TSINGHUA SCIENCE AND TECHNOLOGY
ISSNll1007-0214 06/10 pp575–584
DOI: 10.26599/TST.2018.9010131
Volume 24, Number 5, October 2019

Lattice-Based Double-Authentication-Preventing Ring Signature for Security and Privacy in Vehicular Ad-Hoc Networks

Jinhui Liu, Yong Yu*, Jianwei Jia, Shijia Wang, Peiru Fan, Houzhen Wang, and Huanguo Zhang

Abstract: Amidst the rapid development of the Internet of Things (IoT), Vehicular Ad-Hoc NETwork (VANET), a typical IoT application, are bringing an ever-larger number of intelligent and convenient services to the daily lives of individuals. However, there remain challenges for VANETs in preserving privacy and security. In this paper, we propose the first lattice-based Double-Authentication-Preventing Ring Signature (DAPRS) and adopt it to propose a novel privacy-preserving authentication scheme for VANETs, offering the potential for security against quantum computers. The new construction is proven secure against chosen message attacks. Our scheme is more efficient than other ring signature in terms of the time cost of the message signing phase and verification phase, and also in terms of signature length. Analyses of security and efficiency demonstrate that our proposed scheme is provably secure and efficient in the application.

Key words: Vehicular Ad-Hoc NETwork (VANET); privacy; security; Double-Authentication-Preventing Ring Signature (DAPRS); lattice

1 Introduction

The Internet of Things (IoT) paradigm promises to change the means of interaction between networks and the physical world. A typical IoT deployment includes sensors, actuators, and other smart devices connected to the Internet. These devices facilitate the collection and exchange of information for a wide range of applications. A Vehicular Ad-Hoc NETwork (VANET), a type of mobile ad-hoc network, is a typical IoT application. It provides an important technical support for intelligent traffic control and improves the efficiency and safety of transportation. At present, the biggest challenge with VANETs is how to maintain a balance between security and privacy. The receiver needs to be sure that they are receiving reliable information from the origin, but establishing this reliability may work against the sender's need for privacy.

A large number of security and privacy protection schemes have been proposed for VANETs. They can be classified into anonymous certificates schemes[1, 2], pseudonym-based authentication schemes[3–5], group signature schemes[6, 7], and ring signature schemes[8, 9]. In regard to protecting location privacy, pseudonym-based schemes are popular and have been the focus of extensive research. Unfortunately, pseudonym-based schemes require constant modification of pseudonyms in order to effectively protect privacy, and this creates a bottleneck in the operation of VANETs. Therefore, pseudonym-based authorization schemes may not be the best solution for protecting location privacy.

In recent years, many representative works have concentrated on the use of anonymous certificates. For example, Vijayakumar et al.[2] presented an efficient

• Jinhui Liu and Yong Yu are with the School of Computer Science, Shaanxi Normal University, Xi'an 710119, China. E-mail: jh.liu@snnu.edu.cn; yuyong@snnu.edu.cn.

• Shijia Wang is with the Department of Statistics and Actuarial Science, Simon Fraser University, Burnaby, V5A1S6, Canada. E-mail: shijiaw@sfu.ca.

• Jianwei Jia, Peiru Fan, Houzhen Wang, and Huanguo Zhang are the with School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China. E-mail: jjwwhu@whu.edu.cn; fanpeiru@whu.edu.cn; wanghouzhen@126.com; liss@whu.edu.cn.

∗ To whom correspondence should be addressed.

Manuscript received: 2018-10-16; accepted: 2018-11-10

privacy preserving anonymous authentication scheme for VANETs. The scheme is highly efficient in terms of the delays involved in signature and certificate verification; however, it maintains conditional privacy. For an anonymous certificate, in order to reduce communication overhead and to minimize cryptographic packet loss, Feiri et al.[10] combined certificate pre-distribution and certificate omission in order to reduce communications overhead and minimize cryptographic packet loss. Although the use of anonymous certificates is able to achieve the purpose of privacy protection, it needs further investigation to overcome weaknesses in certificate distribution and revocation, and numerous problems with certificate storage.

Group signature schemes use traits of anonymity and traceability to construct anonymous certificate schemes. For example, Lin et al.[11] used group signatures in proposing a security and privacy-preserving protocol. The key features of this protocol are that the vehicles' On Board Units (OBUs) are not asked to store massive anonymous keys, and the Trust Authority (TA) is able to trace a misbehaving vehicle. The need to store revocation lists is a problem for this group of methods. Some vehicles need to store a revocation list in case of communication with revoked vehicles and, for a wide-ranging network, the demands on the verification process rise linearly as vehicles are added to the revocation list. Moreover, all group signatures schemes have to face up to an important problem, namely how to select a group administrator. The group administrator holds great power in a group signature scheme, but the general assumption that they are honest and reliable may not hold, which poses a threat to the security of group signatures.

On this front, ring signature-based authentication schemes have the advantage of not having an administrator role. All members of the ring have equal status, which is better for the preservation of privacy. Also, compared with anonymous certificate schemes, ring signature authentication does not require to communicate with certificate authorities, making it more flexible and self-contained. Although ring signature schemes are not as simple as pseudonym-based schemes, they can achieve a higher level of security. With the development of quantum computers, there have appeared a few ring signatures for VANETs, especially using a lattice-based ring signature. Most of these are based on traditional mathematical hard problems, such as the discrete logarithm problem or the large integer factorization problem.

In this paper, to prevent fraud by discouraging users from submitting (signing) duplicates, we use Double Authentication Preventing Signatures (DAPSs) instead of conventional signatures, where the address a (or its associated space) can be given some application dependent semantics. DAPSs are stronger signatures in the sense that they can reveal a signer's secret key to the public[11–15]. In anonymous credential systems, revealing the secret key is related to the Public Key Infrastructure (PKI) assured non-transferability concept, which discourages fraudulent behavior. Many instances show that while DAPS in itself offers detection, this may not be enough of a deterrence for fraud. Consequently, by combining ring signature and DAPS, we provide a lattice-based Double-Authentication-Preventing Ring Signature (DAPRS).

Based on DAPRS, we propose a new and practical conditional privacy protection scheme for VANETs. Our latticed-based DAPRS has a number of advantages. First, the use of a ring signature-based scheme means equality between numbers; compared with group signatures, there is no group administrator and therefore the scheme offers enhanced privacy protection. Second, in comparison with anonymous certificate-based schemes, ours does not need to keep in contact with certification distribution agents and offer greater flexibility. Third, although the proposed scheme is more complex than a pseudonym-based scheme, it is more secure and has the useful property of extractability.

Our contribution: This paper presents the first secure lattice-based DAPRS applied to VANETs, covering anonymity, unforgeability, extractability, and non-slanderability. Our scheme has the potential to defend against quantum computer attacks, which have been of widespread concerned for decades[16, 17].

The structure of the paper is as follows. Section 2 presents some preliminaries including notations, mathematical functions, and syntax. Section 3 provides system model and security goals, while the details of our proposed scheme are given in Section 4. Security and efficiency analyses are presented in Sections 5 and 6, respectively.

2 Preliminaries

In this section, we introduce some notations and mathematical tools, and the Existential UnForgeability under Chosen Message Attack (EUF-CMA) security of DAPS and DAPRS syntax.

2.1 Notations

The main symbols used in our scheme are illustrated in Table 1 along with their definitions.

2.2 Collision-resistant hash functions

Suppose that $\mathcal{D}$ is a ring $Z_p[x]/\langle x^n + 1\rangle$, where n is the power of 2. Let $\mathcal{D}_\times = \{y \in \mathcal{D}, \|y\|_\infty \leqslant d\}$ be a set for some integer d and $H(\mathcal{D}, \mathcal{D}_\times, m)$ be a hash function family which satisfies linear property such that $m > \log p/\log(2d)$ and $p \geqslant 4dmn^{1.5}\log n$. That is to say, if $h \in H(\mathcal{D}, \mathcal{D}_\times, m)$, it satisfies properties

$$\begin{cases} h(\widehat{y} + \widehat{z}) = h(\widehat{y}) + h(\widehat{z}), & \widehat{y}, \widehat{z} \in \mathcal{D}^{m_u}, \\ h(\widehat{y}c) = ch(\widehat{y}), & c \in \mathcal{D} \end{cases} \tag{1}$$

where $\widehat{y} = (y_1, \ldots, y_m)$, $\widehat{z} = (z_1, \ldots, z_m)$.

For random $h \in H(\mathcal{D}, \mathcal{D}_\times, m)$, if there exists a polynomial-time algorithm that can solve $\text{Col}(h, \mathcal{D}_\times)$ with a non-negligible probability, then for every lattice in $\mathcal{D}$ there exists a polynomial-time algorithm that can solve $SVP_\gamma(\mathcal{L})$ problem corresponding to an ideal, where $\gamma = 16dmn\log^2 n$[18].

Table 1 Notation.

Notation	Description
Z_p	Quotient ring Z/pZ
κ	Security parameter
n	Power of 2 greater than security parameter κ
p	Prime of order $\Theta(n^{4+c})$ such that $p \equiv 3 \bmod 8$
Ring $\mathcal{D} = Z_p[x]/\langle x^n + 1\rangle$	$x^n + 1$ is irreducible and the elements of $\mathcal{D}$ are represented by $\{-(p-1)/2, \ldots, (p-1)/2\}$.
Polynomials	Roman letters $(a, b, \ldots)$
Vectors of polynomials	Roman letters with a hat $(\widehat{a}, \widehat{b}, \ldots)$
$\widehat{a} = (a_1, \ldots, a_m)$	$a_1, \ldots, a_m$ are polynomials in $\mathcal{D}$.
Infinity norm ℓ_∞	$\|a\|_\infty = \max_i \|a_i\|$ and $\|\widehat{a}\|_\infty = \max_i \|a_i\|_\infty$
$[i]$	Set $\{1, 2, \cdots, i\}$
$x \leftarrow S$	Uniformly random sample from the set S
$x \leftarrow$ *RandomizedAlgorithm*	Sampling from a *RandomizedAlgorithm*
m_u	$3 + (2c/3)\log n$
m	$3 + (2c/3n^c)\log n$
$\mathcal{D}_h$	$\{g \in \mathcal{D} : \|g\|_\infty \leqslant (mn^{1.5} + n^{0.5})\log n\}$
$\mathcal{D}_y$	$\{g \in \mathcal{D} : \|g\|_\infty \leqslant mn^{1.5}\log n\}$
$\mathcal{D}_z$	$\{g \in \mathcal{D} : \|g\|_\infty \leqslant (mn^{1.5} - n^{0.5})\log n\}$
$\mathcal{D}_{S,c}$	$\{g \in \mathcal{D} : \|g\|_\infty \leqslant 1\}$
index(R)	Set of integers corresponding to indexes of pk
Random oracle H	$\{0,1\}^* \longrightarrow \mathcal{D}_{S,c}$
V_i	The i-th vehicle

2.3 Statistical distance

For any function f with domain A which may be possibly randomized, the statistical distance between $f(x)$ and $f(x')$ is at most

$$\Delta(f(x), f(x')) \leqslant \Delta(x, x'),$$

where x and x' are two random variables over a common set A and

$$\Delta(X, X') = \frac{\sum\limits_{x \in S} |Pr[X = x] - Pr[X' = x]|}{2},$$

and $\Delta(f(X), f(X')) =$

$$\frac{\sum\limits_{x \in S} |Pr[f(X) = f(x)] - Pr[f(X') = f(x)]|}{2}.$$

2.4 EUF-CMA of DAPS

For all adversaries $\mathcal{A}$, if there exists a negligible function $\varepsilon(\cdot)$ such that

$$Pr[\exp^{EUF\text{-}CMA}_{\mathcal{A},DAPS}(\kappa) = 1] \leqslant \varepsilon(\kappa),$$

where the experiment $\exp^{EUF\text{-}CMA}_{\mathcal{A},DAPS}(\kappa)$ is given as follows:

```
$(sk_{\mathcal{D}}, pk_{\mathcal{D}}) \leftarrow K\text{Gen}_{\mathcal{D}}(1^\kappa)$,
$\mathcal{Q} \leftarrow \varnothing', \mathcal{R} \leftarrow \varnothing'$,
$(m^*, \sigma^*) \leftarrow \mathcal{A}^{\text{sign}'_{\mathcal{D}}(sk_{\mathcal{D}}, \cdot)}(pk_\Sigma)$,
if $\text{verify}_{\mathcal{D}}(pk_{\mathcal{D}}, m^*, \sigma^*) = 1 \wedge m^* \notin \mathcal{Q}$
return 1,
else
return 0.
```

Then the DAPS scheme is EUF-CMA secure, where the oracle $\text{sign}'_{\mathcal{D}}$ on input m is given as follows:

```
$(a, p) \leftarrow m$,
if $a \in \mathcal{R}$
return $\perp$,
else
$\sigma \leftarrow \text{sign}_{\mathcal{D}}(sk_{\mathcal{D}}, m)$,
$\mathcal{Q} \leftarrow \mathcal{Q} \cup \{m\}, \mathcal{R} \leftarrow \mathcal{R} \cup \{a\}$,
return $\sigma$.
```

DAPS requires a restricted standard notion of unforgeablility, where $\mathcal{A}$ can adaptively query signatures for a message (a, p), but only on a distinct address a.

2.5 Syntax of DAPRS

A DAPRS scheme, is a tuple of four Probabilistic Polynomial-Time (PPT) algorithms (**Setup**, **Sign**, **Verify**, and **Extract**$_{sk}$).

Setup: On inputting a security parameter λ, the algorithm outputs a pair of public key pk, secret key sk, and a set of security parameters *param* which includes λ.

Sign: On inputting *param*, group size l, a private key sk, a set of l public keys, and a message (a, p), the algorithm outputs a signature σ for the message (a, p).

Verify: On inputting *param*, group size l, a set of l public keys, and a message-signature pair $((a, p), \sigma)$, the algorithm returns accept or reject. If it returns accept, the message-signature pair is valid; otherwise, the signature is to be rejected.

Extract$_{sk}$: On inputting *param*, group size l, a private key sk, a set of l public keys, and message-signature pair (a, p_1, σ) and (a, p_2, σ), the algorithm outputs the signer's signature key sk.

The DAPRS scheme must satisfy the following relationships:

Verification correctness. The signature is accepted during the verification algorithm phase.

Double signature extractability. If a signer generates two signatures on two colliding messages (a, p_1) and (a, p_2), the signature key sk can be extracted.

3 System Model and Security Goals

In this section, we provide some of the main entities and attributes of VANETs. In addition, we show some security goals that should be satisfied during communication processes in VANETs.

3.1 System model

The system model for VANETs scenarios consists of three entities: a Trust Authority (TA), a vehicle equipped with an On-Board Units (OBU), and a Road Side Unit (RSU). A typical structure for a VANET is presented in Fig. 1[19]. VANETs feature two communication modes: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I).

TA: TA registers the OBU and RSU, and initializes them with public system information or private keys. It has a powerful computation ability and is responsible for generating the master key and system parameters. It is also responsible for registering OBU and RSU.

OBU: OBU is a stationary wireless access point. Executing the DSRC protocol under which a vehicle should broadcast a message every 100 ms – 300 ms, it receives messages from vehicles, verifies their validity, and sends them to the traffic control center.

RSU: RSU is a tamper-proof device issued by the TA. Through pre-loaded system parameters and private keys, it generates a temporary private key and uses it to sign a message.

3.2 Security requirements

The major goal of our proposed scheme is to provide an efficient privacy-preserving anonymous authentication scheme which satisfies the following security requirements:

(1) Message integrity and anonymous authentication: When a vehicle moves into the region of an RSU, it needs to be authenticated by the RSU before it issues the safety-related messages. A vehicle must also authenticate other vehicles before it receives messages from them. Both of these authentications need to be done anonymously. To preserve the integrity of the transmissions, each message must also be appended with an anonymous signature.

(2) Anonymity: Each vehicle's real identity is hidden from other entities in the network. However, TA has a capacity to obtain the real identity of any malicious vehicle that may be sending bogus messages to other vehicles so as to disrupt traffic.

(3) Unforgeability and non-slanderability: Unforgeability and non-slanderability are based

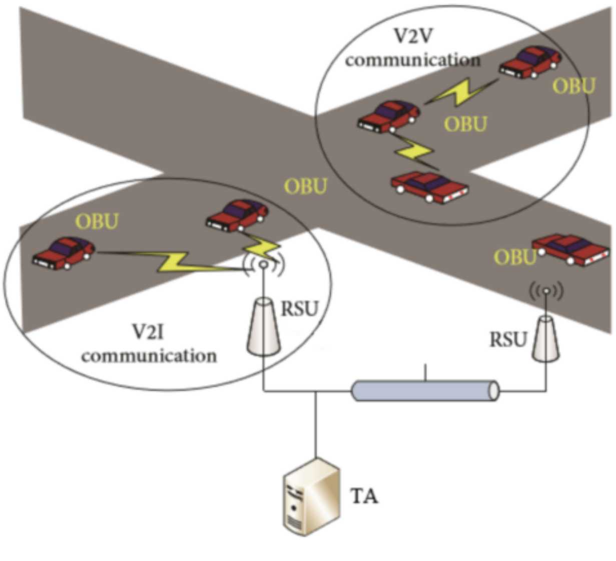


Fig. 1 Typical structure of VANET.

on the underlying hard problem assumption, which can be proved by the ring signature scheme.

(4) Deterable-iff-double signature by one signer: If a vehicle signs on colliding messages (a, p_1) and (a, p_2), it can be identified and its signature keys can be extracted by anyone.

4 DAPRS for VANETs

In this section we present details of our privacy protection scheme for VANETs based on DAPRS. Each vehicle can receive a pair of public keys from other moving vehicles' messages. When a vehicle (sender) wants to authenticate a message $m = (a, p)$, it chooses n valid public keys $(h_1, \ldots, h_n)$ to form a ring R. The the vehicle then makes a ring signature σ with respect to (a, p, R) based on the underlying DAPRS. On the one hand, if σ is a valid signature, then the receiver believes that (a, p) is sent by a member of ring R without knowing which member; so the actual identity of the signer is protected. On the other hand, if there are two valid signatures σ_1 and σ_2 on messages (a, p_1) and (a, p_2) from the same vehicle, then the signature keys of that vehicle can be extracted. In this way, the underlying DAPRS can be unconditionally anonymous for the signer.

Our proposed scheme is made up of four parts: system initialization and membership registration, OBU safety message generation, message verification, and extractability of double signatures by one signer.

4.1 System initialization and membership registration

Given a security parameter κ, TA generates the parameters (κ, n, m_u, p, S), where n is the power of 2 and $n > \kappa$, $m_u = 3\log n$, and p is a prime larger than n^4 such that $p \equiv 3 \bmod 8$. According to these parameters, we define $\mathcal{D}, \mathcal{D}_h, \mathcal{D}_z, \mathcal{D}_y$, and $\mathcal{D}_{s,c}$, the family $\mathcal{H}$, and $S \leftarrow \mathcal{D}$, $S \neq 0$. We then proceed with the following steps.

(1) Set $\widehat{s} = (s_1, \ldots, s_{m_u}) \leftarrow \mathcal{D}_{s,c}^{m_u}$.

(2) If s_i is non-invertible, go to Step 1.

(3) Choose an invertible s_{i_0}, where $i_0 \in \{1, \ldots, m\}$.

(4) Pick $(a_1, a_2, \ldots, a_{i_0-1}, a_{i_0+1}, \ldots, a_{m_u}) \leftarrow \mathcal{D}^{m_u-1}$.

(5) Let $a_{i_0} = s_{i_0}^{-1}(S - \sum_{i\neq i_0} a_i s_i)$ and set $\widehat{a} = (a_1, a_2, \ldots, a_{m_u})$.

(6) TA selects a secure signature algorithm sig$(\cdot)$ and a cryptographic hash functions $h(\widehat{s}) = \widehat{a}\widehat{s} \in \mathcal{H}$ defined by $\widehat{a}$. After that, TA randomly selects $\widehat{s}$ as its private key, and $\widehat{a}$ and h as its public keys.

Each vehicle V_i with its real identity RID_i, then self-generates its key pair by itself and obtains its certificate from TA as follows.

(7) Choose $\widehat{s}_i$ as its private key and compute $\widehat{b}_i = \widehat{a}\widehat{s}_i$ as its public key.

(8) Select $\widehat{t}_i$ to compute verification information $S_i = H(\widehat{a}\widehat{t}_i \| RID_i)$ and $\widehat{c}_i = \widehat{t}_i + \widehat{b}_i S_i$. Then send $(\widehat{b}_i, RID_i, S_i, \widehat{c}_i)$ to TA for registration.

(9) After V_i receives this message, the TA checks whether the following equation holds or not:

$$S_i \overbrace{=}^{?} H(\widehat{a}(\widehat{c}_i - \widehat{b}_i H(\widehat{a}\widehat{t}_i \| RID_i)) \| RID_i).$$

If it does hold, b_i and RID_i are defined as a valid public key and identity of V_i, respectively. After that, the TA stores (b_i, RID_i) and creates $Cert_i = \text{sig}(b_i, RID_i; \widehat{s}_{TRC})$ for V_i with the TA's private key $\widehat{s}_{TRC}$. Finally, the tamper-proof device of each vehicle is preloaded with $(\widehat{s}_i, b_i, RID_i, Cert_i)$.

(10) A ring set generation phase. Once V_i moves into a region which is covered by an RSU, the V_i applies to form a ring R. When the RSU receives the application, it verifies its effectiveness and timeliness. The RSU puts the public keys into the ring, and when the default value is achieved by public keys, RSU broadcasts the ring set. All vehicles contained in the ring set can then use the ring to sign their corresponding messages.

4.2 Message signature

When a vehicle broadcasts messages to other vehicles, it first construct a message with a timestamp, then it chooses a ring containing the public keys of the ring members. The signature generation algorithm is listed as follows.

Taking a common vehicle V_k, once it has been moving on the road for some time it will have collected and stored many public keys of other vehicles. Let these public keys be $\mathcal{R} = \{\widehat{h}_1, \ldots, \widehat{h}_l, S, \widehat{a}, H_1\}$, where H_1 is a cryptographic hash function. When V_k needs to send and authenticate the message $m = (a, p_k)$, it randomly chooses n public keys from set $\mathcal{R}$ to form a ring R. We then proceed with the following steps.

(1) V_k verifies $\widehat{s}_k \in \mathcal{D}_{s,c}^{m_u}$; R is of a size bounded by κ^c; one of the public keys in $\mathcal{R}$ is associated to $\widehat{s}_k$. If verification fails, output a failure result.

(2) For all $i \in [l], i \neq k, \widehat{y}_k \leftarrow \mathcal{D}_{\widehat{z}}^{m_u}$.

(3) For $i = k, \widehat{y}_k \leftarrow \mathcal{D}_y^{m_u}$.

(4) Set $e \leftarrow H_1(\sum_{i\in[l]} h_i(\widehat{y}_k), p_k)$, where e is in $\mathcal{D}_{s,c}$.

(5) For $i = k$, V_k computes $\widehat{z}_k \leftarrow a\widehat{s}_k e + \widehat{y}_k$.

(6) If $\widehat{z}_k \notin \mathcal{D}^{m_u}_{\widehat{z}}$, go to Step 2.

(7) For $i \neq k$, $\widehat{z}_i = \widehat{z}_k$.

The signature with respect to (a, p_k, R) is $\sigma = (\widehat{z}_1, \dots, \widehat{z}_l, e)$. Finally, V_k broadcasts (a, p_k, R, σ).

Note that the signature pair $(\widehat{z}_1, \dots, \widehat{z}_l) \leftarrow \mathcal{D}^{m_u}_{\widehat{z}}$ does not reveal the signer's identity, so we do not need to hide the identity of a ring signer using a Non-Interactive Zero-Knowledge (NIZK) proof.

4.3 Message verification

Upon receiving (a, p_k, R, σ), a nearby receiver V_k, checks whether these public keys b_i in the ring R are presented in Certificate Revocation List (CRL) or not. If none of the public keys b_k are in CRL, V_k checks σ using the following steps:

(1) For all $k \in [l]$, V_k verifies $\widehat{z}_k \in \mathcal{D}^{m_u}_{z}$.

(2) V_k verifies whether the following step holds.

$$e \overbrace{=}^{?} H_1\Big(\sum_{i\in\{1,\dots,l\}} h_i(\widehat{z}_k) - aSe, p_k\Big).$$

If it does hold, V_k believes that the message (a, p_k) is authenticated by one member in the ring R without knowing which member it is.

4.4 Deterable of double signatures

It is necessary for all nodes to find the true identity of a signer who sometimes signs twice in some cases, since duplicate signatures can cause higher traffic load.

We suppose that all nodes actively cooperate. From the input of two signatures $\sigma = (\widehat{z}_1, \dots, \widehat{z}_l, e)$ and $\sigma' = (\widehat{z}'_1, \dots, \widehat{z}'_l, e')$, and also from colliding messages $M_l = (a, p_l)$ and $M'_l = (a, p'_l)$ from a single signer, we first check whether the two signatures are valid. According to the two signatures σ and σ', we then compute

$$\begin{cases} \widehat{s}_j = \frac{\widehat{z}_j - \widehat{z}'_j}{a(e-e')}, & i = j, \\ \widehat{z}_j - \widehat{z}'_j \text{ is a constant}, & i \neq j \end{cases} \tag{2}$$

and verify

$$\sigma = \text{sign}(a, p_k, R, sk_i)$$

and

$$\sigma' = \text{sign}(a, p_k, R, sk_i).$$

If they hold, it is certain that σ and σ' are both generated by a vehicle V_i.

5 Security Analysis

The proposed lattice-based DAPRS for VANETs not only has the potential to resist quantum computation, but also has some specific security requirements: message integrity and authentication, anonymity, spontaneity, existential unforgeability under chosen message attack, and deterable-iff-linked.

5.1 Theoretical analysis

(1) Message integrity and authentication

Under the process followed by the proposed scheme, a signer generates a temporary private key and uses it to generate a signature on the message (a, p_i). According to the security analysis, no adversary is able to generate a legal signature σ_i. Therefore, the RSU can authenticate the OBU and detect any modification of the received signature by checking whether the equation $S_i \overbrace{=}^{?} H(\widehat{a}(\widehat{c}_i - \widehat{b}_i H(\widehat{a}\widehat{t}_i \| RID_i)) \| RID_i)$ holds. Message integrity and authentication for VANETs is thus ensured by the proposed scheme.

(2) Anonymity

Supposing that a receiver has received a true signature σ, every σ is a reasonable value in a corresponding domain. So the success probability of the ring signer's identity being guessed by a person outside the n members is $1/n$. The success probability of the ring signer being guessed by a ring member (except for the actual signer itself) is $1/(n-1)$.

(3) Spontaneity

Each member is able to complete a signature without the participation of any other members. The resulting spontaneity is better able to hide a signer's identity.

(4) Existential unforgeability under chosen message attack

An attacker can not forge a signature because of the ring signature security underlying our scheme, which is EUF-CMA secure[18].

5.2 Security proof

In the anonymity game, an adversary gets a signature depending on public parameter $\mathcal{P} = (\kappa, n, m_u, p, S)$, as well as on a random bit b, secret keys sk_{i_0} and sk_{i_1}, a message (a, p_i), and a ring R. All the parameters can be adversarially chosen except for b.

Suppose that $X_{b,\mathcal{P},sk_{i_b},a,p_i,R}$ is a random variable which represents a signature accepted by the adversary $\mathcal{A}$ for some given parameters. For any choice of $(\mathcal{P}, sk_{i_0}, sk_{i_1}, a, p_i, R)$, the following theorems state that the statistical distance between $X_{0,\mathcal{P},sk_{i_0},a,p_i,R}$ and $X_{1,\mathcal{P},sk_{i_1},a,p_i,R}$ is negligible in k. By using the properties of statistical distance, our scheme for VANETs ensures unconditional anonymity under chosen message attack.

Theorem 1 (Anonymity) For $b \in \{0,1\}$, let $X_{b,\mathcal{P},sk_{i_b},a,p_i,R}$ be the random variable. If domains of these variables are different from $\{failed\}$, we have

$$\Delta(X_{0,\mathcal{P},sk_{i_0},a,p_i,R}, X_{1,\mathcal{P},sk_{i_1},a,p_i,R}) = n^{-\omega(1)}.$$

Proof Let X_0 and X_1 be two random variables. $\ell + 1$ coordinates vector X_b^i of the ring signature algorithm represents the random variable related to the i-th coordinate of X_b for $i \in [\ell + 1]$ and $b \in \{0,1\}$. The set

$$\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1}) =$$

$$\{c \in \mathcal{D}_{s,c} : \|sk_{i_0}\|_\infty, \|sk_{i_0}\|_\infty \leqslant \sqrt{n}\log n\}$$

has a cardinality negligibly close to $\mathcal{D}_{s,c}$. Since

$$\frac{|\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})|}{|\mathcal{D}_{s,c}|} = 1 - n^{-\omega(1)},$$

it guarantees sk_{i_0} and $sk_{i_1} \in \mathcal{D}_{s,c}$, where $n \geqslant \kappa$ and $n^{-\omega(1)}$ is a negligible function.

Let

$$\Delta(X_0, X_1) =$$

$$\frac{1}{2}\sum_{\widehat{\alpha}_i \in \mathcal{D}_z^{mu}, i\in[\ell], \beta\notin\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})} |Pr[X_0 = (\alpha_i; i \in [\ell], \beta)] - Pr[X_1 = (\alpha_i; i \in [\ell], \beta)]| +$$

$$\frac{1}{2}\sum_{\widehat{\alpha}_i \in \mathcal{D}_z^{mu}, i\in[\ell], \beta\in\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})} |Pr[X_0 = (\alpha_i; i \in [\ell], \beta)] - Pr[X_1 = (\alpha_i; i \in [\ell], \beta)]|.$$

As for the first part of $\Delta(X_0, X_1)$, we have

$$\frac{1}{2}\sum_{\widehat{\alpha}_i \in \mathcal{D}_z^{mu}, i\in[\ell], \beta\notin\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})} |Pr[X_0 = (\alpha_i; i \in [\ell], \beta)] - Pr[X_1 = (\alpha_i; i \in [\ell], \beta)]| \leqslant$$

$$\frac{1}{2}\sum_{\widehat{\alpha}_i \in \mathcal{D}_z^{mu}, i\in[\ell], \beta\notin\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})} |Pr[X_0 = (\alpha_i; i \in [\ell], \beta)]| + |Pr[X_1 = (\alpha_i; i \in [\ell], \beta)]|.$$

For any $b \in \{0,1\}$, $\sum_{\forall A} Pr[A \wedge B] = Pr[B]$, we have

$$\sum_{\widehat{\alpha}_i \in \mathcal{D}_z^{mu}, i\in[\ell], \beta\notin\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})} |Pr[X_b = (\alpha_i; i \in [\ell], \beta)]| = \sum_{\beta\notin\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})} Pr[X_b^{(\ell+1)} = \beta].$$

$X_b^{(\ell+1)}$ is obtained by a call to a random oracle $H(\sum_{i\in[\ell]} h_i(y_i), p_i)$, if h_i in $H(\sum_{i\in[\ell]} h_i(y_i), rp_i)$ is adversarially chosen, the probability is $1/|\mathcal{D}_{s,c}|$. Using it for all $\beta \notin \mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})$, the following equation

$$\frac{1}{2}\sum_{\widehat{\alpha}_i \in \mathcal{D}_z^{mu}, i\in[\ell], \beta\notin\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})} |Pr[X_0 = (\alpha_i; i \in [\ell], \beta)] - Pr[X_1 = (\alpha_i; i \in [\ell], \beta)]| \leqslant$$

$$1 - \frac{|\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})|}{|\mathcal{D}_{s,c}|} = n^{-\omega(1)}$$

holds.

For the second part of $\Delta(X_0, X_1)$,

$$\frac{1}{2}\sum_{\widehat{\alpha}_i \in \mathcal{D}_z^{mu}, i\in[\ell], \beta\in\mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})} |Pr[X_0 = (\alpha_i\ i \in [\ell], \beta)] - Pr[X_1 = (\alpha_i; i \in [\ell], \beta)]|,$$

each term in the sum can be transformed to

$$|Pr[(X_0^{(i)}; i \in [\ell]) = (\widehat{\alpha}_i; i \in [\ell]) | X_0^{(\ell+1)} = \beta] -$$

$$Pr[(X_1^{(i)}; i \in [\ell]) = (\widehat{\alpha}_i; i \in [\ell]) | X_1^{(\ell+1)} = \beta]|.$$

For $i \neq i_b$, if $\widehat{y}_b^{(i)} = \widehat{\alpha}_i$, we have $X_b^{(i)} = \widehat{\alpha}_i$. Since $\widehat{y}_b^{(i)}$ is drawn uniformly from $\mathcal{D}_z^{m_u}$ and $\widehat{\alpha}_i \in \mathcal{D}_z^{m_u}$, the probability that both value $Pr[X_0 = (\alpha_i; i \in [\ell], \beta)]$ and $Pr[X_1 = (\alpha_i; i \in [\ell], \beta)]$ are equal to $1/|\mathcal{D}_z^{m_u}|$.

For $i = i_b$, if $\widehat{y}_{b,i_b}^{(i)} = \widehat{\alpha}_{i_b} - sk_{i_b}\beta$, we get $X_b^{(i_b)} = \widehat{\alpha}_{i_b}$. Since $\widehat{y}_{b,i}$ is drawn uniformly at random from $\mathcal{D}_y^{m_u}$, if this value is in $\mathcal{D}_y^{m_u}$, the probability that is equal to $1/|\mathcal{D}_y^{m_u}|$. If this value is not in $\mathcal{D}_y^{m_u}$, the probability is equal to 0. By the definition of $\beta \in \mathcal{D}_{s,c}(sk_{i_0}, sk_{i_1})$, we get $sk_{i_b}\beta \leqslant \sqrt{n}\log n$ and $\widehat{\alpha}_{i_b} - sk_{i_b}\beta \in \mathcal{D}_y^{m_u}$.

Thus the first part of $\Delta(X_0, X_1)$ is negligible and the second part of $\Delta(X_0, X_1)$ is equal to zero. We thereby complete the proof. ■

Theorem 2 (Unforgeability) If there is a polynomial time algorithm that can break the existential unforgeability of our proposed scheme under chosen message attack about different a of the first part of the message, then SVP$_\gamma$ can be solved for every lattice $\mathcal{L}$, where $\gamma = O(n^{2.5} + 2c)$.

Proof Suppose that an adversary $\mathcal{A}$ can output a forged signature for our proposed DAPRS with a non-negligible probability, there exists a polynomial time challenger $\mathcal{B}$ who is able to output a forgery for Lyubashevsky's scheme with a non-negligible probability.

Setup: $\mathcal{B}$ describes a hash function, an element S of $\mathcal{D}$, and has access to random oracle H_L of the signing algorithm. For $i \in [\ell]$, $\mathcal{B}$ splits polynomial sets in ℓ sets of m_u polynomials $(a_{i,1}, \ldots, a_{i,m_u})$. Then $\mathcal{B}$

initializes $\mathcal{A}$, the associated public parameters and has access to DAPRS random oracle H which it controls.

Query phase: $\mathcal{B}$ answers random oracles and signs queries of $\mathcal{A}$. For each random oracle query (x_y, x_h, x_m), $\mathcal{B}$ tests whether it has replied to such a query. If so, it replies consistently. If not, it replies with $H(x_y, x_h \| x_m)$. For each signing query $(\{h_i\}_{i\in T}, i_0, \mu)$ for $i_0 \in T \subseteq [\ell]$, $\mathcal{B}$ performs H to produce a signature.

(1) Follow the signing step by generating $\hat{y}_i \leftarrow \mathcal{D}_y^{m_u}$ for $i \in T$.

(2) Generate randomly $r \leftarrow \mathcal{D}_{s,c}$.

(3) Check whether H_L has been called with parameters $\sum_i h_i(\widehat{y}_i - aSr, \{h_i\}_{i\in T} \| \mu)$, if so, abort.

(4) Program H so that $H(\sum_i h_i(\widehat{y}_i - aSr, \{h_i\}_{i\in T} \| \mu)) = r$ and store it.

(5) Output $(\widehat{y}_i; i \in T, r)$.

Forgery phase: $\mathcal{A}$ finishes and outputs a forgery $((z_i, i \in T, e), \mu, \{h_i\}_{i\in T})$ for $T \subseteq [\ell]$ with a non-negligible probability. In order to constitute a valid signature, the forgery must be different from $((\widehat{z}'_i, i \in T', e), \mu', \{h_i\}_{i\in T'})$ and the forger knows either $\{h_i\}_{i\in T'} \| \mu' \neq \{h_i\}_{i\in T} \| \mu$ or $\mu' \neq \mu$. Then

$$H(\sum_{i\in T'} h_i(\widehat{z}_i) - aSe, \{h_i\}_{i\in T'} \| \mu') =$$

$$H(\sum_{i\in T} h_i(\widehat{z}_i) - aSe, \{h_i\}_{i\in T} \| \mu) = r.$$

Thus

$$\sum_{i\in T'} h_i(\widehat{z}_i) - aSe = \sum_{i\in T} h_i(\widehat{z}_i) - aSe.$$

for $(\widehat{z}'_i; i \in T') \neq (\widehat{z}_i; i \in T)$. Set $\widehat{z}_i = 0$ for $i \in [\ell]\backslash T$ and $\widehat{z}'_i = 0$ for $i \in [\ell]\backslash T$, there exists a collision hash function $\mathcal{H}(\mathcal{D}, \mathcal{D}_h, \ell)$.

If the event happens with a non-negligible probability, $\mathcal{B}$ is able to solve the SVP$_\gamma$ problem using a collision-resistant hash function. That is to say, $\mathcal{B}$ can output a forgery for Lyubashevsky's scheme with a non-negligible probability. So Theorem 2 is thus proved. ■

Theorem 3 (Extractability) Given a set of signing keys $sk = \{sk_1, \ldots, sk_k\}$, it is impossible to produce $N+1$ signatures $\sigma_1, \sigma'_1, \ldots, \sigma_k, \sigma'_k, \sigma_{2k+1}$ on k collision message (a, p_i) and (a, p'_i), such that any two of them can pass the link procedure, respectively, in which $N = 2k$.

Proof Suppose that an adversary can produce $2k+1$ valid signatures $\sigma^i = (\widehat{z}^i_1, \ldots, \widehat{z}^i_l, e^i)$, $\sigma'^i = (\widehat{z}'^i_1, \ldots, \widehat{z}'^i_l, e'^i)$, $i = 1, 2, \ldots, k$, and $\sigma^{2k+1} = (\widehat{z}^{2k+1}_1, \ldots, \widehat{z}^{2k+1}_l, e^{2k+1})$, such that σ^i and σ'^i are pairwise distinct signatures on (a, p_i) and (a, p'_i).

Table 2 Security comparison.

	Zhang et al.[7]	Wang et al.[19]	Cui et al.[9]	Our proposed scheme
SR_1	√	√	√	√
SR_2	√	√	√	√
SR_3	√	√	√	√
SR_4	×	×	√	√
SR_5	×	×	×	√

Since $sk = \{sk_1, \ldots, sk_k\}$, σ_{2k+1} does not belong to the signature set $\{\sigma, \sigma'\}_{i=2k+1}$. For $j = 1, 2, \ldots, k$, according to linkability, we have

$$\begin{cases} \widehat{sk}_j = \dfrac{\widehat{z}^j - \widehat{z}'^j}{a(e^i - e'^i)}, & i = j, \\ \widehat{z}^j - \widehat{z}'^j \text{ is a constant}, & i \neq j \end{cases} \tag{3}$$

Without loss of generality, consider that this signature σ_{2k+1} is a valid signature on (a, p_k) by signature key sk_k. From Eq. (2), we have

$$\begin{cases} \widehat{sk}_k = \dfrac{\widehat{z}^k - \widehat{z}'^k}{a(e^k - e'^k)}, & i = j = k, \\ \widehat{z}^k_i - \widehat{z}'^k_i = \widehat{z}^k_j - \widehat{z}'^k_j \text{ is a constant}, & i \neq j \end{cases} \tag{4}$$

then $\sigma_{2k+1} = (\widehat{z}^k_1, \ldots, \widehat{z}^k_l, e^k) = \sigma_k$. This yields a contradiction to the hypothesis that an adversary can produce $2k+1$ valid signatures with k signing keys on k collision message (a, p_i) and (a, p'_i). Consequently, our scheme is extractable. ■

Theorem 4 (Non-slanderability) If there exists a polynomial time algorithm that can break non-slanderability against insider corruption attacks of the DAPRS for VANETs, there is a polynomial time algorithm that can break the unforgeability of the underlying DAPRS.

Proof The proof procedure is similar to that of Theorem 2. ■

6 Security and Efficiency Analysis

Let SR_1, SR_2, SR_3, SR_4, and SR_5 represent message integrity and authentication, anonymity, spontaneity, existential unforgeability under chosen message attack, and post quantum attack and Deterable-iff-double ring signature by one signer, respectively. Security comparisons of our DAPRS with some related schemes for VANETs are listed in Table 2.

The operating efficiency of our scheme is mostly affected by the signature and verification phases. The final double-signature algorithm only executes in particular cases, so the deterable of double signatures phase is not under consideration when analyzing the performance of our scheme. We compare the efficiency of our scheme with some related schemes on signature generation time, verification of signature time, and signature length. Since the cost of addition operations and hash values are very small, here we will ignore their time cost here[20, 21]. Suppose that the number of ring signature is R, T_{mul} and T_{Sample} represent the time cost of the point multiplications and SamplePre algorithms, respectively, and T_{NIZK} represents the time cost of a non-interactive zero knowledge proof. The efficiency comparisons of our DAPRS with some related schemes for VANETs are listed in Table 3. From Table 3, we can see that our scheme achieves much greater efficiency.

Table 3 Efficiency comparison.

Scheme	Signature cost	Verification cost	Signature length
Cui et al.[9]	$5lT_{mul}$	$T_{NIZK}+5lT_{mul}$	$2(l+1)m$
Wang and Sun[22]	$mT_{Sample}+$ $m(l+k-1)T_{mul}$	$m(l+k)T_{mul}$	$(l+k)m+l$
Tian et al.[23]	$mT_{Sample}+$ $m(l+1)T_{mul}$	$m(l+2)T_{mul}$	$(l+2)m$
Our scheme	$2lT_{mul}$	$2lT_{mul}$	$(l+1)m$

7 Conclusion

In this paper, we investigated a new primitive. We provided a new construction of this primitive and showed that it achieves four security properties of anonymity, unforgeability, extractability, and non-slanderability. We demonstrated that the proposed scheme achieves unconditional anonymity of messages. We conducted security and efficiency analysis, which show that our scheme for VANETs is efficient and practical.

Acknowledgment

The author would like to thank the anonymous reviewers for their constructive comments and suggestions. This work was supported by the National Key R&D (973) Program of China (No. 2017YFB0802000), the National Natural Science Foundation of China (Nos. 61772326, 61572303, 61872229, and 61802239), the NSFC Research Fund for International Young Scientists (No. 61750110528), the National Cryptography Development Fund during the 13th Five-Year Plan Period (Nos. MMJJ20170216 and MMJJ201701304), the Foundation of State Key Laboratory of Information Security (No. 2017-MS-03), the Fundamental Research Funds for the Central Universities (No. GK201702004, GK201803061, and 2018CBLY006), and the China Postdoctoral Science Foundation (No. 2018M631121).

References

[1] H. Zhu, W. Pan, B. Liu, and H. Li, A lightweight anonymous authentication scheme for VANET based on bilinear pairing, in *Proc. 4th International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, Bucharest, Romania, 2012, pp. 222–228.

[2] P. Vijayakumar, M. Azees, and L. Deborah, CPAV: Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad-hoc networks, in *Proc. IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, USA, 2015, pp. 62–67.

[3] D. Förster, F. Kargl, and H. Löhr, PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET), in *Proc. Vehicular Networking Conference (VNC)*, Paderborn, Germany, 2014, pp. 25–32.

[4] J. Petit, F. Schaub, M. Feiri, and F. Kargl, Pseudonym schemes in vehicular networks: A survey, *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 228–255, 2015.

[5] Z. Liu, L. Zhang, and X. Lin, MARP: A distributed MAC layer attack resistant pseudonym scheme for VANET, *IEEE Transactions on Dependable and Secure Computing*. DOI: 10.1109/TDSC.2018.2838136.

[6] K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, A scalable and secure key distribution scheme for group signature-based authentication in VANET, in *Proc. 8th Annual Ubiquitous Computing, Electronics, and Mobile Communication Conference (UEMCON)*, New York, NY, USA, 2017, pp. 478–483.

[7] L. Zhang, C. Li, Y. Li, Q. Luo, and R. Zhu, Group signature-based privacy protection algorithm for mobile ad-hoc network, in *Proc. IEEE International Conference on Information and Automation (ICIA)*, Wuyishan, China, 2017, pp. 947–952.

[8] 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.

[9] Y. Cui, L. Cao, X. Zhang, and G. Zeng, Ring signature based on lattice and VANET privacy preservation, *Chinese Journal of Computers*, vol. 40, no. 169, pp. 1–14, 2017.

[10] M. Feiri, R. Pielage, J. Petit, N. Zannone, and F. Kargl, Pre-distribution of certificates for pseudonymous broadcast authentication in VANET, in *Proc. IEEE 81st Vehicular Technology Conference (VTC Spring)*, Glasgow, UK, 2015, pp. 1–5.

[11] X. Lin X, X. Sun, P. H. Ho, and X. Shen, GSIS: A secure and privacy preserving protocol for vehicular communication, *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, 2008.

[12] B. Poettering and D. Stebila, Double-authentication-preventing signatures, *International Journal of Information Security*, vol. 16, no. 1, pp. 1–22, 2017.

[13] M. Bellare, B. Poettering, and D. Stebila, Deterring certificate subversion: Efficient double-authentication-preventing signatures, in *Proc. IACR International Workshop on Public Key Cryptography*, Amsterdam, the Netherlands, 2017, pp. 121–151.

[14] D. Boneh, S. Kim, and V. Nikolaenko, Lattice-based DAPS and generalizations: Self-enforcement in signature schemes, in *Proc. International Conference on Applied Cryptography and Network Security*, Kanazawa, Japan, 2017, pp. 457–477.

[15] B. Poettering, Shorter double-authentication preventing signatures for small address spaces, in *Proc. International Conference on Cryptology in Africa*, Stellenbosch, South Africa, 2018, pp. 344–361.

[16] S. Mao, P. Zhang, H. Wang, H. Zhang, and W. Wu, Cryptanalysis of a lattice-based key exchange protocol, *Science China Information Sciences*, vol. 60, no. 2, pp. 028101–028105, 2017.

[17] W. Wu, H. Zhang, H. Wang, S. Mao, S. Wu, and H. Han, Cryptanalysis of an MOR cryptosystem based on a finite associative algebr, *Science China Information Sciences*, vol. 59, no. 3, p. 32111, 2016.

[18] C. A. Melchor, S. Bettaieb, X. Boyen, L. Fousse, and P. Gaborit, Adapting Lyubashevsky's signature schemes to the ring signature setting, in *Proc. International Conference on Cryptology in Africa*, Cairo, Egypt, 2013, pp. 1–25.

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

[20] D. Li, J. Liu, Z. Zhang, Q. Wu, and W. Liu, Revocable hierarchical identity-based broadcast encryption, *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 539–549, 2018.

[21] S. Liang, Y. Zhang, B. Li, X. Guo, C. Jia, and Z. Liu, SecureWeb: Protecting sensitive information through the web browser extension with a security token, *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 526–538, 2018.

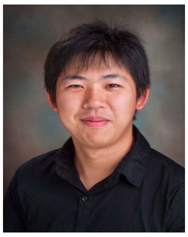
[22] J. Wang and B. Sun, Ring signature schemes from lattice basis delegation, in *Proc. International Conference on Information & Communications Security*, Beijing, China, 2011, pp. 15–28.

[23] M. Tian, L. Huang, and W. Yang, Efficient lattice-based ring signature scheme, *Chinese Journal of Computers*, vol. 39, no. 4, pp. 712–717, 2016.

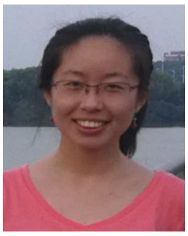
Jinhui Liu is currently a lecturer at the School of Computer Science, Shaanxi Normal University. She graduated from Wuhan University in 2017 with a PhD degree. Her research interests include post quantum cryptography and digital signature.

Yong Yu is currently a professor at the School of Computer Science, Shaanxi Normal University. He graduated from Xidian University in 2010 with a PhD degree. His research interests include information security and cryptography.

Jianwei Jia graduated from Wuhan University in 2018 with a PhD degree. His mainly research interest is information security.



Shijia Wang is a PhD candidate at Simon Fraser University, Burnaby, Canada. His research mainly focuses on statistical machine learning, computational biology, and information security.



Peiru Fan is a PhD candidate in information security with Wuhan University, China. Her current interest lies in the area of virtualization, cloud computing, and security.

Houzhen Wang received the PhD degree in information security from Wuhan University in 2011. He is currently a lecturer at the School of Cyber Science and Engineering of Wuhan University. His research interests include cryptography and information security.

Huanguo Zhang is currently a professor and a PhD supervisor at the School of Cyber Science and Engineering of Wuhan University. He graduated from Xidian University in 1970 with a bachelor degree. His research interests include information security and trusted computing.