IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 28, 2020, accepted November 10, 2020, date of publication November 16, 2020,
date of current version November 25, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3038042

Privacy Protection of VANET Based on Traceable Ring Signature on Ideal Lattice

LONGBO HAN, SUZHEN CAO, XIAODONG YANG, (Member, IEEE), AND ZHIQIANG ZHANG
College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China

Corresponding author: Suzhen Cao (576342353@qq.com)

This work was supported by the National Natural Science Foundation of China under Grant 61662071, Grant 61662069, and Grant 61562077.

ABSTRACT With the development of the Vehicular Ad-Hoc Network (VANET), protecting user privacy while ensuring security has become an immense challenge. A ring signature has the characteristics of no manager and unconditional anonymity, which can substantially protect user privacy. However, two problems exist in practical applications: first, unconditional anonymity cannot track the signer, which has potential security risks; and second, ordinary ring signatures cannot resist quantum attacks. In response to these problems, this paper proposes a Traceable Ring Signature (TRS) scheme on ideal lattice. In the scheme, the traceability of the ring signature is achieved by adding information to the ring signature. Selecting the algorithm on the ideal lattice to generate the master key can effectively resist quantum attacks. The scheme gives a detailed security proof and efficiency analysis. The new scheme has strong unforgeability for the difficult problem of Short Integer Solution (SIS) Question and a smaller signature size.

INDEX TERMS Ideal lattices, ring signature, traceability, small integer solution problem.

I. INTRODUCTION

Ring signature technology was proposed by Rivest *et al.* [1] in 2001. Any member of a ring can sign any message on behalf of the ring, and the verifier will know that the signature originated in this ring but will not know specific signer information. This characteristic renders the ring signature without administrators unconditionally anonymous. The ring signature scheme received extensive attention, and many scholars proposed different ring signature schemes [2]–[4], but they are based on number theory assumptions and bilinear pairings. With the practical application of quantum computers, the method proposed by Shor [5] to solve these difficult problems with quantum conditions enables these difficult problems to be solved in polynomial time. As a result, these schemes have lost their security. Thus, research on cryptosystems of quantum resistance has become an important research direction in recent years.

For these reasons, many scholars are seeking a new cryptosystem that can resist quantum attacks, which are referred to as postquantum cryptosystems. Lattice is a very important concept in number theory, and lattice-based cryptography has attracted the attention of many cryptographers because of its multifunction and potential resistance to quantum attacks. However, the signature size of a standard lattice and the calculation complexity are excessive.

To improve the efficiency of lattice-based cryptographic algorithms, cryptographers proposed the concept of ideal lattice [6]. Compared with standard lattices, ideal lattices have more algebraic structures, which can accelerate operation and reduce space storage. For example, standard lattice needs multiple lattice bases for representation, but the lattice basis of ideal lattice has a cyclic property; a principal ideal basis can represent the whole lattice. Therefore, the public key cryptosystem that is constructed by the ideal lattice based on a polynomial quotient ring has a more compact ciphertext and shorter key length [7].

Lyubashevsky and Micciancio [8] proposed a one-time signature scheme based on ideal lattices in 2008. The signature length of this scheme is short enough, and its algorithm is simple, shown to be safe and progressively effective. However, the disadvantage is that only a single message can be signed. In the same year, Gentry *et al.* [9] proposed another signature scheme on lattice by the 'Hash-and-Sign' method

The associate editor coordinating the review of this manuscript and approving it for publication was Sabu M. Thampi.

and introduced the original image sampling function. This scheme belongs to the standard lattice signature and allows arbitrary messages to be signed. However, the signature algorithm of this scheme is complex and only satisfies the security with the random prediction model, and the signature size is large. In 2009, Lyubashevsky [10] reconstructed the signature scheme on the ideal lattice. The scheme uses Fiat-Shamir's conversion technology, which is based on the difficult problem of ring-SIS to improve the one-time signature scheme. Peikert [11] published the latest achievements at the E-print in 2009 using the lattice and base expansion technology and the preimage sampling function on the Bonsai Trees model to construct a signature scheme with the standard model and a hierarchical identity encryption scheme. In 2010, Wang *et al.* [12] constructed the first identity-based ring signature scheme with Peikert's bonsai tree technology. In 2014, Ducas and Micciancio [13] constructed a digital signature scheme with a shorter public key length in the ideal lattice and proved the security of the scheme with the standard model.

The VANET is an extension of traditional mobile ad hoc networks (MANETs) and can provide services such as traffic warnings. According to the World Health Organization, the world's economic losses caused by traffic accidents are as much as $500 billion a year [14]. With an increase in the number of vehicles, urban traffic congestion is becoming increasingly serious, which causes unnecessary energy waste and environmental pollution. The VANET can ensure safe driving by improving traffic flow, which reduces traffic accidents and traffic jams. However, the VANET faces great challenges in terms of security, and any change to the real-time information of a vehicle will cause system failure, which will affect its safety. In addition, for skilled attackers, public information about a vehicle (such as beacons, speed, and steering) can be obtained by intercepting radio waves. This public information accumulated to a certain extent, and some private information of the vehicle can be easily calculated. Therefore, how to protect the privacy of users while ensuring security has become an immense challenge. Many scholars have also proposed many privacy protection schemes for the VANET [15]–[18], but these schemes have no security under quantum attacks.

In the VANET, if the ring signature technology with unconditional anonymity is employed, other vehicles only know that the information originates with a member of a ring in the VANET. However, the vehicles do not know the identity of the member; thus, the privacy of the member is protected. In a special case, such as when a signer needs to be tracked after a traffic accident, increasing the traceability is a better solution to enable the authority to track the signer. Cui *et al.* [19] also gave a solution idea in the VANET environment, but the signature length is too long, and detailed proof of strong unforgeability is lacking.

Our Contribution: In this paper, based on the ideal lattice-based signature technology of Lyubashevsky and Micciancio [20] and the trapdoor generation algorithm of Stehlé *et al.* [21], a Traceable Ring Signature (TRS) scheme on ideal lattice is proposed. The security proof is given in the standard model.

(1) Bender *et al.* [22] proposed the definition of anonymity and unforgeability with different security intensity. Based on their research, we prove that our scheme has strong unforgeability and unconditional anonymity with the standard model and is safe under the attack of selective subrings and adaptive selective messages [23].

(2) Ideal lattice has a more algebraic structure, and it can accelerate the operation speed and reduce the storage space. For example, standard lattice needs a multiple lattice basis for representation, but the lattice basis of ideal lattice has a cyclic property. A principal ideal basis can represent the whole lattice. Thus, our scheme effectively reduces the signature time and length by generating public keys and trapdoors on ideal lattice.

(3) In VANET, if public information is accumulated to a certain extent, the privacy of users can be obtained via calculation. By the unconditional anonymity of the ring signature, our scheme enables other VANET members to know that the signature originates with a legitimate user but does not know the user's specific identity, which blocks an effective way for attackers to collect members' information.

(4) According to the security requirements in the VANET [24], the practical application of the VANET must achieve traceability. We add some information to the signature and track the signer via the cooperation of nodes when necessary (such as vehicles that break the law). Therefore, our scheme achieves the balance between privacy and security and has more practical significance.

The remainder of the paper is organized as follows: The section PRELIMINARIES present a review of preliminary knowledge. The section SYSTEM FRAMEWORK AND SECURITY REQUIREMENTS introduces the system and security models of the proposed scheme. The section OUR SCHEME describes the TRS scheme, which is based on ideal lattice, and the Section SCHEME APPLICATION introduces how the TRS scheme on ideal lattice protects vehicle privacy in the VANET. The section THEORETICAL ANALYSIS presents the safety analyses. The section EFFICIENCY ANALYSIS implements the proposed scheme by numerical simulation experiments and evaluates its performance. The section CONCLUSION concludes this work.

II. PRELIMINARIES

In this section, we will introduce some notations and mathematical tools and will show the cryptographic tools on the lattice.

A. SYMBOL DESCRIPTION

In this paper, the symbolic meaning is shown in TABLE 1.

Let $\mathbb{Z}_q[x]$ and $\mathbb{R}_q[x]$ be a set of polynomials whose coefficients are integers and real numbers. For the ring R, define the ring $\mathbb{R}_q[x] = \mathbb{Z}_q[x] \big/ \langle f(x) \rangle$. $f(x)$ is a monic polynomial with integer $\mathbb{Z}_q$.

TABLE 1. Notation.

Notation	Description
□	integral number set
□	real number set
□$_q[x]$	set of polynomials with integral coefficients
□$_q[x]$	set of polynomials with real coefficients
$\hat{g}$	ring vector
Λ^*	dual lattice of lattice Λ
R	ring
$[l]$	set $(1,2\ldots,l)$
$\Lambda_q(\mathrm{A})$	q-ary lattice generated based on the row vector of matrix A
$\Lambda_q^{\perp}(\mathrm{A})$	q-ary lattice generated by the integer vector which is orthogonal to the row vector of matrix A
$\Lambda_q^{u}(\mathrm{A})$	coset of $\Lambda_q^{\perp}(\mathrm{A})$
$\rho_\sigma(x)$	Gaussian function with 0 as the center and parameter σ
$D_{\Lambda_q^{\perp},\sigma}(x)$	discrete Gaussian distribution on lattice $\Lambda_q^{\perp}$
$D_{\Lambda,s,c}$	discrete Gaussian distribution with center c and parameter s on lattice Λ
$\eta_\varepsilon(\Lambda)$	smoothing parameters of lattice Λ
$poly(n)$	polynomial function of the variable n
$\lVert\hat{g}\rVert$	2-norm of vector $\hat{g}$
$\otimes$	$\hat{g}\otimes\hat{e}=\sum_{i=1}^{m}(g_i e_i)$

Let vector $a = \left(a, a_1 g, a_2 g^2 \ldots, a_{n-1} g^{n-1}\right) \in \mathbb{Z}_q[x]/\langle f(x)\rangle$ and express it as

$$rot_{f,m}(a) = \begin{bmatrix} a \\ ag \bmod f \\ \vdots \\ ag^{m-1} \bmod f \end{bmatrix} \tag{1}$$

$$Rot_{f,m}(\hat{g}) = \begin{bmatrix} rot_{f,m}(g_1) \\ rot_{f,m}(g_2) \\ \vdots \\ rot_{f,m}(g_n) \end{bmatrix} \tag{2}$$

Generally, we do not need to explicitly point out m, so we denote it as $rot_f(a)$ and $Rot_f(\hat{g})$.

B. LATTICE DEFINITION

Definition 1: A lattice Λ is a discrete addition subgroup in n-dimensional Euclidean space $\mathbb{R}^n$, namely, m linearly independent vectors $b_1, b_2 \ldots, b_m$, where $b_i \in \mathbb{R}^n$ and $B = \{b_1, b_2 \ldots, b_m\} \in \mathbb{R}^{m\times n}$, generated Lattice $\Lambda(B) = \left\{\sum_{i=1}^{m} x_i b_i, x_i \in \mathbb{Z}\right\}$. Thus, B is referred to as the basis of Lattice $\Lambda(B)$. m and n are referred to as the rank and dimension, respectively, of lattice. If $n = m$, then lattice $\Lambda(B)$ is referred to as a full-rank lattice.

Definition 2: Ideal lattice is a lattice with a special ring structure. The ideal Γ is a Quotient Ring of ring $\mathbb{R}_q[x] = \mathbb{Z}_q[x]/\langle f(x)\rangle$. Γ-Sets of the nth order integer group $\mathbb{Z}^n$ are referred to as ideal lattices. Compared with lattice, ideal lattice can represent an n-dimensional lattice using a single lattice basis, which greatly reduces spatial complexity. Moreover, the special algebraic structure of ideal lattice can be fast computing and greatly reduces the time complexity.

Definition 3: Given the matrix $\mathrm{A} \in \mathbb{Z}_q^{n\times m}$ and the vector $x \in \mathbb{Z}_q^n$, then the n-dimensional q-ary lattice is defined as $\Lambda^{\perp}(\mathrm{A}) = \{x \in \mathbb{Z}^n | \mathrm{A}x = 0 \bmod q\}$, namely, all the vectors that are orthogonal to the row vector module q of matrix A.

C. GAUSSIAN DISTRIBUTION

Gaussian distribution on lattice is an important tool for lattice public key cipher design [25], [26]. The following definition is given:

Definition 4: The Gaussian distribution function is defined as $\rho_{c,\sigma}(x) = \exp\left(\frac{-\pi\|x-c\|^2}{2\sigma^2}\right)$, where $\sigma \in \mathbb{R}^n$ is the standard deviation and $c \in \mathbb{R}^n$ is the center. Thus, the definition of the discrete Gaussian distribution on a lattice $\Lambda_q^{\perp}$ is

$$D_{\Lambda_q^{\perp},\sigma,c}(x) = \frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}\left(\Lambda_q^{\perp}\right)} \tag{3}$$

In particular, c is often omitted in discrete Gaussian distributions, where c is 0. We can use the following Lemma to define smoothing parameters and illustrate the role of the Gaussian distribution in lattice cryptosystems:

Lemma 1 [27]: Let $\Lambda^{\perp}(\mathrm{A})$ be an n-dimensional lattice and $\varepsilon > 0$ a rational number. The smooth parameter $\eta_\varepsilon(\Lambda)$ is defined as the smallest positive integer σ, which satisfies the existence of $\rho_{1/\sigma}(\Lambda^* \backslash \{0\}) \leq \varepsilon$. Almost all $\mathrm{A} \in \mathbb{Z}_q^{n\times m}$, and ε always satisfies $\eta_\varepsilon\left(\Lambda_q^{\perp}\right) \leq \omega\left(\sqrt{\log m}\right)$ [9].

When the Gaussian parameter of the Gaussian distribution is greater than the smooth parameter, the Gaussian distribution on the lattice shows excellent cryptographic properties, namely, the basic shape of the Gaussian distribution will not change because of the transmission of the lattice. The following Lemma ensures that the length of the signature is not very large in the construction of the lattice signature:

Lemma 2 [28]: If $k > 1$, then for the Gaussian distribution, it satisfies the following properties:

$$\Pr\left\{\|\mathrm{v}\| > k\sigma\sqrt{m} : v \leftarrow D_\sigma^m\right\} < k^m e^{\frac{m}{2}(1-k^2)} \tag{4}$$

D. DIFFICULT PROBLEM ON LATTICE

Definition 5: Given the matrix $\mathrm{A} \in \mathbb{Z}_q^{n\times m}\ (m > n)$, which satisfies a uniform distribution, and the parameters n, m, q, β, the SIS problem is defined as follows: find a nonzero vector $v \in \mathbb{Z}_q^m$, satisfy $\|v\| < \beta$ and $\mathrm{A}v = 0$.

E. GAUSSIAN SAMPLING ALGORITHM

Definition 6: The Gaussian sampling algorithm can output an integer sampling algorithm based on the Gaussian distribution, which is denoted as *Sample*$\mathbb{Z}$. The algorithm *Sample*$\mathbb{Z}$ outputs the Gaussian distribution $D_{\mathbb{Z},s,c}$ with the real number c as the center. The specific process is described as follows:

Let n be the safety parameter, the parameter $t = \log n$, and s is the Gaussian parameter. The algorithm uniformly and randomly selects the integer $x \in \mathbb{Z} \cap [c - st, c + st]$ and then outputs x with probability $\rho_s(x - c) \in (0, 1]$.

Lemma 3: In 2008, the Gaussian sampling algorithm proposed by Gentry *et al.* [9] improved *Definition 5*, which will be denoted as *SampleD*. The algorithm *SampleD* inputs basis B of the arbitrary n-dimensional lattice Λ, center $c \in \mathbb{R}^n$, and the Gaussian parameter $s > 0$. *SampleD* can sample on any lattice Λ according to the Gaussian distribution $D_{\Lambda,s,c}$.

Lemma 4 [29]: For any n-dimensional lattice Λ, the center is $c \in \mathbb{R}^n$, the rational number $\varepsilon > 0$ and the Gaussian parameter $s > 2\eta_\varepsilon(\Lambda)$ satisfies $D_{\Lambda,s,c} \leq \frac{1+\varepsilon}{1-\varepsilon}2^{-n}$. If $\varepsilon < \frac{1}{3}$, then the minimum entropy of the discrete distribution $D_{\Lambda,s,c}$ on the lattice is at least $n - 1$.

F. TRAPDOOR GENERATION ALGORITHM AND PRE-IMAGE SAMPLING FUNCTION

Ajtai [30] investigated a probabilistic polynomial time (PPT) algorithm, which can generate lattice $\Lambda^{\perp}(\mathrm{A})$ and its trapdoor base. The algorithm later became a basic tool of the lattice cryptosystem. Alwen and Peikert [31] proposed a more efficient algorithm. We refer to the algorithm of Ajtai and Alwen as the trapdoor sampling algorithm. The description of the algorithm is presented as follows:

Lemma 5: Given the parameters $q = poly\,(n)$ and $m > 5n \log q$, the PPT algorithm input 1^n, output matrix $\mathrm{A} \in \mathbb{Z}_q^{n\times m}$ and a full rank set $S \in \Lambda^{\perp}\,(\mathrm{A})$ exist, where the matrix A is nearly uniformly distributed and satisfies $\|S\| \leq O\,(n \log q)$. Afterward, the set S can be effectively transformed into the trapdoor T of lattice $\Lambda^{\perp}\,(\mathrm{A})$.

Stehlé *et al.* [21] extend *Lemma 5* to the ideal lattice.

Lemma 6: An ideal lattice trapdoor generation algorithm *Ideal − TrapGen* exists. Let n be the security parameter, $m > 5n \log q, q = poly\,(n)$. The algorithm *Ideal − TrapGen* can simultaneously obtain the polynomial vector $\hat{g} = (g_1, g_2 \ldots, g_m) \in \mathbb{Z}_q^m$ and trapdoor $\mathrm{T}_{\hat{g}} \in \mathbb{Z}_q^{mn\times mn}$ that are statistically close to a uniform distribution in polynomial time, which satisfies $\left\|\mathrm{T}_{\hat{g}}\right\| \leq \tilde{\mathrm{O}}\left(\sqrt{n}\right)$ and $Rot_f\,\left(\hat{g}\right)^{\mathrm{T}} \cdot \mathrm{T}_{\hat{g}} = 0$.

Definition 7: The preimage sampling function *SamplePre* (A, T_A, u, s) exists on the standard lattice: Let n be the security parameter, $m > 5n \log q$, $q = poly(n)$, and $s \geq \left\|\tilde{T}_A\right\| \omega\left(\sqrt{\log m}\right)$. First, the trapdoor sampling algorithm of *Lemma 5* is used to generate matrix $\mathrm{A} \in \mathbb{Z}_q^{n\times m}$ and trapdoor $\mathrm{T_A}$. Second, for any vector $u \in \mathbb{Z}_q^{\mathrm{n}}$, *Lemma 3* is utilized to return the random nonzero vector $e \in \Lambda_q^u(A)$, whose distribution is similar to $D_{\Lambda_q^u(A),s}$, which satisfies $\mathrm{A}e = u(\mathrm{mod}\ q)$. Last, from *Lemma 4,* the minimum entropy of vector u is $n - 1$.

Liqiang *et al.* [32] extended *Lemma 6* to the ideal lattice:

Lemma 7: Ideal − SamplePre (A, T_A, u, s)A preimage sampling function exists on the ideal lattice: it inputs the loop polynomial vector $\hat{g} \in \mathbb{Z}_q^m$ that corresponds to the trapdoor $\mathrm{T}_{\hat{g}}$, Gaussian parameter s and vector $v \in \mathbb{Z}_q^m$; enables the algorithm to generate the random sample $\hat{e} \in \mathbb{Z}_q^m$ with a distribution similar to $D_{\mathbb{Z}^{m\times n},s}$, and satisfies $\hat{g} \otimes \hat{e} = v$.

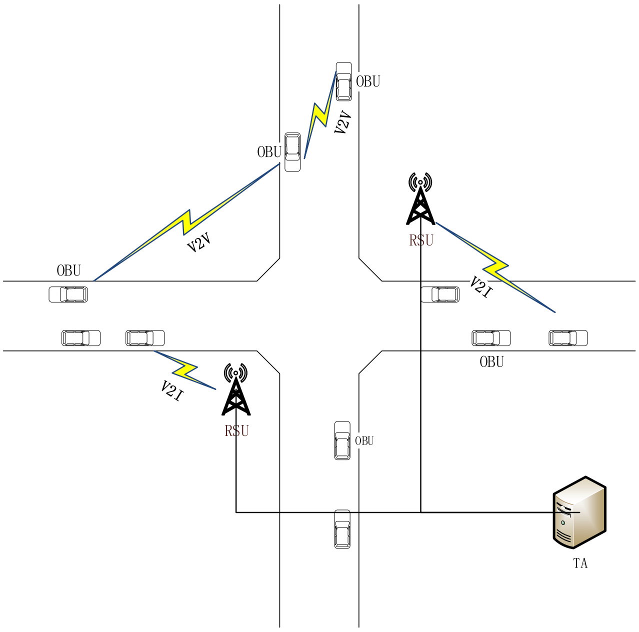


FIGURE 1. VANET model.

III. SYSTEM FRAMEWORK AND SECURITY REQUIREMENTS

In this part, first, we introduce our car networking model. Second, we introduce the syntax of the TRS scheme. Last, we introduce the security requirements of the scheme.

A. VANET MODEL

As shown in FIG. 1. The VANET model is composed of three parts: A Trust Authority (TA), a vehicle equipped with an On-Board Unit (OBU), and a Road Side Unit (RSU). Communications in VANETs can be divided into two types: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) communication. Both types of communication are carried out using the Dedicated Short Range Communications (DSRC) protocol [16].

TA: The TA has powerful computing power and is responsible for generating master keys and system parameters. The TA is also responsible for registering the OBU and RSU and initializing them with public system information or private keys.

RSU: The RSU is a fixed infrastructure that is connected to the TA with wired links; it has a higher computation capability than the OBU. Within its coverage, the RSU uses the DSRC protocol to transmit and receive secure messages with a vehicle's OBU. The main function of the RSU is to store and forward information.

OBU: The OBU is a wireless communication device that is equipped on a vehicle. It is a tamper-proof device (TPD) that can communicate with other vehicles or the RSU via the DSRC protocol. According to the specification of the DSRC protocol, each vehicle periodically broadcasts messages about road traffic and vehicles' conditions every 100–300 ms.

In our network model, the infrastructure RSU is managed by the transportation department via trusted authorization, and the RSU enters the VANET by wired connection. The information that is periodically broadcast by vehicles (such as beacon messages, including location, speed, timestamp, etc.) and the public information that is broadcast by the RSU does not need to be kept secret. However, because these messages are also public to the surrounding vehicles, an attacker can easily intercept this information via some devices and obtain private information, such as vehicle owner information, driving route information, frequent stay location information, etc. Therefore, our main purpose is to solve the problem of privacy protection of user identity in the VANET.

We employ a ring signature to propose a new privacy protection scheme for the VANET. Because the periodic broadcast information of vehicles and the RSU does not need to be kept secret, the sender must be responsible for the signed message. Signature technology can verify whether the message is true and complete, so we use signature technology to ensure that the message originates with legitimate network members, is complete and has not been subject to tampering. The ring signature technology can hide the real identity of the signer while ensuring the reliability of the message. Vehicles quickly form a ring with surrounding vehicles via the RSU and sign information via ring signature technology, which can effectively achieve anonymous communication in the vehicle network. To ensure the practical security of car networking, we have also increased the traceability. This feature can be hosted by the TA when needed (such as illegal driving, sending false messages for eliminating road congestion, etc.) and can be traced to the signer according to the signed message, which ensures traffic safety and completes the unconditional anonymous private communication in the vehicle network.

B. SYNTAX OF TRS

A TRS scheme includes the following five polynomial time algorithms:

(1) **Setup**: On inputting the security parameter n, the algorithm outputs master key MSK and public parameter PP.

(2) **Key Extraction**: On inputting master key MSK, public parameters PP, and user identity ID_i, the algorithm outputs a user's public key PK_i, private key SK_i, and tracking key TK_i.

(3) **Signature**: On inputting ring R_1, message M, and public parameter PP, the algorithm outputs signature μ for message M.

(4) **Verification**: On inputting public parameter PP, ring R_1, and message-signature pair (μ, M), the algorithm returns accept or reject. If the message-signature pair is valid, the algorithm returns accept; otherwise, the signature is rejected.

(5) **Signature Track**: On inputting the message-signature pair (μ, M), the algorithm outputs the signer s.

C. SECURITY REQUIREMENTS

A secure and effective ring signature scheme needs to satisfy both anonymity and unforgeability. Bender *et al.* [22] gave the security definition of anonymity and unforgeability of signature schemes for different security strengths. Moreover, in some special cases (such as illegal driving, sending false messages for eliminating road congestion, etc.), the ring signature scheme, which satisfies traceability, is more secure, and the tracking of the TA is more authoritative. We comprehensively consider the strongest definition of ring signature security given by Bender *et al.* [22], combine it with more secure traceability, and propose a TRS scheme on the ideal lattice. The scheme needs to meet the following security requirements:

ANONYMITY: After the vehicle has registered with the TA to become a legitimate user, each vehicle's real identity is hidden from other entities in the network.

STRONG UNFORGEABILITY: Strong unforgeability is based on the underlying hard problem assumption, which can be proved by the ring signature scheme.

TRACEABILITY: The TA has the capacity to obtain the real identity of any malicious vehicle (such as illegal driving, sending false messages for eliminating road congestion, etc.).

IV. OUR SCHEME

In this section, we will introduce our proposed scheme. We choose to use the key generation center (KGC) to generate a secret key via a user's ID, which is consistent with reality.

A. SETUP

Select n as the security parameter, and set $q = poly(n)$ and $s \geq m^2\omega\left(\sqrt{\log m}\right)$. Define the quotient ring: $\mathbb{R}_q = \mathbb{Z}_q[x]\big/x^n + 1$. Select the hash function: $H = \{0,1\}^* \rightarrow \mathbb{Z}_q^{n\times m}$. The purpose of the hash function is to complete the mapping of the bit string on the ring and verify the integrity of the message. KGC performs the algorithm *Ideal−TrapGen* of *Lemma 6* to generate the polynomial vector $\hat{\mathrm{g}} \in \mathbb{Z}_{\mathrm{q}}^{m}$ and the master key $MSK = \mathrm{T}_{\hat{\mathrm{g}}} \in \mathbb{Z}_q^{mn\times mn}$.

(2) Output the public parameters $PP = \left\{H, \hat{g}\right\}$ and master key MSK.

B. KEY EXTRACTION

On inputting the master key MSK, public parameters PP, user identity ID_i. For a user with ID_i, KGC performs the following operations:

(1) KGC encodes the ID_i as a ring polynomial $H(ID_i) = r(ID_i) \in \mathbb{R}_q$ and randomly selects the vector $\hat{a}, \hat{b}, \hat{v}_0 \in \mathbb{R}_q^m$ with a uniform distribution of the coefficient polynomials. Calculate the vector $\hat{v}_i = \hat{a} + r\left(ID_i\right)\hat{b}$. KGC performs the algorithm *Ideal − SamplePre* $\left(\hat{g}, MSK, s\ , \hat{v}_0 - \hat{v}_i\right)$ of *Lemma 7* to calculate $\hat{g} \otimes \hat{e}_i = \hat{v}_0 - \hat{v}_i$.

(2) Output user tracking key $TK_i = \left(\hat{e}_i, 1\right) \in \mathbb{R}^{m+1}$ and public-private key pair (SK_i, PK_i).

C. SIGNATURE

On inputting the ring $R_1 = \{PK_1, PK_2, \ldots, PK_l\}$, message M, and public parameter PP. The signature process of U_s is described as follows:

(1) Simulate other members' signatures. By *definition 5*, U_s sample l polynomial vectors $\hat{k}_i \in \mathbb{R}_q\,(i \subset [l])$, which satisfies D_σ^{m+1}. Simulate other members' signatures $\sigma_i = \hat{k}_i\,(i \subset [l] \setminus s)$.

(2) U_s completes its signature. Calculate $\hat{u} = H\,(R_1|M) \in \mathbb{R}_q$. Let $\hat{z} = \hat{u} - PK_i \otimes \hat{k}_i$. By *definition 5*, sampling polynomial vector $\hat{x} \in \mathbb{R}_q$ satisfies $\hat{v}_0 \cdot \hat{x} = \hat{z}$. Generate signature $\sigma_s = \left(\hat{x} \otimes \hat{e}_s, \hat{x}\right) + \hat{k}_s$. Combine with Step (1) to generate the ring signature $\sigma_i = \{\sigma_1, \ldots, \sigma_l\}$.

(3) Generate a tracking signature. Randomly select a group of random numbers $t_i = t_1, \ldots, t_{max}$. Calculate $T = (t_i \otimes \hat{v}_0) \cdot PK_s$ and $TP_i = t_i PK_i\,(i = 1, \ldots, max)$. Combine to generate the tracking signature $\tau = \{T, TP_1, \ldots, TP_{max}\}$. In this way, generating T is pseudorandom, which is the security guarantee of the tracking signature.

(4) Combine with Step (2) and Step (3). Output the traceable ring signature $\mu = \{\sigma_i, \tau, M, R_1\}$.

D. VERIFICATION

On inputting public parameter PP and signature $\mu = \{\sigma_i, \tau, M, R_1\}$. First, verify the validity of the ring, and directly reject the message if the public key fails. Second, if it does not exist, calculate $h(R|M)$ and encode it as the ring polynomial $\hat{u} \in \mathbb{R}_q^m$. Last, calculate whether $PK_i \otimes \sigma_i = \hat{u}$ and $\|\sigma_i\| < 2\sigma\sqrt{n(m+1)}$. If both conditions hold, output accept; otherwise, output reject.

E. SIGNATURE TRACK

On inputting signature $\mu = \{\sigma_i, \tau, M, R_1\}$, KGC performs the following steps:

(1) Perform the Step (*VERIFICATION*) to verify whether the signature is valid or invalid. If the signature is invalid, reject the message. If the signature is valid, KGC sends TP_i to all members of ring R_1 and asks that signature γ_i of the TP_i is returned.

(2) Verify that the returned γ_i is a valid signature. If the signature is valid, $PK_i \otimes \gamma_i = TP_i$ and $\|\gamma_i\| < 2\sigma\sqrt{l(m+1)}$ according to Step (*VERIFICATION*). Verify that $T_i \cdot PK_i = TP_i \cdot \hat{v}_0$. When both conditions are true, the return value is proven to be valid.

When both conditions are met, the return value is proven to be valid.

(3) Calculate $T' = \left(\sum_{i=1}^{\max} T_i\right) \cdot PK_i$; when $i = s$, $T' = T$ holds. Output the signer s.

V. SCHEME APPLICATION

In this section, we will introduce how the TRS scheme on the ideal lattice protects vehicle privacy in the VANET. In our VANET model, the TA is responsible for the functions of KGC. Each vehicle needs to register with the TA, and the TA generates the public key and private key of the vehicle using the identity information of the vehicle. When a vehicle moves into the region of an RSU, the vehicle makes a ring request to the RSU, and the RSU stores its public key in the ring set R. When a vehicle wants to send a message, it randomly selects n valid public keys to form the subring R_1 and then carries on the ring signature. For the verifier, if the signature is a valid signature, by the unconditional anonymity of the ring, the verifier only knows that the signature originates with the ring but does not know the identity of the vehicle, so the privacy of the vehicle is protected. The details provided as follows:

(1) First, the TA performs **Setup** to generate master key MSK and public parameters PP. Second, when a vehicle with the identity ID_i submits a registration request, the TA performs **Key Extraction** to generate the public-private key pair (SK_i, PK_i) and tracking key $TK_i = (\hat{e}_i, 1) \in \mathbb{R}^{m+1}$ of the vehicle via MSK. Last, the TA records the vehicle information and sends (SK_i, PK_i) and TK_i to the vehicle. The vehicle retains (SK_i, PK_i) for signature, and TK_i can be employed for collaborative tracking.

(2) When the vehicle enters the coverage area of the RSU, the vehicle makes a ring request to the RSU. The RSU detects the received request information, verifies the validity and timeliness to the TA, and then stores the user's public key in the ring set.

When the number of vehicles reaches a custom maximum number, RSU generates the ring $R = \{PK_1, PK_2, \ldots, PK_{\max}\} \in \mathbb{R}_q$, which corresponds to the vehicle identity $ID_1, ID_2, \cdots, ID_{\max}$, and broadcasts the ring information. Members of the ring can sign messages with their private key SK_i.

(3) When a vehicle with the identity ID_i broadcasts the message to other vehicles, message $M \in (0, 1)^*$, which contains a timestamp, is generated, and the subring $R_1 = \{PK_1, PK_2, \cdots, PK_s, \cdots, PK_l\} \in R$ is randomly selected. The vehicle performs Signature to output $\mu = \{\sigma_i, \tau, M, R_1\}$ and broadcasts μ for other vehicles.

When other vehicles receive a message from a neighboring vehicle, a vehicle performs **Verification**. Receive the message if it is valid; otherwise, reject it.

(4) When necessary (such as traffic accident handling), the TA performs **Signature Track** to track specific signers to ensure traffic safety.

VI. THEORETICAL ANALYSIS

According to the security requirement given in Section III of this paper, we give the proof of the correctness, anonymity, strong unforgeability and traceability of our scheme.

A. CORRECTNESS

Theorem 1: If $\|\sigma_i\| < 2\sigma\sqrt{n(m+1)}$ and $PK_i \otimes \sigma_i = \hat{u}\,(\text{mod}\ q)$ of OUR SCHEME hold, then this signature is true and valid.

Proof: To verify that $PK_i \otimes \sigma_i = \hat{u}$ is true, we assume that the formula is true. $\hat{u}$ satisfies $\hat{z} = \hat{u} - PK_i \otimes \hat{k}_i$ during the signing process, namely, $\hat{v}_0 \cdot \hat{x} = PK_i \otimes \sigma_i - PK_i \otimes \hat{k}_i$ holds. The derivation is expressed as follows:

$$\begin{aligned} \hat{v}_0 \cdot \hat{x} &= PK_i \otimes \sigma_i - PK_i \otimes \hat{k}_i \\ &= PK_i \otimes \sigma_i - PK_i \otimes \hat{k}_i \end{aligned}$$

$$
\begin{aligned}
&= PK_s \cdot \sigma_s - PK_s \cdot \hat{k}_s \\
&= PK_s(\sigma_s - \hat{k}_s) \\
&= PK_s(\hat{x} \otimes \hat{e}_s, \hat{x}) \\
&= (\hat{g}, \hat{v}_0 - \hat{g} \otimes \hat{e}_s)(\hat{x} \otimes \hat{e}_s, \hat{x}) \\
&= \hat{v}_0 \cdot \hat{x} \qquad (5)
\end{aligned}
$$

Because the equation holds, the hypothesis holds. $\|\sigma_i\| < 2\sigma\sqrt{l(m+1)}$ holds because the signature σ_i satisfies the distributed D_σ^{m+1}. According to *Lemma 2*, a high probability exists that $\|\sigma_i\| < 2\sigma\sqrt{l(m+1)}$ holds. Therefore, we can state that signature μ is true and valid.

B. ANONYMITY

Theorem 2: Our proposed scheme satisfies unconditional anonymity.

Proof: If opponent A that can win the following game with a significant margin exists, then there must be a Challenger C that can identify the signer of this scheme by some nonnegligible advantages.

(1) Challenger C selects the security parameter λ and runs the algorithm Setup to generate the master key MSK and public parameter PP. C generates the maximum user set $R = \{U_1, U_2, \ldots, U_{\max}\}$ and runs the algorithm Key Extraction to obtain the public key-private key pair $[PK_i, SK_i]_1^{\max}$ of all users and sends $[PK_i]_1^{\max}$, user set R and public parameters PP to adversary A.

(2) Adversary A submits message $M' \in (0, 1)^*$ and subring $R_1 = \{U_1, U_2, \cdots, U_l\} \subseteq R$ to Challenger C. Challenger C uses the private key SK_i to execute the algorithm Signature and returns the result μ to A.

(3) Adversary A adaptively asks user $U_i \in R$ the corresponding private key, and Challenger C returns SK_i.

(4) Challenge: Adversary A submits message $M' \in (0, 1)^*$ and two users $U_0, U_1 \in R_1'$. Challenger C randomly selects $a \in \{0, 1\}$, executes the algorithm Signature to output sign μ via U_a's private key SK_a, and returns the result to A.

(5) Adversary A outputs a' as a guess about the signer's identity.

Assume that the arbitrary polynomial time opponent A has a wins games advantage of $Adv_{RS,A}^{anon} = Succ_{RS,A}^{anon} - 1/2 = \varepsilon$. To prove that the advantage of adversary A is negligible, only prove that the signature of an arbitrary signer in the ring is indistinguishable. Since all legitimate signatures are random vectors of specific sets, we only need to consider their distribution. As shown by the SIGNATURE in section IV, for any ring R_1' and message M, the verification formula of any legal signature σ_i and σ_i' is $PK_i \otimes \sigma_i = PK_i \otimes \sigma_i' = \hat{u}$. According to reference [29], signatures σ_i and σ_i' are indistinguishable, namely, for any adversary A, the win game advantage ε is negligible.

C. STRONG UNFORGEABILITY

Theorem 3: If opponent A can forge a signature with a significant margin, then Challenger C must exist. In time $t' \leq t + Q \cdot \left[(l+1)T_{sp} + 2T_{mul}\right]$, an example of the SIS problem with parameter $2\sigma\sqrt{l(m+1)}$ is solved with a significant margin. The symbolic definition of the comparison is shown in TABLE 6.

Proof: Assuming that adversary A can forge the signature of message (R_1', M') with probability ε, which cannot be disregarded within time t, the process for Challenger C to crack an SIS instance in polynomial time via A is detailed as follows:

Assume that adversary A forges signature $\mu' = \left\{\sigma_i', \tau' , M', R_1\right\}$ after Q times signature inquiries. We can forge the tracking key τ' if we can forge σ_i', so we only need to prove the strong unforgeability of σ_i'. When Challenger C obtains μ', calculate $H\left(R'|M_1'\right) = \hat{u}' \in \mathbb{R}_q^m$. If $\hat{u}' = 0(\bmod p)$, C fails; otherwise, two possible situations exist:

(1) Signature (R_1', M') has not been questioned. Set the verification matrix

$$
\begin{aligned}
PK_i \otimes \sigma_i' &= (PK_1, PK_2, \cdots, PK_s, \cdots, PK_l) \\
&\quad \times (\sigma_1', \sigma_2', \cdots, \sigma_s', \cdots, \sigma_l')^{\mathrm{T}} \\
&= \hat{u}' \\
&= \hat{v}_0 \cdot r(\bmod q) \qquad (6)
\end{aligned}
$$

An extended nonzero vector $r' = (r^{\mathrm{T}}, 0)^{\mathrm{T}} \in \mathbb{Z}_q^{m+1}$ can be obtained by adding 0 to vector $r \in \mathbb{Z}_q^m$; it satisfies $PK_i \otimes \sigma_i' = PK_i \otimes r'(\bmod p)$.

Let $x = (x_1, x_2, \cdots, x_s, \cdots, x_l) = \sigma_i' - r'$. From reference [29], for any matrix $A \in \mathbb{Z}_q^{n\times m}$, if $Ax' = Ax\ (\bmod p)$, then $prob(x' = x) \leq 2^{-\omega(\log n)}$. The probability of $x = 0$ is negligible. Thus, Challenger C obtains the nonzero vector x to satisfy $\sum_{i=1}^{l} PK_i x_i = 0(\bmod q)$. Let $u' = (x_1, x_2, \cdots, x_l)$, if any $x_i (i \in [l])$ is nonzero, then $\hat{u}' \neq 0$. Otherwise, according to *Lemma 26* of reference [30], we know $prob(\hat{u}' \neq 0) \geq 2/3$. Furthermore, the extended nonzero vector $u \in \mathbb{Z}_q^{l(m+1)}$ can be obtained by filling 0 in the appropriate position of u', which satisfies $PK_i \otimes u = 0(\bmod q)$ and makes $\|u\| < 2\sigma\sqrt{l(m+1)}$.

Therefore, in the case of no trapdoor, Challenger C obtains a nonzero solution of this SIS instance with a significant margin.

(2) Signature (R_1', M') has been questioned. According to $PK_i \otimes \sigma_i' = u' = PK_i \otimes c(\bmod p)$ the definition of strongly unforgeable, $\sigma_i' \neq c$; so C obtains the nonzero vector $e' = (e_1', e_2', \cdots, e_s', \cdots, e_l') = \sigma_i' - c$, which satisfies $PK_i \otimes e' = 0(\bmod q)$. Similar to Step 1, Challenger C obtains the nonzero vector e' with high probability. After filling 0 in the appropriate position, C obtains a nonzero vector $e \in \mathbb{Z}_q^{l(m+1)}$, which satisfies $PK_i \otimes e = 0(\bmod q)$ and $\|e\| < 2\sigma\sqrt{l(m+1)}$.

Based on this analysis, we can make the parameters $\beta = 2\sigma\sqrt{l(m+1)}$ of the SIS instance. The time cost of Challenger C to successfully crack the SIS problem includes the time of Q times signature inquiries and the time t of forging signatures. Thus, $t' \leq t + Q \cdot [(l+1)T_{sp} + 2T_{mul})]$. Therefore, if an adversary A who can forge a signature of this scheme with a nonnegligible advantage ε within time t exists, then

TABLE 2. Hardware configuration description.

Equipment	Version
Operating system	Ubuntu
CPU	Intel Core i7-7700HQ
Memory	16 G
Word Size	64 bits
CPU Clock Speed	2.8 GHz

algorithm C that can successfully solve an SIS instance on a lattice with a nonnegligible probability in time t' exists.

This finding contradicts the SIS hypothesis, so the ring signature scheme in this paper is secure.

D. TRACEABILITY

Theorem 4: If all members cooperate, the signer can be traced. The scheme in this paper is traceable.

Proof: The tracking key of all users is $TK_i = (\hat{e}_i, 1) \in \mathbb{R}^{m+1}$, and the tracking target signature is $\mu = \{\sigma_1, \ldots, \sigma_l, T, TP_1, \ldots, TP_{\max}\}$. $TP_i = t_i PK_i$, and $T = (t_i \otimes \hat{v}_0) \cdot PK_s$. The tracking steps are detailed as follows:

(1) KGC checks the validity of the signature. If the signature is legal and valid, KGC sends TP_i to all ring members and asks them to return the signature σ_i' for TP_i.

(2) Verifying the validity of σ_i' satisfies $T_i = PK_i \otimes \mu_i$ and $\left\| \sigma_i' \right\| < 2\sigma\sqrt{n(m+1)}$.

(3) Verify the validity of T_i:

$$\begin{aligned} T_i &= TK_i \otimes TP_i \\ &= (\hat{e}_i, 1) \otimes t_i PK_i \\ &= t_i \otimes (\hat{e}_i, 1) \otimes (\hat{g}, \hat{v}_0 - \hat{g} \otimes \hat{e}_i) \\ &= t_i \otimes \hat{v}_0 \end{aligned} \tag{7}$$

Therefore, if $T_i \cdot PK_i = TP_i \cdot \hat{v}_0$ holds, T_i is valid. Calculate $T' = \left(\sum_{i=1}^{\max} T_i \right) \cdot PK_i = \left(t_i \otimes \hat{v}_0 \right) \cdot PK_i$. When $i = s$ holds, $T' = T$ holds. The signer can be traced to s.

VII. EFFICIENCY ANALYSIS

To evaluate the performance of our proposed scheme, our scheme is simulated in the Network Simulator NS-2.45. We are mainly concerned with the vehicle-intensive areas of the city, where the privacy of vehicles is more vulnerable to threats. The hardware environment is shown in TABLE 2.

Using the Fast Library for Number Theory (FLINT), we change the value of the security parameter n when we fix the number of members to 5. The time cost of the signature and verification is shown in TABLE 3.

We change the value of the security parameter n when we fix the number of members to 10. The time cost of the signature and verification is shown in Table 4.

TABLE 3. Experimental data sheet.

n	Signature time	Verification time
128	0.05572	0.01538
256	0.08197	0.03056
384	0.13947	0.03987
416	0.15118	0.04306
440	0.17519	0.04960
464	0.18062	0.05328

TABLE 4. Experimental data sheet.

n	Signature time	verification time
128	0.05460	0.02180
256	0.13650	0.03926
384	0.16605	0.04570
416	0.19920	0.04824
440	0.20911	0.05230
464	0.22190	0.05827

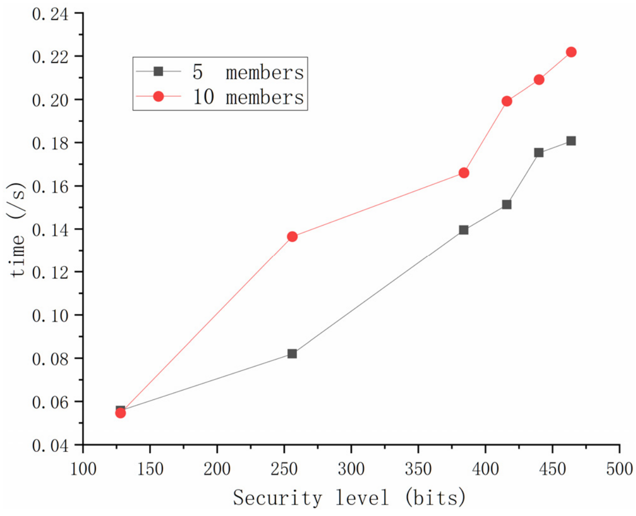


FIGURE 2. Time cost of signature.

We display the experimental data in FIG. 2 and FIG. 3. The signature time and verification time increase with an increase in security parameters, but the impact of the increase in the number of vehicles on the cost is not obvious. Therefore, without considering other network environments, our scheme can be applied to the VANET when the security parameters are 128 bits and 256 bits.

According to these experiments, we choose the security parameter as 128 bits for simulation. We simulate an intersection with a length of 500 m, and the simulation time is 200 s. In the VANET, vehicles move randomly with an average speed of 10 km/h within a domain. The VANET parameters are shown in TABLE 5.

The number of vehicles ranges from 20-60 and randomly appear from four ports. The RSU is located in the middle of the intersection, and the messaging range is 250 m. The result is shown in FIG. 4 and FIG. 5. The delay is the average delay of each mobile node in the experiment, and the data throughput is the total throughput in the environment per unit time.

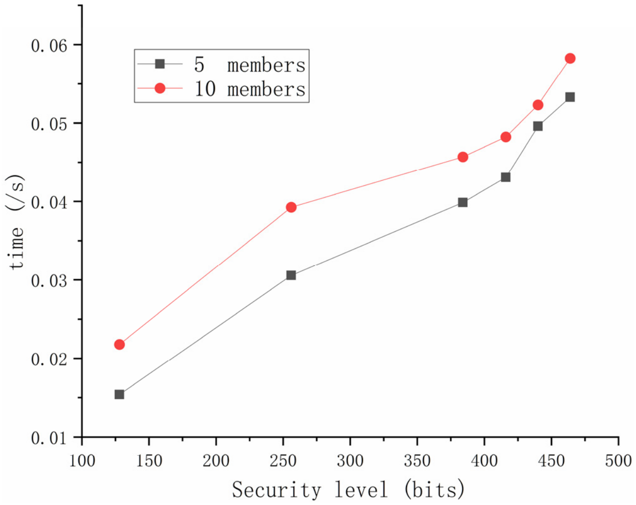


FIGURE 3. Time cost of verification.

TABLE 5. VANET parameters and values.

Parameters	Values
Vehicle speed (kilometer/hour)	10
Inter vehicle distance (meter)	30
Usable bandwidth (Mbps)	6
Number of lanes	6
Messaging range (meter)	250

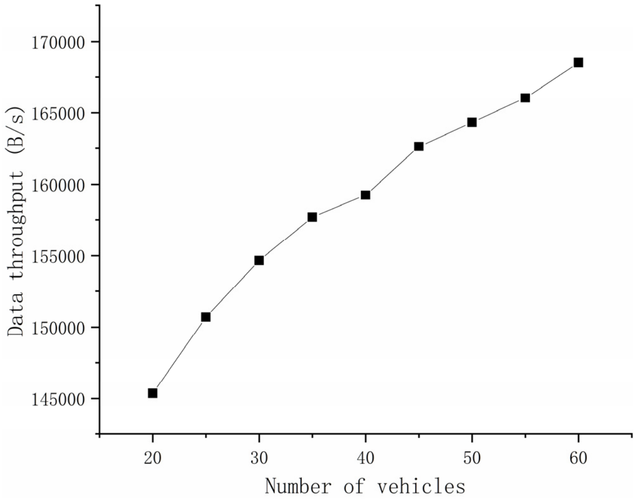


FIGURE 4. Vehicle density and data throughput.

As shown in FIG. 4, the throughput increases linearly with vehicle density, but it is approximately 160 Kb/s, which is less than the 6 Mbps with the minimum bandwidth of VANET. However, the delay is similar to the maximum delay of 300 ms allowed by the VANET, because the lattice-based cryptosystem is still in the theoretical stage and is still not ready for practical application.

We compare the efficiency of our scheme with that of other methods for privacy protection of VANET schemes. Table 6 shows a comparison with existing schemes considering the security requirements.

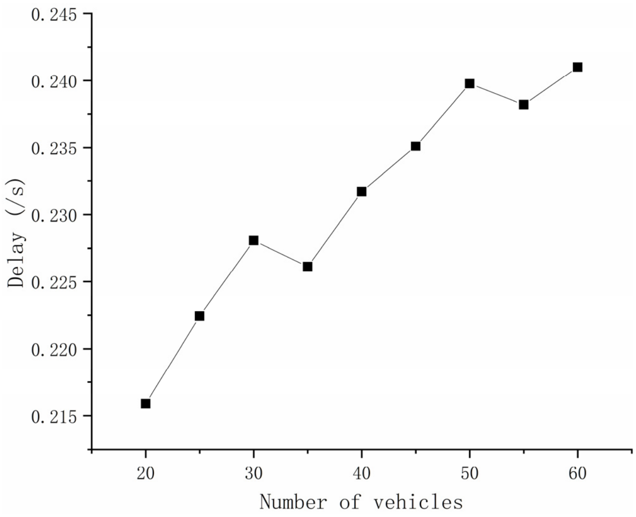


FIGURE 5. Vehicle density and delay.

TABLE 6. Security requirements comparison.

Security Requirements	Cui *et al.* [19]	Han *et al.* [33]	Liu *et al.* [34]	Our scheme
Anonymous	Yes	Yes	Yes	Yes
Quantum Resistance	Yes	No	Yes	Yes
Anonymous	Yes	Yes	Yes	Yes
Traceability	Yes	No	No	Yes
Strong Unforgeability	No	No	No	Yes

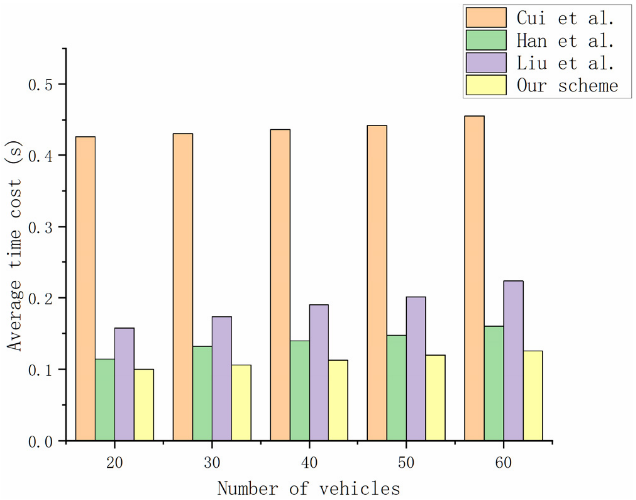


FIGURE 6. Vehicle density and delay.

As shown in TABLE 6, existing schemes fail to provide some of the security requirements in the VANET, but our scheme has achieved more security requirements.

With the same parameters and environments, we tested the performance with four schemes. To facilitate a comparison, we preset the secret key for all vehicles and disregard the process of secret key generation in vehicles. The result is shown in FIG. 6. Compared with existing schemes, our scheme has greater advantages compared with Cui *et al.* and has some advantages compared to the other two schemes.

VIII. CONCLUSION

As the forefront of the current new technology, VANET technology especially depends on security technology. We apply the latest lattice technology to the vehicle network and solve the privacy protection problem in the VANET with the help of ring signature.

This paper has the following contributions. First, based on previous work, we use the ideal lattice to improve the lattice-based ring signature to make it quantum-resistant and optimize the efficiency. Second, the traceability is increased by means of additional information so that the ring signature has a wider application space. Last, combined with the application environment of VANET, we give its privacy protection scheme; its performance is evaluated in NS-2.

Generally, the TRS scheme on the ideal lattice that we proposed has a great improvement in efficiency. However, a lattice-based ring signature needs to be further optimized in the application. This research direction will be valuable in future work.

REFERENCES

[1] R. L. Rivest, A. Shamir, and Y. Tauman, “How to leak a secret,” in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2001, pp. 552–565.

[2] F. Zhang and K. Kim, “ID-based blind signature and ring signature from pairings,” in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2002, pp. 533–547.

[3] J. Herranz and G. Sáez, “New identity-based ring signature schemes,” in *Proc. Int. Conf. Inf. Commun. Secur.* Berlin, Germany: Springer, 2004, pp. 27–39.

[4] S. S. Chow, S.-M. Yiu, and L. C. Hui, “Efficient identity based ring signature,” in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Berlin, Germany: Springer, 2005, pp. 499–512.

[5] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, Jan. 1999.

[6] C. Peikert, “Lattice cryptography for the Internet,” in *Proc. Int. workshop Post-Quantum Cryptogr.* Berlin, Germany: Springer, 2014, pp. 197–219.

[7] J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö. Dagdelen, “Authenticated key exchange from ideal lattices,” in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2015, pp. 719–751.

[8] V. Lyubashevsky and D. Micciancio, “Asymptotically efficient lattice-based digital signatures,” in *Proc. Theory Cryptography Conf.* Berlin, Germany: Springer, 2008, pp. 37–54.

[9] C. Gentry, C. Peikert, and V. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” in *Proc. Annu. ACM Symp. Theory Comput.*, 2008, pp. 197–206.

[10] V. Lyubashevsky, “Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures,” in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2009, pp. 598–616.

[11] C. Peikert, “Bonsai trees (or, arboriculture in lattice-based cryptography),” Cryptol. ePrint Arch., Tech. Rep. 2009/359, Jul. 2009. [Online]. Available: http://eprint.iacr.org/

[12] F.-H. Wang, Y.-P. Hu, and C.-X. Wang, “A lattice-based ring signature scheme from bonsai trees,” *J. Electron. Inf. Technol.*, vol. 32, no. 10, pp. 2400–2403, Dec. 2010.

[13] L. Ducas and D. Micciancio, “Improved short lattice signatures in the standard model,” in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2014, pp. 335–352.

[14] D. Zhang, T. Zhang, and X. Liu, *Novel Self-Adaptive Routing Service Algorithm for Application in VANET*. Berlin, Germany: Springer, 2019, pp. 1866–1879.

[15] D. He, S. Zeadally, B. Xu, and X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Aug. 2015.

[16] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, “PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks,” *IEEE Trans. Dependable Secure Comput.*, early access, Mar. 11, 2019, doi: 10.1109/TDSC.2019.2904274.

[17] J. Cui, J. Zhang, H. Zhong, and Y. Xu, “SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Nov. 2017.

[18] M. Azees, P. Vijayakumar, and L. J. Deboarh, “EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[19] Y. Cui, L. Cao, X. Zhang, and G. Zeng, “Ring signature based on lattice and VANET privacy preservation,” *Chin. J. Comput.*, vol. 40, pp. 1–14, Dec. 2017.

[20] V. Lyubashevsky and D. Micciancio, “Asymptotically efficient lattice-based digital signatures,” *J. Cryptol.*, vol. 31, no. 3, pp. 774–797, Jul. 2018.

[21] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa, “Efficient public key encryption based on ideal lattices,” in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2009, pp. 617–635.

[22] A. Bender, J. Katz, and R. Morselli, “Ring signatures: Stronger definitions, and constructions without random oracles,” *J. Cryptol.*, vol. 22, no. 1, pp. 114–138, Jan. 2009.

[23] J. Liu, “Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks,” *Tsinghua Sci. Technol.*, vol. 24, pp. 575–584, Apr. 2019.

[24] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” *Veh. Commun.*, vol. 1, pp. 7–20, Jan. 2017.

[25] S. Agrawal, D. Boneh, and X. Boyen, “Efficient lattice (H) IBE in the standard model,” in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2010, pp. 553–572.

[26] S. Agrawal, D. Boneh, and X. Boyen, “Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE,” in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2010, pp. 98–115.

[27] E. Ben-Sasson, S. Kopparty, and S. Saraf, “Worst-case to average case reductions for the distance to a code,” in *Proc. 33rd Comput. Complex. Conf. (CCC)*, 2018, pp. 1–5.

[28] V. Lyubashevsky, “Lattice signatures without trapdoors,” in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2012, pp. 738–755.

[29] C. Peikert and A. Rosen, “Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices,” in *Proc. Theory Cryptography Conf.* Berlin, Germany: Springer, 2006, pp. 145–166.

[30] M. Ajtai, “Generating hard instances of the short basis problem,” in *Proc. Int. Colloq. Automata, Lang., Program.* Berlin, Germany: Springer, 1999, pp. 1–9.

[31] J. Alwen and C. Peikert, “Generating shorter Bases for hard random lattices,” in *Proc. 26th Int. Symp. Theor. Aspects Comput. Sci.*, vol. 3. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2009, pp. 535–553.

[32] W. Liqiang, Y. Xiaoyuan, and H. Yiliang, “An efficient FIBE scheme based on ideal lattices,” *Chin. J. Comput.*, vol. 38, no. 4, pp. 775–782, 2015.

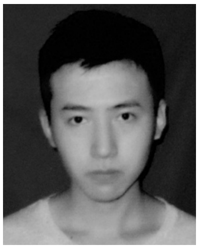
[33] Y. Han, N.-N. Xue, B.-Y. Wang, Q. Zhang, C.-L. Liu, and W.-S. Zhang, “Improved dual-protected ring signature for security and privacy of vehicular communications in vehicular ad-hoc networks,” *IEEE Access*, vol. 6, pp. 20209–20220, 2018.

[34] H. Liu, Y. Sun, Y. Xu, R. Xu, and Z. Wei, “A secure lattice-based anonymous authentication scheme for VANETs,” *J. Chin. Inst. Eng.*, vol. 42, pp. 66–73, Jan. 2019.

LONGBO HAN was born in Luoyang, Henan, in 1997. He is currently pursuing the master’s degree with the School of Computer Science and Engineering, Northwest Normal University. His research interests include lattice cryptography and privacy protection.

SUZHEN CAO was born in 1976. She received the bachelor's degree from Northwest Normal University, in 2000, and the master's degree from Lanzhou Jiaotong University, in 2010. Since July 2000, she has been teaching with the School of Computer Science and Engineering, Northwest Normal University. She is currently an Associate Professor with the School of Computer Science and Engineering, Northwest Normal University. Her research interests include public key cryptography and software security. She is a member of the China Cryptography Society.

XIAODONG YANG (Member, IEEE) received the master's degree in cryptography from the School of Science, Tongji University, in March 2005, and the Ph.D. degree in cryptography from the School of Mathematics and Information Science, Northwest Normal University, in June 2010. He was with the State Key Laboratory of Cryptography and Technology to engage in Postdoctoral Research, in September 2016. He is currently a Professor with Northwest Normal University, the Director of the Institute of Information Security, and a Postdoctoral Fellow with the State Key Laboratory of Cryptography and Technology. He is mainly engaged in research and development of modern cryptography, cloud computing security, big data security, the Internet of Things security, blockchain, information, and network security. He has served as a Reviewer for computer journals, such as IEEE Access and the *Journal of Software*. He has served as a Review Expert for the National University Student Information Security Competition.



ZHIQIANG ZHANG was born in Jining, Shandong, in 1995. He is currently pursuing the master's degree with the School of Computer Science and Engineering, Northwest Normal University. His research interests include information security cryptography and attribute-based encryption.