LaRRS: Lattice-Based Revocable Ring Signature and its application for VANETs

Jiaming Wen

Joint work with Lu Bai, Zhichao Yang, Huanguo Zhang, Houzhen Wang, and Debiao He

November 2022

Overview

1. Motivation
2. Related Work and Our Result
3. Preliminaries
4. Proposed Scheme
5. Evaluations and Comparisons

1. **Motivation**
2. **Related Work and Our Result**
3. **Preliminaries**
4. **Proposed Scheme**
5. **Evaluations and Comparisons**

Background

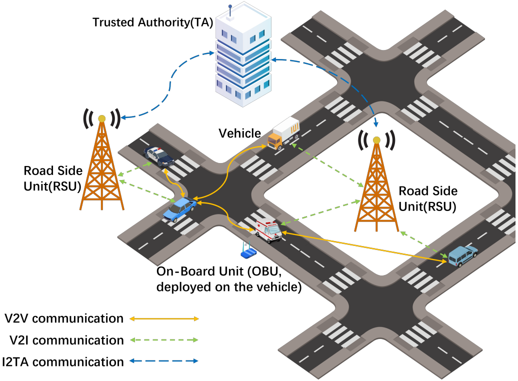


Figure: A simple example for VANETs

The VANET system mainly comprises three parts:

- Trusted Authority(TA)
- Road Side Units(RSUs) installed along the road
- On-Board Units(OBUs) deployed on vehicles

The figure shows a representative instance of VANETs.

System model

1. Trusted Authority, or TA: functions as a trusted third party in the network model and possesses strong computational capabilities. TA's duties include:
   - Generates system parameters.
   - TA is the only party with access signer's real identity.
2. Road Side Units(RSUs): fixed infrastructures at the road, communicate with nearby OBUs(on vehicles) through the DSRC protocol, and check the validity of messages received from vehicles. Then, it transmits messages to TA or processes them locally.
3. On-Board Units(OBUs): essential for each vehicle in the VANET. The device is tamper-proof and ensures that data is never leaked. Additionally, using the DSRC protocol, the OBU could offer wireless communication between the vehicle and a nearby RSU (V2I) or another vehicle (V2V).

Security Requirements

In a VANET system,

- TA is completely trusted.
- RSUs are honest but curious, they will check the validity of messages and transmit to TA, but may eavesdrop and try to analyze the identities of the broadcaster by colluding malicious OBUs rather than other RSUs.
- OBUs can be malicious, i.e., send fake information or try to impersonate other OBU.

Therefore, before using received messages, it is important to verify they are from a legitimate user(authentication) and to ensure that they have not been modified(integrity).

Security Requirements

Concretely, the major requirements of VANET models are in four aspects.

1. **Privacy-Preserving Authentication.** The vehicle users/ RSUs should be able to verify message does come from another legitimate user in the VANET. At the same time, true identities of signer should not be known by anyone in the VANET except the TA.
2. **Message Integrity.** Messages that have been modified should also be detected.
3. **Unlinkability.** Malicious vehicles and curious RSUs cannot link two different signatures from a vehicle.
4. **Mandatory Revocability.** The TA can revoke all users' anonymous identities at any time he/she wants.

$$\left.\begin{array}{l}\text{Privacy-Preserving Authentication}\\ \text{Mandatory Revocability}\end{array}\right\}\text{Conditional Privacy-Preserving Authentication(CPPA)}$$

1. Motivation
2. **Related Work and Our Result**
3. Preliminaries
4. Proposed Scheme
5. Evaluations and Comparisons

Related Work

The most common ways are using pseudonyms, ID-Based Cryptography, and special digital signatures such as group signature, ring signature.

- Pseudonyms-Based: Original from Raya and Hubaux[RH07], and based on Public Key Infrastructure(PKI). Every OBU on vehicle firstly sends related information to the TA in their real-name, then the TA registers pseudonyms for them after verifying.
  Shortcomings: enormous storage overhead in maintaining and revoking(the CRL, Certificate Revocation List, increase dramatically)
  Countermeasure: Lu et al.[Lu+08], the first protocol that supports a vehicle obtaining an Interim Pseudonymous Certificate(IPC) when it passes through a RSU. A vehicle holds the IPC only for a short time, and need not store a copy of CRL. However, frequent interactions between OBUs and RSUs will affect efficiency.
- ID-Based Signature: [Zha+08; Shi12] built ID-Based CPPA protocols from bilinear pairing, which is a time-consuming operation. He et al.[He+15] removes bilinear pairing by using CRHF and Elliptic Curve Cryptography(ECC). Li et al.[Li+22] extended it to Lattice.

Related Work

- Group Signature: Shao et al.[Sha+15] used bilinear pairing to construct a group signature scheme, and adopted it to achieve threshold anonymous authentication for VANETs scenario, supporting efficient Mandatory Revocability.
  Shortcomings: An important problem for group signature in reality applications is how to determine the group manager, it is difficult to find a trusted party and persuade others to believe.
- Ring Signature: Previous work[Mun+20a; JX21] by conventional Ring Signature only provide Unconditional Privacy-Preserving Authentication. In order to realize CPPA:
  - [Mun+20b] used ring signature joint operation of pseudonyms from the TA, making TA can disclose the vehicles' identities from pseudonyms issued by him/her, achieving CPPA.
  - [Han+20; BS20] used Traceable Ring Signature.
- Our Work: Revocable Ring Signature.

Ring Signature

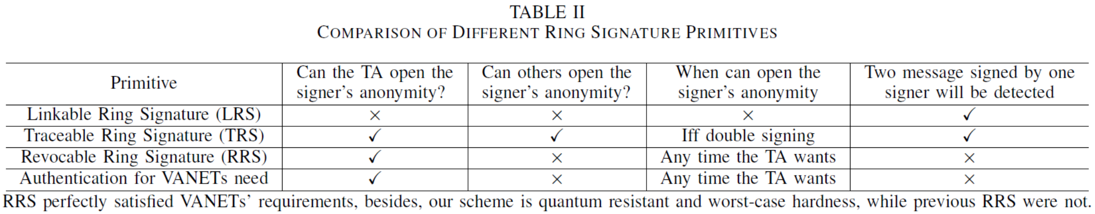


TABLE II
COMPARISON OF DIFFERENT RING SIGNATURE PRIMITIVES

Primitive	Can the TA open the signer's anonymity?	Can others open the signer's anonymity?	When can open the signer's anonymity	Two message signed by one signer will be detected
Linkable Ring Signature (LRS)	×	×	×	✓
Traceable Ring Signature (TRS)	✓	✓	Iff double signing	✓
Revocable Ring Signature (RRS)	✓	×	Any time the TA wants	×
Authentication for VANETs need	✓	×	Any time the TA wants	×

RRS perfectly satisfied VANETs' requirements, besides, our scheme is quantum resistant and worst-case hardness, while previous RRS were not.

Revocable Ring Signature support predefined Trusted Authorities(TA) to open the anonymity of a signer from signatures at any time they want, also called Mandatory Revocability.

Revocable/Accountable Ring Signature schemes

Revocable Ring Signature(RRS) schemes:

- [Liu+07] discrete logarithm and pairing.
- [Zha+19] discrete logarithm, Decisional Diffie-Hellman(DDH) Assumption.

Accountable Ring Signature(ARS) schemes:

- [Boo+15] DDH Assumption.
- [Lai+16] q-SDH Assumption.
- [KP17] $i\mathcal{O}$, absence of post-quantum constructions.
- [Chu+21] Isogeny.

We present the first Lattice-Based Revocable Ring Signature scheme in this paper.

1. Motivation
2. Related Work and Our Result
3. **Preliminaries**
4. Proposed Scheme
5. Evaluations and Comparisons

Hard Problems

Definition ($\mathrm{MSIS}_{q,h,v,\gamma}$ Problem, [Duc+18])

Given a random matrix $\mathrm{A} \leftarrow R_q^{h\times v}$*, the advantage for the (Hermite normal form)* $\mathrm{MSIS}_{q,h,v,\gamma}$ *Problem for an algorithm* $\mathcal{A}$ *is*

$$\Pr\left[0 < \|\mathrm{y}\|_\infty \leq \gamma \wedge [\mathrm{A}\|\mathrm{I}] \cdot \mathrm{y} = 0 \middle| \mathrm{A} \leftarrow R_q^{h\times v}; \mathrm{y} \leftarrow \mathcal{A}(\mathrm{A})\right].$$

Definition ($\mathrm{D}-\mathrm{MLWE}_{q,h,v,\chi}$ Problem, [Duc+18])

Given a random matrix $\mathrm{A} \leftarrow R_q^{h\times v}$*, and a probability distribution* χ *over* R_q*, the advantage for the decisional* $\mathrm{D}-\mathrm{MLWE}_{q,h,v,\chi}$ *Problem for an algorithm* $\mathcal{A}$ *is*

$$\Big|\Pr[\mathcal{A}(\mathrm{A}, \mathrm{A}\mathrm{s}+\mathrm{e}) \rightarrow 1] - \Pr[\mathcal{A}(\mathrm{A}, \mathrm{v}) \rightarrow 1]\Big|.$$

where $\mathrm{A} \leftarrow R_q^{h\times v}, \mathrm{s} \leftarrow \chi^v, \mathrm{e} \leftarrow \chi^h$ *and* $\mathrm{v} \leftarrow R_q^h$*.*
Namely, distinguish distributions $(\mathrm{A}, \mathrm{A}\mathrm{s}+\mathrm{e})$ *and* (A, v)*.*

Correctness and Security of RRS

Definition (Correctness)

A Revocable Ring Signature scheme satisfied Verification Correctness and Revocability Correctness as follows:

- *Verification Correctness: An honest signer executes the* Sign *algorithm to generate a message-signature pair, and it should be valid with overwhelming probability.*
- *Revocability Correctness: An honest signer executes the* Sign *algorithm to generate a message-signature pair, and it should be able to be revoked by the TA with overwhelming probability.*

Definition (Anonymity)

Malicious user tries to guess Actual Signer's identity, would not have non-negligible probability greater than randomly guessing.

Correctness and Security of RRS

Definition (Unforgeability)

Malicious user without the secret key cannot generate corresponding signatures. In security models with the strongest adversary ability, the adversary is able to obtain the signature on any message(adaptive Chosen Message Attack, access to $\mathcal{O}_S$) and public key(adaptive Chosen Public Key Attack, access to $\mathcal{O}_K$), but it is still hard for he/she to forge a new valid message-signature pair.

Definition (Revocability)

If one user generates a signature, then its identity must be able to be revoked by the TA with overwhelming probability. The adversary is modeling as a malicious user who tries to hide its identity from being extracted from its signature by the TA, even he/she can use a secret key of a extra ring member in aid of avoiding being revoked, but still fails.

1. Motivation
2. Related Work and Our Result
3. Preliminaries
4. **Proposed Scheme**
5. Evaluations and Comparisons

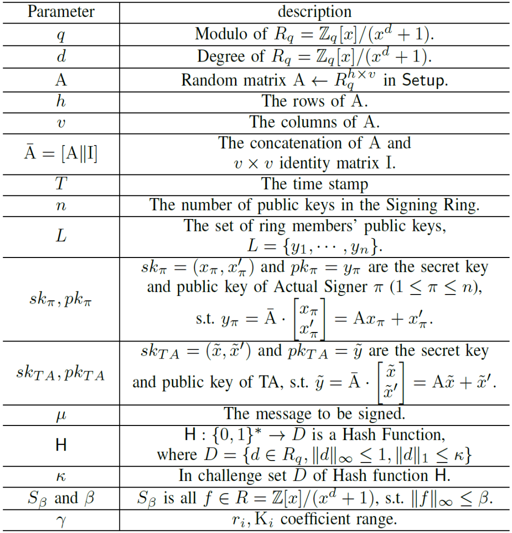
Proposed Scheme-Setup and KeyGen

Setup: TA executes the Setup Algorithm, inputs security parameter 1^λ, and samples a random matrix $\mathrm{A} \leftarrow R_q^{h\times v}$, outputs it as public parameters *param*, we denote $\bar{\mathrm{A}} = [\mathrm{A}\|\mathrm{I}]$.

KeyGen: Same as Dilithium[Duc+18], vehicle user *i* uniform randomly chooses $(x_i, x_i') \leftarrow S_\beta^v \times S_\beta^h$ as his/her secret key and stores in its OBU, the corresponding public key is $y_i = \bar{\mathrm{A}}x_i + x_i'$. The secret key $(\tilde{x}, \tilde{x}')$ and public key $\tilde{y}$ for the TA are defined similar, such that $\tilde{y} = \mathrm{A}\tilde{x} + \tilde{x}'$.

Remark: It is worth noting that processes of Setup and KeyGen can be done entirely offline. The secret key should be kept by every signer itself rather than transmit, and the public key need to be certified by the TA.

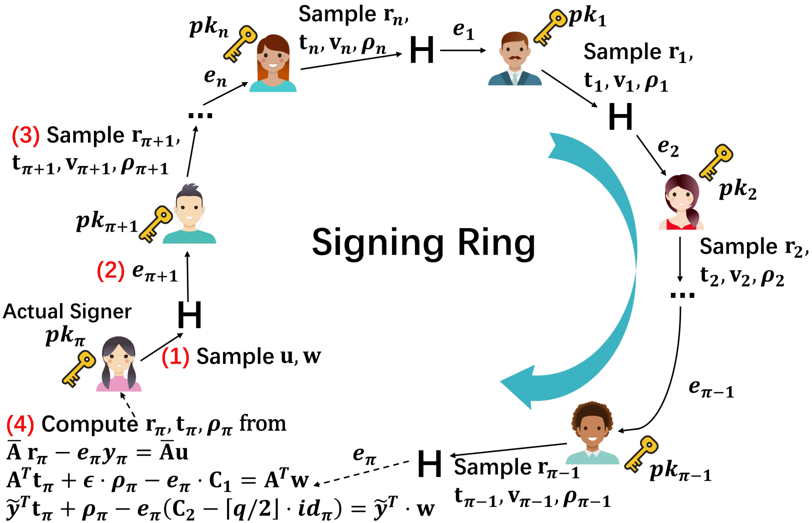
Proposed Scheme-Sign



Parameter	description
q	Modulo of $R_q = \mathbb{Z}_q[x]/(x^d+1)$.
d	Degree of $R_q = \mathbb{Z}_q[x]/(x^d+1)$.
A	Random matrix $\mathrm{A} \leftarrow R_q^{h\times v}$ in Setup.
h	The rows of A.
v	The columns of A.
$\bar{\mathrm{A}} = [\mathrm{A}\|\mathrm{I}]$	The concatenation of A and $v \times v$ identity matrix I.
T	The time stamp
n	The number of public keys in the Signing Ring.
L	The set of ring members' public keys, $L = \{y_1, \cdots, y_n\}$.
sk_π, pk_π	$sk_\pi = (x_\pi, x'_\pi)$ and $pk_\pi = y_\pi$ are the secret key and public key of Actual Signer π $(1 \leq \pi \leq n)$, s.t. $y_\pi = \bar{\mathrm{A}} \cdot \begin{bmatrix} x_\pi \\ x'_\pi \end{bmatrix} = \mathrm{A}x_\pi + x'_\pi$.
sk_{TA}, pk_{TA}	$sk_{TA} = (\tilde{x}, \tilde{x}')$ and $pk_{TA} = \tilde{y}$ are the secret key and public key of TA, s.t. $\tilde{y} = \bar{\mathrm{A}} \cdot \begin{bmatrix} \tilde{x} \\ \tilde{x}' \end{bmatrix} = \mathrm{A}\tilde{x} + \tilde{x}'$.
μ	The message to be signed.
H	$\mathsf{H} : \{0,1\}^* \to D$ is a Hash Function, where $D = \{d \in R_q, \|d\|_\infty \leq 1, \|d\|_1 \leq \kappa\}$
κ	In challenge set D of Hash function H.
S_β and β	S_β is all $f \in R = \mathbb{Z}[x]/(x^d+1)$, s.t. $\|f\|_\infty \leq \beta$.
γ	r_i, K_i coefficient range.

User $\pi(\pi \in \{1, 2, \cdots, n\})$ who desires to generate a ring signature on the ring L, performs the Signature Generation Algorithm with inputs $(T, n, L, sk_\pi, pk_{TA}, \mu)$ in the left Table.

Proposed Scheme-Sign



Signing Ring

pk_n

e_n

Sample $\mathbf{r}_n$, $\mathbf{t}_n, \mathbf{v}_n, \rho_n$

H

e_1

pk_1

Sample $\mathbf{r}_1$, $\mathbf{t}_1, \mathbf{v}_1, \rho_1$

H

e_2

pk_2

Sample $\mathbf{r}_2$, $\mathbf{t}_2, \mathbf{v}_2, \rho_2$

...

$e_{\pi-1}$

$pk_{\pi-1}$

Sample $\mathbf{r}_{\pi-1}$ $\mathbf{t}_{\pi-1}, \mathbf{v}_{\pi-1}, \rho_{\pi-1}$

H

e_π

Actual Signer pk_π

(1) Sample $\mathbf{u}, \mathbf{w}$

H

(2) $e_{\pi+1}$

$pk_{\pi+1}$

(3) Sample $\mathbf{r}_{\pi+1}$, $\mathbf{t}_{\pi+1}, \mathbf{v}_{\pi+1}, \rho_{\pi+1}$

...

(4) Compute $\mathbf{r}_\pi, \mathbf{t}_\pi, \rho_\pi$ from

$$\bar{\mathbf{A}}\,\mathbf{r}_\pi - e_\pi y_\pi = \bar{\mathbf{A}}\mathbf{u}$$
$$\mathbf{A}^T\mathbf{t}_\pi + \epsilon \cdot \rho_\pi - e_\pi \cdot \mathbf{C}_1 = \mathbf{A}^T\mathbf{w}$$
$$\tilde{y}^T\mathbf{t}_\pi + \rho_\pi - e_\pi(\mathbf{C}_2 - \lceil q/2 \rfloor \cdot id_\pi) = \tilde{y}^T \cdot \mathbf{w}$$

Proposed Scheme-Sign

1. Samples small elements $\mathbf{s} \leftarrow S_\beta^h$ and $(\epsilon_1, \epsilon_2) \leftarrow S_\beta^v \times S_\beta$, computes $\epsilon = \epsilon_1 \cdot \epsilon_2^{-1}$ (ϵ_2 is invertible with high probability, if not, resample) and its Revocable Tag:

$$\mathbf{C}_\pi = (\mathbf{C}_1, \mathbf{C}_2) = \left(\mathbf{A}^T\mathbf{s} + \epsilon_1, \tilde{\mathbf{y}}^T \cdot \mathbf{s} + \epsilon_2 + \lceil q/2 \rfloor \cdot id_\pi\right) \tag{1}$$

2. Computes the user $\pi + 1$ in the Signing Ring:
   2.1 Samples $\mathbf{u} \leftarrow S_{\gamma-1}^{v+h}$ and $\mathbf{w} \leftarrow S_{\gamma-1}^h$.
   2.2 Set $e_{\pi+1} = \mathrm{H}(T, L, \mu, \bar{\mathbf{A}}\mathbf{u}, \mathbf{A}^T\mathbf{w}, \tilde{\mathbf{y}}^T \cdot \mathbf{w})$.
3. Computes other users in the Signing Ring:
   3.1 For $i = \pi + 1, \cdots, n, 1, \cdots, \pi - 1$, samples $\mathbf{r}_i \leftarrow S_{\gamma-1}^{v+h}, \mathbf{t}_i \leftarrow S_{\gamma-1}^h$, $\mathbf{v}_i \leftarrow S_\beta$, computes $\rho_i = e_i \cdot \mathbf{v}_i$.
   3.2 Sets $e_{i+1} = \mathrm{H}(T, L, \mu, \alpha_i, \Omega_i, \delta_i)$, where

$$\alpha_i = \bar{\mathbf{A}}\mathbf{r}_i - e_i \cdot \mathbf{y}_i$$
$$\Omega_i = \mathbf{A}^T\mathbf{t}_i + \epsilon \cdot \rho_i - e_i \cdot \mathbf{C}_1$$
$$\delta_i = \tilde{\mathbf{y}}^T \cdot \mathbf{t}_i + \rho_i - e_i \cdot (\mathbf{C}_2 - \lceil q/2 \rfloor \cdot id_i)$$

Proposed Scheme-Sign

4. Computes $\mathbf{r}_\pi = \mathbf{u} + e_\pi \cdot \begin{bmatrix} \mathbf{x}_\pi \\ \mathbf{x}'_\pi \end{bmatrix}, \mathbf{t}_\pi = \mathbf{w} + e_\pi \cdot \mathbf{s}, \rho_\pi = e_\pi \cdot \epsilon_2$.
5. If $\|\mathbf{r}_\pi\|_\infty \geq \gamma - \kappa \cdot \beta$ or $\|\mathbf{t}_\pi\|_\infty \geq \gamma - \kappa \cdot \beta$, aborts and restarts at $i = \pi - 1$ in step 3) A).
6. The signature is

$$z = (T, e_1, \mathbf{r}_1, \mathbf{t}_1, \rho_1, \cdots, \mathbf{r}_n, \mathbf{t}_n, \rho_n, \epsilon, \mathbf{C}_\pi).$$

Rejection Sampling!!!

Proposed Scheme-Verify

When other OBUs/RSUs receiving the size n, the public keys $L = \{pk_1, \cdots, pk_n\}$, and a message μ with the corresponding signature $z = (T, e_1, \mathbf{r}_1, \mathbf{t}_1, \rho_1, \cdots, \mathbf{r}_n, \mathbf{t}_n, \rho_n, \epsilon, \mathbf{C}_\pi)$, it can check the validity of the signature z as follows.

1. Checks if $\|\mathbf{r}_i\|_\infty < \gamma - \kappa \cdot \beta$ and $\|\mathbf{t}_i\|_\infty < \gamma - \kappa \cdot \beta$, else abort.
2. Parses the Revocable Tag $\mathbf{C}_\pi = (\mathbf{C}_1, \mathbf{C}_2)$ from z.
3. For $i = 1, \cdots, n-1$, computes

$$e_{i+1} = \mathrm{H}(T, L, \mu, \bar{\mathbf{A}}\mathbf{r}_i - e_i \cdot \mathbf{y}_i, \mathbf{A}^T\mathbf{t}_i + \epsilon \cdot \rho_i - e_i \cdot \mathbf{C}_1, \\ \tilde{\mathbf{y}}^T \cdot \mathbf{t}_i + \rho_i - e_i \cdot (\mathbf{C}_2 - \lceil q/2 \rfloor \cdot id_i)).$$

4. After obtaining e_n, checks

$$e_1 = \mathrm{H}(T, L, \mu, \bar{\mathbf{A}}\mathbf{r}_n - e_n \cdot \mathbf{y}_n, \mathbf{A}^T\mathbf{t}_n + \epsilon \cdot \rho_n - e_n \cdot \mathbf{C}_1, \\ \tilde{\mathbf{y}}^T \cdot \mathbf{t}_n + \rho_n - e_n \cdot (\mathbf{C}_2 - \lceil q/2 \rfloor \cdot id_n)).$$

If verified, output *accept*, else output *reject*.

Proposed Scheme-Revocability

On input the public key set L with member size n and a signature z, the TA who owned $sk_{TA} = (\tilde{\mathbf{x}}, \tilde{\mathbf{x}}')$ can revoke the anonymous identity of Actual Signer as follows:

1. Check whether z is valid. If so, continue, otherwise abort;
2. Parse $(\mathbf{C}_1, \mathbf{C}_2)$ from the Revocable Tag $\mathbf{C}_\pi$ in z;
3. Compute $\mathbf{C}_2 - \tilde{\mathbf{x}}^T \cdot \mathbf{C}_1$, and the TA can recover id_π, corresponding user in group L is Actual Signer.

Revocation Correctness. If a signer executes the protocol and generates signature z honestly, since the infinity norm $\|(\mathbf{x}')^T \cdot \mathbf{s} + \epsilon_2 - \mathbf{x}^T \cdot \epsilon_1\|_\infty \leq \lceil q/4 \rfloor$. According to Lattice-Based PKE, the TA owned $\tilde{\mathbf{x}}$ could compute

$$\mathbf{C}_2 - \tilde{\mathbf{x}}^T \cdot \mathbf{C}_1 = \left[(\mathbf{x}')^T \cdot \mathbf{s} + \epsilon_2 - \mathbf{x}^T \cdot \epsilon_1\right] + \lceil q/2 \rfloor \cdot id_\pi \bmod q.$$

The bits of id_π can be recovered by rounding each coefficient of $\mathbf{C}_2 - \tilde{\mathbf{x}}^T \cdot \mathbf{C}_1$ back to either 0 or $q/2$, whichever is closest modulo q, then the TA can trace user π's real identity from id_π.

1. Motivation
2. Related Work and Our Result
3. Preliminaries
4. Proposed Scheme
5. **Evaluations and Comparisons**

Satisfied Requirements Comparison

Table: Comparison of Satisfied Requirements

Satisfied Requirements	This work	[Mun+20a]	[JX21]	[Mun+20b]	[Han+20]	[BS20]	[Zha+19]
Privacy-Preserving Authentication	✓	✓	✓	✓	✓	✓	✓
Message Integrity	✓	✓	✓	✓	✓	✓	✓
Unlinkability	✓	✓	✓	✓	×	×	✓
Traceability(for the TA)	✓	×	×	✓	✓	✓	✓
Mandatory Revocability	✓	×	×	✓(combines with pseudonym)	×	×	✓
Quantum-Resistance	✓	✓	✓	✓	✓	✓	×

Parameter Settings and Sizes

Table: Parameter Settings and Sizes

Parameter Set	I	II
Security Level	NIST Level 1- (90 bits)	NIST Level 2 (128 bits)
q (modulo of polynomial ring)	8380417	8380417
d (degree of polynomial ring)	256	256
h (the rows of $\mathbf{A}$)	3	4
v (the columns of $\mathbf{A}$)	3	4
κ (in challenge set D of H)	30	39
β (in secret key range S_β)	3	2
γ (r_i, t_i coefficient range)	2^{17}	2^{17}
Public Key Size (each user)	2.19 KB	2.90 KB
Secret Key Size (each user)	0.56 KB	0.75 KB
Signature Size ($n = 1$)	10.3 KB	13.4 KB
Signature Size ($n = 2$)	15.6 KB	20.4 KB
Signature Size ($n = 4$)	26.2 KB	34.4 KB
Signature Size ($n = 8$)	47.5 KB	62.4 KB

Runtime

We combine the official implementations of CRYSTALS-Dilithium with the renowned number theory library Python3-cypari2.

Table: Total Execution Time Comparison (Microseconds/μs)

Scheme		SystemSetup and KeyGen	SigGen	SigVerify	SigRevoke
Our	I	158.4	$1056.6n + 4024.5$	$955.1n$	54.0
	II	250.1	$2066.2n + 9424.9$	$1938.9n$	74.2
[Zha+19]		531.8	$5381.7n + 26.3$	$5380.3n$	534.2
[Li+22]		28419000.0	3867770.1	60120	558.1
[DM20]		1721700.2	1786880.2	49784	558.1

Platform: 2.3 GHz Quad-Core Intel Core i5, 16 GB RAM, macOS BigSur for 64 bit operation system.

Runtime

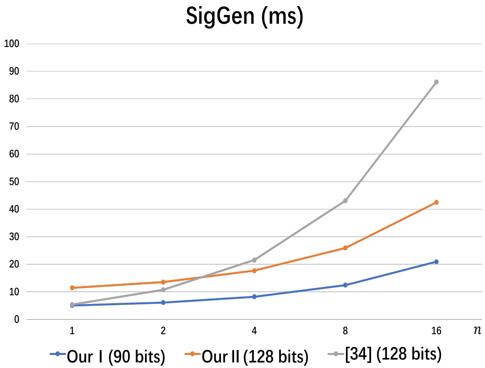


Figure: Signature Generation

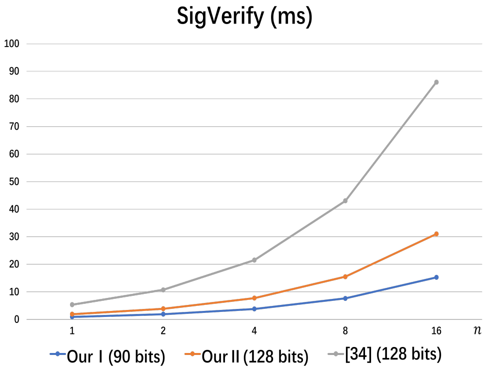


Figure: Signature Verification

The End, Thanks