{W}_1' = \mathbf{a}_1^T y'$ $\mathbf{W}_2 = \delta \mathbf{a}_2^T \mathbf{y} - \mathbf{a}_2^T y'$ π_2': $\mathbf{W}_{1,5} = \sigma_5^{-1}(\mathbf{a}_1^T)\mathbf{y}_5$ $\mathbf{W}_{2,5} = \mathbf{a}_2^T \mathbf{y} - \sigma_5^{-1}(\mathbf{a}_2^T)\mathbf{y}_5$ π_3': $\mathbf{W}_s = \mathbf{v}^T \mathbf{y}_s$
$\mathbf{S}_{e_1} = \mathbf{y}_{e_1} + c\mathbf{e}_1$ $\mathbf{S}_{e'} = \mathbf{y}_{e'} + ce'$ if rej $([\mathbf{S}_{e_1} \vert \mathbf{S}_{e'}],$ $[c\mathbf{e}_1, c\mathbf{e}\prime], \xi) = 1$, rebort	$\xleftarrow{c}$ $\xrightarrow{(S_{e1}, S_{e'})}$	$c = \mathbf{H}(\delta, \sigma_5, \mathbf{W}_1, \mathbf{W}_{1'}, \mathbf{W}_2, \mathbf{W}_{1,5}, \mathbf{W}_{2,5}, \mathbf{W}_s, \mu, t, \mathbf{t}, t', \mathbf{v})$ π_1': $\mathbf{z} = \mathbf{r}c + \mathbf{y}$ $z' = r'c + y'$ π_2': $\mathbf{z}_5 = \sigma_5^{-1}(\mathbf{r})c + \mathbf{y}_5$ π_3': $\mathbf{z}_s = \mathbf{s}c + \mathbf{y}_s$ if rej $([\mathbf{z} \vert \mathbf{z} \vert \mathbf{z}_5 \vert \mathbf{z}_s],$ $[\mathbf{r}c, r'c, \sigma_5^{-1}(\mathbf{r})c, \mathbf{s}c], \xi) = 1$, rebort $\xrightarrow{(z, z', z_5, c, S_{e1}, S_{e'})}$

Finally, the identity credentials PSCert = (nym‖sig$_1$ ‖sig$_2$) are generated and saved on the Host platform.

6.4. Sign/Verify. When the vehicle is moving in VANETs, the Host generates messages about the location and speed of the vehicle and transmits them to TPM. TPM signs messages using *Sign* protocol in Table 5 with pseudonym private key $(e_1, e\prime)$ and pseudonym public key nym = $de_1 + e\prime \in R_q$ and returns m_{sign} to Host. The Host creates msg = $\{m_{\text{plain}} \| m_{\text{sign}} \| \text{PSCert}\}$ and sends it to the receiver. After receiving *msg*, the receiver first calls *BlindVerify* Protocol as in Table 4 to verify sig$_2$, confirming that the message comes from a legal user. Then use pseudonym public key *nym* to verify m_{sign} as in Table 5.

6.5. Revoke. The revocation instruction msg = {revoke‖nym‖reason} generated by RA is encrypted with the RA private key sk_{ra} and broadcast in VANETs so that all legitimate users can receive it. After receiving the message, the Host passes it on to TPM. TPM uses RA public key pk_{ra} to decrypt *msg* and recognizes that the target of the instruction is itself according to *nym*. Then TPM creates $\text{sig}_1^{ra} = H_{R_q}(\text{nym}, \mathbf{e})$ and calls *BlindSign* to generate sig_2^{ra} on message "confirm," which is used to prove that TPM has received the revocation instruction and completed the self-revocation. After that, TPM deletes its own public and private key pairs and all identity certificates independently. The Host sends $\text{sig}^{rvk} = \{\text{sig}_1^{ra} \| \text{sig}_2^{ra}\}$ to RA. Since RA has knowledge of the misbehaving vehicle's *PScert*, it checks whether $\text{sig}_1 = \text{sig}_1^{ra}$ and guarantees that the target vehicle has been revoked. Then, RA calls *BlindVerify* to confirm that sig^{rvk} is indeed issued by the revoked vehicle.

It can be seen from the entire revocation process that RA can correctly revoke the target vehicle without any pseudonym resolution operations. The vehicle provides RA with proof that the identity certificate has been forcibly revoked by TPM. If the vehicle wants to communicate with the users in VANETs again, it must rerun the Join phase to generate a new identity certificate.

7. Security Analysis

The security comparison between V-LDAA, the lattice-based ring signature schemes in [7, 8, 20], and the VPKI scheme in [1] are shown in Table 6. Compared with lattice-based ring signatures in VANETs, V-LDAA has the advantage of achieving user-controlled unlinkability and unforgeability. In contrast to the existing VPKI scheme, V-LDAA achieves postquantum security and realizes the user's independent pseudonym update scheme and the distributed vehicle certificate revocation scheme.

7.1. Unforgeability. Suppose CA public parameters are set as follows: $[\mathbf{a}|\mathbf{b}], u, \mathbf{a}_2$, where $i^* \in \mathcal{S}_q$, $\mathbf{R} \in R_1^{2\times 2}$, $R' \leftarrow R^{4\times 2}$, $\mathbf{s}_u \in D_\sigma$, $\mathbf{g} = [1\sqrt{q}]$, $\mathbf{b} = \mathbf{a} \cdot \mathbf{R} - i^* \mathbf{g}$, $\mathbf{a}_2 = [\mathbf{a}|\mathbf{a}\mathbf{R}] \cdot \mathbf{R}\prime$, $u = [\mathbf{a}|\mathbf{a}\mathbf{R}] \cdot \mathbf{s}_u$.

Suppose we have a fake sampling algorithm. The adversary chooses the identity $i \in \mathcal{S}_q$ and secret value $\mathbf{e}$. When $i \neq i^*$, use the original MP − Sampler to generate $\mathbf{s}$ satisfying $[\mathbf{a}|\mathbf{a}\mathbf{R} + [i - i^*]\mathbf{g}] \cdot \mathbf{s} = u + \mathbf{a}_2 \cdot \mathbf{e}$ and output $\mathbf{s}$ to the adversary. When $i = i^*$, the gadget matrix vanishes and $[\mathbf{a}|\mathbf{a}\mathbf{R}] \cdot \mathbf{s} = u + \mathbf{a}_2 \cdot \mathbf{e}$. Therefore, compute $\mathbf{s}^* = \mathbf{s}_u + R'\mathbf{e}^*$, which is also a valid signature and output $\mathbf{s}^*$ to the adversary and the adversary verifies $[\mathbf{a}|\mathbf{a}\mathbf{R}]\mathbf{s}^* = u + \mathbf{a}_2 \cdot \mathbf{e}^*$. According to [11], based on Ring-LWE and NTRU assumptions, the adversary cannot distinguish whether it is generated by the

Table 4: BlindVerify.

Host		Verifier
	$\xrightarrow{(z, z', z_5, z_s, c, S_{e1}, S_{e'})}$	$\|(\mathbf{z}, z', \mathbf{z}_5, \mathbf{z}_s, \mathbf{S}_{e_1}, \mathbf{S}_{e'})\| \le \beta_z$, π_1': $\mathbf{W}_1' = \mathbf{a}_1^T\mathbf{z} - t_1 c$ $\mathbf{W}_1' = \mathbf{a}_1^T z' - t_{1'} c$ $\mathbf{W}_2' = \delta\mathbf{a}_2^T\mathbf{z} - \mathbf{a}_2^T z' - (\delta t_2 - t_{2'})c$ π_2': $\mathbf{W}_{1,5}{}' = \sigma_5^{-1}(\mathbf{a}_1^T)\mathbf{z}_5 - \sigma_5^{-1}(t_1)c$ $\mathbf{W}_{2,5}{}' = \mathbf{a}_2^T\mathbf{z} - \sigma_5^{-1}(\mathbf{a}_2^T)\mathbf{z}_5 - (t_2 - \sigma_5^{-1}(t_2))c$ π_3': $\mathbf{W}_s' = \mathbf{v}^T\mathbf{z}_s - uc$ $t = \mathbf{dS}_{e_1} + \mathbf{S}_{e'} - c\mathbf{nym}$ if $c = \mathbf{H}(\delta, \sigma_5, \mathbf{W}_1', \mathbf{W}_1', \mathbf{W}_2', \mathbf{W}_{1,5}{}', \mathbf{W}_{2,5}{}', \mathbf{W}_s', \mu, t, \mathbf{t}, t', \mathbf{v})$ Output 1 else Output 0

Table 5: Sign and verify.

TPM		Verifier
Public: $\mathbf{a}, \mathbf{y} = \mathbf{as} + \mathbf{e}$ Private: $\mathbf{s}, \mathbf{e}$		Public: $\mathbf{y}, \mathbf{a}, \beta_z$
$\mathbf{r}_s, \mathbf{r}_e \longleftarrow D_\xi, \mathbf{t} = \mathbf{ar}_s + \mathbf{r}_e$ $c = \mathbf{H}(\mathbf{t}, \mu)$ $\mathbf{z}_s = c\mathbf{s} + \mathbf{r}_s$ $\mathbf{z}_e = c\mathbf{e} + \mathbf{r}_e$ if rej$([\mathbf{z}_s, \mathbf{z}_e], [c\mathbf{s}, c\mathbf{e}], \xi) = 1$, abort	$\xrightarrow{(t, c, z_s, z_e)}$	$\mathbf{t} = \mathbf{az}_s + \mathbf{z}_e - cy$ if $\|\mathbf{z}_s\|, \|\mathbf{z}_e\| \le \beta_z$ and $c = \mathbf{H}(\mathbf{t}, \mu)$ Output 1 else Output 0

real public parameters and the real preimage sampling algorithm or generated by the above public parameters and the fake preimage sampling algorithm.

According to the above conclusion, we can prove the unforgeability of the V-LDAA signature.

During BlindSign, the Host needs to generate a zero-knowledge proof about $\mathbf{r}, r'$ such that

$$\begin{bmatrix} \mathbf{a}_1' \\ \mathbf{a}_2' \end{bmatrix} \cdot [\mathbf{r}\,\mathbf{r}'] + \begin{bmatrix} 0 & 0 \\ ci & ci\sqrt{q} \end{bmatrix} = c \cdot \begin{bmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{bmatrix}. \tag{3}$$

In parallel, it will also prove that

$$[\mathbf{a}|\mathbf{b} + [\,t_{21}\;\; t_{22}\,]] \cdot \begin{bmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \end{bmatrix} = cu + \mathbf{a}_2 \cdot \mathbf{e} + \mathbf{a}_2' \cdot \tilde{\mathbf{r}}. \tag{4}$$

Combine (3) and (4) to get the following:

$$c[\mathbf{a}|\mathbf{b} + i \cdot \mathbf{g}] \begin{bmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \end{bmatrix} + \mathbf{a}_2'\tilde{\mathbf{r}} = c^2 u + c\mathbf{a}_2 \cdot \mathbf{e} + c\mathbf{a}_2' \cdot [\mathbf{r}\,\mathbf{r}']\mathbf{s}_2. \tag{5}$$

The adversary randomly selects $i \in \mathcal{S}_q$, and the probability of selecting $i = i^*$ is $1/q^2$. At this time i is vanished, that is,

$$c[\mathbf{a}|\mathbf{a} \cdot \mathbf{R}] \begin{bmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \end{bmatrix} + \mathbf{a}_2'\tilde{\mathbf{r}} = c^2 u + c\mathbf{a}_2 \cdot \mathbf{e} + c\mathbf{a}_2' \cdot [\mathbf{r}\,\mathbf{r}']\mathbf{s}_2. \tag{6}$$

Sampling algorithm outputs $\mathbf{e}^*$ satisfying the following:

$$c^2[\mathbf{a}|\mathbf{b}] \begin{bmatrix} \mathbf{s}_1' \\ \mathbf{s}_2' \end{bmatrix} = c^2(u + \mathbf{a}_2 \cdot \mathbf{e}^*). \tag{7}$$

Subtract (6) and (7) to get the following:

$$\mathbf{a}\left(c\mathbf{s}_1 - c^2 s' + c\mathbf{R}\mathbf{s}_2 - c^2\mathbf{R}\mathbf{s}_2'\right) + \mathbf{a}_2\left(c^2\mathbf{e}^* - c\mathbf{e}\right) + \mathbf{a}_2'[\tilde{\mathbf{r}} - c[\mathbf{r}\,\mathbf{r}']s_2] = 0, \tag{8}$$

which can be written as follows:

$$[\mathbf{a}|\mathbf{aR}|\mathbf{a}_2|\mathbf{a}_2'] \cdot \begin{bmatrix} c\mathbf{s}_1 - c^2 s' \\ c\mathbf{s}_2 - c^2 s' \\ c^2\mathbf{e}^* - c\mathbf{e} \\ \tilde{\mathbf{r}} - [\mathbf{r}\,\mathbf{r}']c\mathbf{s}_2 \end{bmatrix} = 0. \tag{9}$$

Because $\mathbf{s}_1$, s', c, $\mathbf{e}$, $\mathbf{e}^*$, $\mathbf{s}_2$ are all polynomials with small coefficients, (9) is a nonzero Ring-SIS solution to $[\mathbf{a}|\mathbf{aR}|\mathbf{a}_2|\mathbf{a}_2']$ unless all multiplicands are 0. Therefore, if the adversary can successfully generate a zero-knowledge proof that satisfies (9), the Ring-SIS problem can be solved with a probability of $1/q^2$. To generate a zero solution, it requires $c^2\mathbf{e}^* - c\mathbf{e} = 0$. That is, $c\mathbf{e}^* = \mathbf{e}$, which means every $\mathbf{e}$ extracted from the zero-knowledge proof sig_2 in the blind signing phase must be equal to a certain $c\mathbf{e}^*$, where $\mathbf{e}^*$ is a TPM secret value of a legal certificate VID generated in the Join phase. So far, the unforgeability of the V-LDAA signature can be proved. If the adversary wants to break the unforgeability, the difficulty of using the secret value of a platform

Table 6: Security comparison.

Security requirement	ECPB in [20]	DAPRS in [7]	LRMA in [8]	Scheme in [1]	V-LDAA
Anonymity	✓	✓	✓	✓	✓
Spontaneity	✓	✓	✓	✓	✓
Unforgeability	✗	✓	✓	✓	✓
Postquantum security	✗	✓	✓	✗	✓
User-controlled unlinkability	✗	✗	✗	✗	✓
Distributed revocation mechanism	—	—	—	✗	✓
Pseudonym update spontaneity	—	—	—	✗	✓

without a legal identity certificate to generate a legal signature can be reduced to solve the Ring-SIS problem.

7.2. Anonymity. Anonymity means the adversary cannot extract the user identity value i from the signature. Suppose the adversary knows the TPM private key sk_1, sk_2 and outputs the message $\mathbf{m}^*$ to be signed and two identity values i_1, i_2 to the challenger. The challenger randomly selects an identity value i to sign and returns the signature to the adversary. After receiving the signature, the adversary guesses whether the identity value chosen by the challenger is i_1 or i_2. According to [19], the commitment scheme used in this article has hiding property based on the difficulty of M-LWE. That is, the adversary cannot distinguish the commitment value of two different messages. When signing, the challenger can replace the identity value at will to calculate the commitment value, and the generated signature is completely independent of the identity value i, so the difficulty of the adversary's guessing the id value used from the blind signature can be reduced to the M-LWE problem. In VANETs, the identity certificate generated in the Create stage only contains pseudonym information and does not contain any real identity information, and the TPM signing key cannot be associated with the vehicle user, so the adversary cannot distinguish different vehicles from the signature unless the user reveals his or her identity information.

7.3. User-Controlled Unlinkability. During Create protocol, the user can choose whether to use the same secret key sk to generate the same or different pseudonym private key so as to control whether the generated signature is linked. Once a different pseudonym is selected, the adversary cannot determine whether the two signatures are from the same user. Since sig_1 is generated by hashing the TPM private key and the pseudonym private key, the adversary cannot determine which TPM private key is used. In addition, sig_2 is a blind signature and cannot be linked.

7.4. Unforgeability of Revocation Instruction. In order to prevent the adversary from maliciously revoking the legal vehicle, it should be ensured that the revocation instruction received by TPM is from the real RA and not forged by an adversary. Adding the signature of RA to each revocation instruction can meet this requirement. TPM can confirm the authenticity of the revocation instruction by verifying the RA signature.

7.5. Unforgeability of Revocation Certificate. When RA receives the revocation certificate returned by TPM, RA must ensure that it is from the correct target vehicle and has honestly performed certificate and key destruction operations. In V-LDAA, the credibility of the revocation operation is guaranteed by the trusted hardware chip TPM. By comparing the signatures in the revocation certificate, RA can confirm that the target vehicle has indeed performed the revocation operation. No other user can forge this signature as long as the TPM key is not leaked.

7.6. Consistency of Revocation Operation. When the revocation instruction is correctly delivered to TPM, TPM will perform a series of destruction operations. However, the revocation instruction needs to be passed through the Host. If the Host is controlled by an adversary and maliciously intercepts the transmission of the revocation instruction, TPM cannot receive the correct information from RA and cannot complete the revocation operation, which is a major challenge in the distributed revocation mechanism. In V-LDAA, TPM receives information from RA at fixed time intervals which include time stamps and RA's signature. If TPM stops receiving the time stamp information, it is considered that the communication between TPM and RA interferes, and corresponding countermeasures should be taken.

8. Experimental Results and Analysis

We compare the performance of V-LDAA from two aspects: theoretical analysis and experimental simulation. Firstly, we compare V-LDAA with existing lattice-based authentication schemes in VANETs in Section 8.1 to measure the advantages of V-LDAA in the scenario of the Internet of Vehicles. Secondly, the BlindSign protocol in V-LDAA is compared with that in existing LDAA in Section 8.2 to highlight the improvement of computing efficiency after adopting the optimized signature scheme as presented in Section 4.2. This article uses Python language and SageMath9.2 library to simulate V-LDAA, LRMA in [8], DAPRS in [7], and LDAA in [11], in which the polynomial multiplication is accelerated by the NTL library. Based on the Intel(R) Core (TM) i5-7500 CPU @3.40 GHz memory 8 GB processor, we tested the execution time and signature size of each scheme.

8.1. Comparison with Existing Lattice-Based Authentication Schemes in VANETs. We compare the proposed V-LDAA scheme with existing lattice-based authentication schemes in

Table 7: Comparison of costs.

	Sign	Verify	Signature size
Scheme in [21]	$mT_{\text{samp}} + m(N+1)T_{\text{mult}}$	$M(N+2)T_{\text{mult}}$	$(N+2)m$
Scheme in [6]	$5NT_{\text{mult}}$	$T_N + 5NT_{\text{mult}}$	$2(N+1)m$
DAPRS in [7]	$2NT_{\text{mult}}$	$2NT_{\text{mult}}$	$(N+1)m$
LRMA in [8]	NT_{mult}	T_{mult}	$(N+1)m$
V-LDAA	$2T_{\text{mult}}$	$T_N + 2T_{\text{mult}}$	$3m$ + PSCert

```
Verification pass
Scheme: V-LDAA
degree= 128
q= 114356107
ParamGen Running time: 7.452999999999999 Seconds
BlindSign Running time: 5.922000000000001 Seconds
BlindVerify Running time: 0.0470000000000006 Seconds
Sign Running time: 0.03100000000000236 Seconds
Verify Running time: 0.0470000000000006 Seconds
/opt/sagemath-9.2/local/lib/python3.7/site-packages/sage/repl/ipython_kernel/__main__.py
```

Figure 3: V-LDAA protocol experimental results.

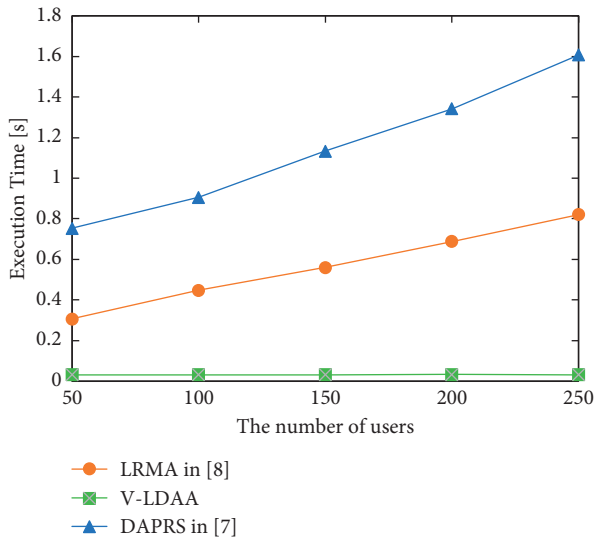

Figure 4: Signing performance for V-LDAA, DAPRS in [7], and LRMA in [8].

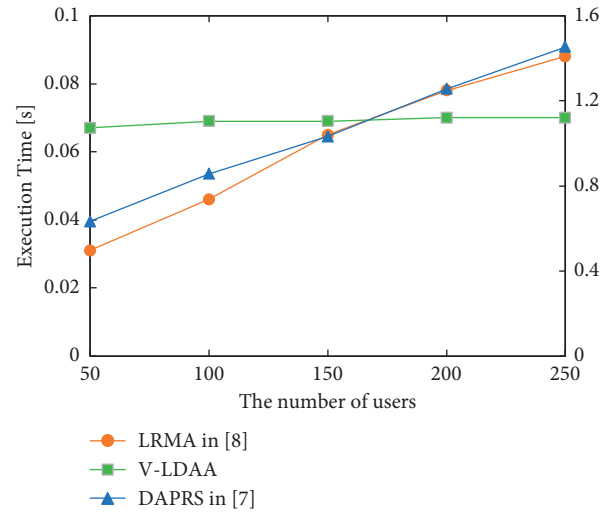

Figure 5: Verification performance for V-LDAA, DAPRS in [7], and LRMA in [8].

VANETs. Assuming that the time for a preimage sampling is T_{samp}, the time for a polynomial multiplication is T_{mult}, and the time for a zero-knowledge proof is T_N. The signing and verification calculation costs and signature length of each scheme are shown in Table 7. The studies in [6–8, 21] are all lattice-based ring signature schemes. In the ring signature scheme, users need to use their private key and all other users' public keys to sign messages. For a ring with numerous users, that is, when N is large, the computation burden is considerable. In addition, the members in a ring change as vehicles move. Thus, the member public key also needs to be updated consequently. However, in V-LDAA, users only need to sign with their pseudonym private keys each time, regardless of N.

The experimental results are shown in Figures 3–6 . We implement *Sign*, *Verify*, *BlindSign*, and *BlindVerify* protocols and measure the running time. The results are shown in Figure 3. The execution time is averaged after 10 runs of each protocol. We also compare the V-LDAA scheme with DAPRS in [7] and LRMA in [8]. A lattice-based double-authentication-preventing ring signature (DAPRS) is introduced in [7] using double-authentication-preventing signatures (DAPSs) instead of conventional signatures. A lattice-based ring signature scheme for message authentication (LRMA) is presented in [8], providing unconditional privacy to vehicles. The number of users N varies from 50 to 200. The degree of cyclotomic $d = 128$, and $q = 114356107$. Since *BlindSign* protocol is called only when users want to update their pseudonyms and recreate *PScert*, we ignore the cost of *BlindSign*. In Figure 4, the signing time required for LRMA and DAPRS increases tremendously as the number of users rises, while in V-LDAA the execution time in signing

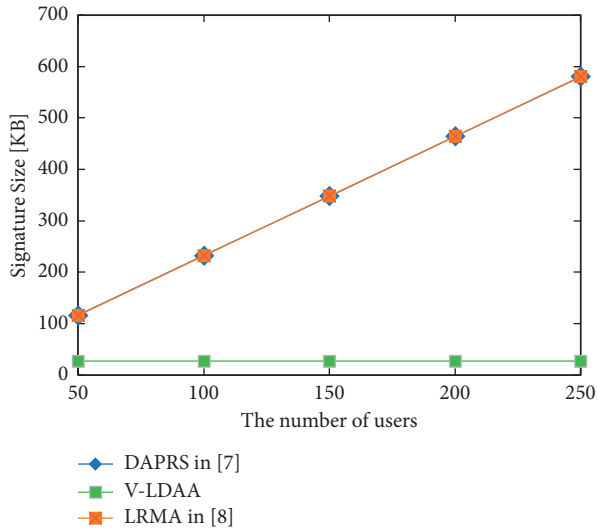

Figure 6: Signature size for V-LDAA, DAPRS in [7], and LRMA in [8].

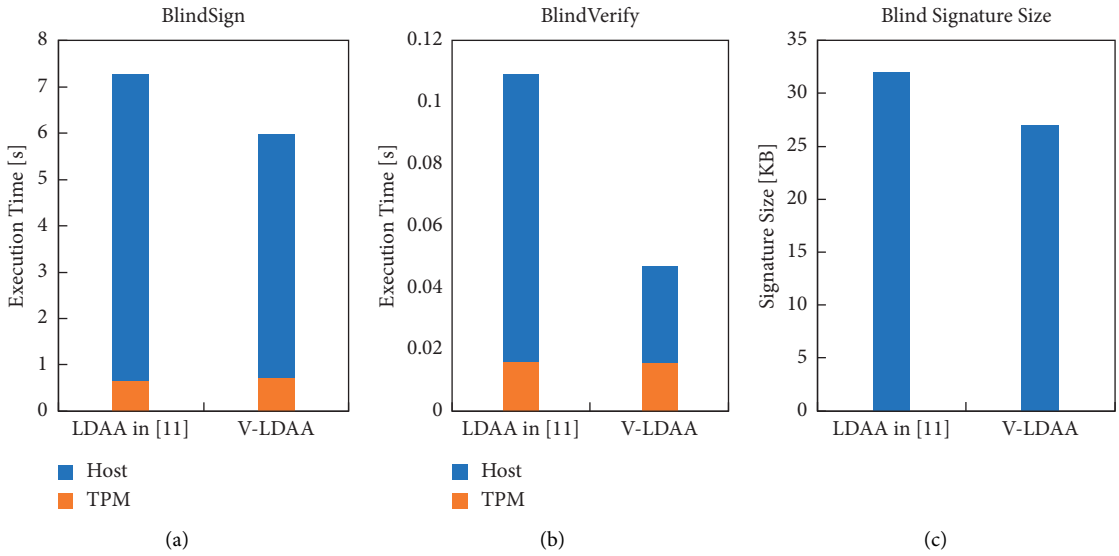

Figure 7: Comparison among V-LDAA and LDAA in [12] in terms of signing execution time (a), verification execution time (b), and signature size (c).

operations maintains at a low level with slight fluctuations. In Figure 5, additional verification of PScert is required in V-LDAA, so the verification execution time is longer than LRMA when N is small but is exceeded as N increases. The size of the certificate generated by V-LDAA is significantly smaller than that of LRMA and DAPRS, as shown in Figure 6, and it will not increase with the growth of the number of users.

8.2. Comparison with the Existing LDAA Scheme. We compare the performance of the proposed V-LDAA protocol with the existing LDAA protocol in [11] during the blind signing and blind verification on computation and storage resource consumption. In the blind signing phase, V-LDAA adopts an optimized signature scheme which removes the proof for $\sigma_5(m) = m$ and thus reduces the number of response values to the challenge, so the number of polynomials that the generated signature contains is reduced from 40 in [11] to 36.

In the Joining phase, V-LDAA adds public and secret values to the Host and enables the Host's secret value to participate in the generation of the identity certificate. This change encourages TPM and Host to interact in the Joining phase to generate a zero-knowledge proof of their respective secret values. Although the amount of calculation is increased, considering that the long-term identity certificate of each legal user only needs to be generated once, it has little effect on the overall computing efficiency. In VANETs, the participation of TPM and Host in the generation of identity

certificates can effectively resist TPM chip theft attacks and prevent TPM from being transplanted to a new vehicle platform by the adversary and signed with the replaced identity certificate. The experimental results are shown in Figure 7, where $d = 128$, $\beta = 128$, and $q = 114356107$.

As shown in Figure 7(a), the speed of the Host blind signing operation is increased by 30% by reducing the number of proofs for automorphism stability. The Host operation during blind verification is accelerated 3 times, according to Figure 7(b). Also, V-LDAA reduces the signature size by 18%, as in Figure 7(c).

9. Conclusion

To solve the security and user privacy issues in VANETs, we propose a lattice-based direct anonymous attestation scheme in VANETs that achieves postquantum security. We introduce a lattice-based long-term certificate generation mechanism, a pseudonym certificate renewal mechanism, and a distributed certificate revocation mechanism. Users can update the pseudonym certificate by themselves and control the linkability of signatures. RA does not need to perform pseudonym resolution or maintain CRLs, which overcomes the shortcomings of the traditional VPKIs. We also demonstrate that V-LDAA has significant advantages in computing efficiency and storage consumption compared with the existing lattice-based direct anonymous attestation by adopting an optimized signature scheme based on automorphism stability. Experimental results show that V-LDAA reduces the signature size by 18%. And the speed of blind signing is increased by 30% and blind verification operations are accelerated 3 times compared with the existing LDAA scheme. The main shortcoming of the proposed V-LDAA scheme is the computation and storage costs in the BlindSign protocol. In future work, we will aim to further optimize the proposed scheme to make it more suitable for resource-constrained TPM chips and vehicle platforms.

Data Availability

All of the data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This research was supported by the National Key Research and Development Program of China, Joint Research of IoT Security System and Key Technologies Based on Quantum Key (2020YFE0200600).

References

[1] M. Asghar, R. R. M. Doss, and L. Pan, "A scalable and efficient PKI based authentication protocol for VANETs," in *Proceedings of the 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–3, IEEE, Sydney, Australia, November 2018.

[2] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Computing*, vol. 20, no. 3, pp. 2439–2450, 2017.

[3] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[4] S. F. Tzeng, S. J. Horng, T. Li, X. Wang et al., "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235–3248, 2015.

[5] I. Ullah, A. Wahid, M. A. Shah et al., "VBPC: velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET," in *Proceedings of the 2017 International Conference on Communication Technologies (ComTech)*, pp. 132–137, IEEE, Rawalpindi, Pakistan, April 2017.

[6] Y. Cui, L. Cao, X. Zhang, and G. Zeng, "Ring signature based on lattice and VANET privacy preservation," *Chinese Journal of Computers*, vol. 42, no. 51, pp. 1–14, 2017.

[7] J. Liu, Y. Yu, J. Jia et al., "Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks," *Tsinghua Science and Technology*, vol. 24, no. 5, pp. 575–584, 2019.

[8] P. Mundhe, V. K. Yadav, S. Verma, and S. Venkatesan, "Efficient lattice-based ring signature for message authentication in VANETs," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5463–5474, 2020.

[9] R. E. Bansarkhani and A. E. Kaafarani, "Direct anonymous attestation from lattices," Cryptology ePrint Archive, Report 2017/1022, 2017.

[10] N. El Kassem, L. Chen, R. El Bansarkhani et al., "More efficient, provably-secure direct anonymous attestation from lattices," *Future Generation Computer Systems*, vol. 99, pp. 425–458, 2019.

[11] L. Chen, N. Kassem, A. Lehmann et al., "A framework for efficient lattice-based daa," in *Proceedings of the 1st ACM Workshop on Workshop on Cyber-Security Arms Race*, pp. 23–34, London, UK, November 2019.

[12] D. Micciancio and C. Peikert, "Trapdoors for lattices: simpler, tighter, faster, smaller," in *Advances in Cryptology—EUROCRYPT 2012*, pp. 700–718, Springer, Berlin, Germany, 2012.

[13] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, pp. 197–206, Victoria Canada, May 2008.

[14] C. Baum, I. Damgård, V. Lyubashevsky, S. Oechsner, and C. Peikert, "More efficient commitments from structured lattice assumptions," in *Lecture Notes in Computer Science*, pp. 368–385, Springer, Cham, Berlin, Germany, 2018.

[15] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 738–755, Springer, Cambridge,UK, April 2012.

[16] X. Boyen, "Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more," in *Proceedings of the International Workshop on Public Key Cryptography*, pp. 499–517, Springer, Paris, France, April 2010.

[17] S. Katsumata and S. Yamada, "Partitioning via non-linear polynomial functions: more compact IBEs from ideal lattices and bilinear maps," in *Advances in Cryptology—ASIACRYPT 2016*, pp. 682–712, Springer, Berlin, Germany, 2016.

[18] B. Libert, S. Ling, K. Nguyen, and H. Wang, "Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 1–31, Springer, Vienna, Austria, May 2016.

[19] R. Del Pino, V. Lyubashevsky, and G. Seiler, "Lattice-based group signatures and zero-knowledge proofs of automorphism stability," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 574–591, Toronto Canada, October 2018.

[20] Y. Wang, H. Zhong, Y. Xu, and J. Cui, "ECPB: efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs," *IJ Network Security*, vol. 18, no. 2, pp. 374–382, 2016.

[21] M. M. Tian, L. S. Huang, and W. Yang, "Efficient lattice-based ring signature scheme," *Chinese Journal of Computers*, vol. 35, no. 4, pp. 712–718, 2012.