Yanhua ZHANG, Ximeng LIU, Yupu HU, Yong GAN, Huiwen JIA, 2022. Verifier-local revocation group signatures with backward unlinkability from lattices. *Frontiers of Information Technology & Electronic Engineering,* 23(6):876-892. https://doi.org/10.1631/FITEE.2000507

Verifier-local revocation group signatures with backward unlinkability from lattices

Key words: Group signature; Lattice-based cryptography; Verifier-local revocation; Backward unlikability; Short integer solution

Corresponding authors: Yanhua ZHANG; Huiwen JIA
E-mail: yhzhang@email.zzuli.edu.cn; hwjia@gzhu.edu.cn
ORCID: https://orcid.org/0000-0001-7946-5262; https://orcid.org/0000-0002-9289-5918

Motivation

- For group signature (GS) with membership revocation, the verifier-local revocation (VLR) mechanism is a more flexible choice compared with re-initialization of the whole system or a dynamic accumulator, when considering a large group.
- Backward unlinkability (BU), a significant security for GS supporting membership revocation, ensures that the previously issued signatures will remain anonymous and unlinkable even after the corresponding signer is revoked. BU security is essential to ensure privacy for honest members who voluntarily leave the group or inadvertently lose the signing secret-keys.
- None of the existing lattice-based VLR-GS schemes provide BU security. All signatures issued by the revoked member will become linkable, which inevitably undermines privacy.

Main idea

- Based on two well-known worst-case hardness assumptions, the short integer solution (SIS) problem and the learning with error (LWE) problem, the first lattice-based VLR-GS scheme with BU security (VLR-GS-BU) is proposed.
- Each group member has many revocation tokens (RTs) over the lifetime, and the signer can adopt different RTs in the signature algorithm. Once a group member is revoked, the manager can add his/her unused RTs to the revocation list (RL), and the used ones remain anonymous.
- The generation of RTs satisfies one-way security, which means leaking the revoked member's RTs at period j, no one including an adversary can compute any RT before period j.

Method

1. To realize two essential conditions—many RTs generated over TPs and one-way security, for RTs with BU security, the encoding with full-rank differences (FRD) function $\mathcal{H}_1$ is adopted. Further, to avoid some deadly attacks to the underlying SIS problem and BU security, we sample two random matrices $\boldsymbol{B}_0, \boldsymbol{B}_1 \in \mathbb{Z}_q^{n\times m}$; thus, for time period j, the revocation token RT_j of the member id is

$$\boldsymbol{grt}_{i,j} = \left(\boldsymbol{B}_0 + \mathcal{H}_1\left(\mathrm{TP}_j\right)\boldsymbol{B}_1\right)\boldsymbol{e}_{i,0} \bmod q$$

where $\boldsymbol{e}_{i,0}$ is a short Gaussian vector and is the first part of the signing secret-key $\boldsymbol{e}_i = \left(\boldsymbol{e}_{i,0}, \boldsymbol{e}_{i,1}\right) \in \mathbb{Z}^{(2m)}$ satisfying

$$\boldsymbol{A}_{\mathrm{id}}\boldsymbol{e}_i = \boldsymbol{u} \bmod q \qquad (1)$$

where $\boldsymbol{A}_{\mathrm{id}} = (\boldsymbol{A} | \boldsymbol{A}_0 + i\boldsymbol{A}_1) \in \mathbb{Z}_q^{n\times(2m)}$.

Method

2. For the revocation mechanism, due to a flaw in Langlois et al. (2014) that an inequality test method was adopted to check whether the signer's RT belongs to a given RL, a new and corrected technique which realizes revocation by binding the signer's RT to an LWE function (in our design, the concept of TP is adopted, and for id with an index i at period j, $\mathrm{RT}_j = \boldsymbol{grt}_{i,j}$) was proposed

$$\boldsymbol{b}_j = \boldsymbol{B}^{\mathrm{T}} \boldsymbol{grt}_{i,j} + \boldsymbol{e}_0$$

(2)
$$= \boldsymbol{B}^{\mathrm{T}} \underbrace{\left(\boldsymbol{B}_0 + \mathcal{H}_1\left(\mathrm{TP}_j\right)\boldsymbol{B}_1\right)}_{\boldsymbol{B}'_j} \boldsymbol{e}_{i,0} + \boldsymbol{e}_0 \bmod q$$

where $\boldsymbol{B}$ is from a random oracle as in Ling et al. (2018) and $\boldsymbol{e}_0 \in \mathbb{Z}^m$ is sampled from an LWE error χ^m.

Method

3. Putting all innovative ideas, design approaches, and the Stern-type argument system introduced by Ling et al. (2013) together, design a Stern-type interactive ZKP protocol to prove Eqs. (1) and (2).

- Public inputs: $\boldsymbol{A}' = [\boldsymbol{A}|\, \boldsymbol{A}_0|\, \boldsymbol{g}_\ell \otimes \boldsymbol{A}_1] \in \mathbb{Z}_q^{n\times(\ell+2)m}$, $\boldsymbol{B}, \boldsymbol{B}_0, \boldsymbol{B}_1 \in \mathbb{Z}_q^{n\times m}$, $\boldsymbol{u} \in \mathbb{Z}_q^n, \boldsymbol{b}_j \in \mathbb{Z}_q^m$, and current time period $j \in \{1,2,\cdots,t\}$.
- Signer's witness: $\boldsymbol{e}_i' = \left(\boldsymbol{e}_{i,0}', \boldsymbol{e}_{i,1}', \mathrm{Bin}(i) \otimes \boldsymbol{e}_{i,1}'\right) \in \mathbf{Sec}_\beta(\mathrm{id})$ for a secret index $i \in \{0,1,\cdots,N-1\}$, and an LWE vector $\boldsymbol{e}_0 \in \chi^m$.
- Signer's goal: to convince any verifier in zero-knowledge that:

  ✓ $\boldsymbol{A}'\boldsymbol{e}_i' = \boldsymbol{u} \bmod q$, where $\boldsymbol{e}_i' \in \mathbf{Sec}_\beta(\mathrm{id}), \mathrm{id} = \mathrm{Bin}(i)$;

  ✓ $\boldsymbol{b}_j = \left(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{B}_j'\right)\boldsymbol{e}_{i,0}' + \boldsymbol{e}_0 \bmod q$, $\left\|\boldsymbol{e}_{i,0}'\right\|_\infty, \|\boldsymbol{e}_0\|_\infty \le \beta$.

Major results

Detailed comparisons

Table 3 Comparison of known lattice-based VLR-GS schemes ($N = 2^\ell$)

Scheme	|Gpk|	|**gsk**|	$\|\sigma\|$	Functionality	Free of encryption	BU-security
Ling et al. (2013)'s	$\ell\tilde{\mathcal{O}}(n^2)$	$\ell\tilde{\mathcal{O}}(n)$	$\ell\tilde{\mathcal{O}}(n)$	VLR	Yes	No
Zhang et al. (2016)'s	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	$\tilde{\mathcal{O}}(n+\ell)$	VLR	No	No
Gao et al. (2017)'s	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	$\tilde{\mathcal{O}}(n+\ell)$	VLR	No	No
Ling et al. (2018)'s	$\ell\tilde{\mathcal{O}}(n^2)$	$\ell\tilde{\mathcal{O}}(n)$	$\ell\tilde{\mathcal{O}}(n)$	VLR	Yes	No
Perera and Koshiba (2018a)'s	$\ell\tilde{\mathcal{O}}(n^2)$	$\ell\tilde{\mathcal{O}}(n)$	$\ell\tilde{\mathcal{O}}(n)$	VLR	Yes	No
Perera and Koshiba (2018b)'s	$\ell\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	$\ell\tilde{\mathcal{O}}(n)$	Fully dynamic	No	No
Perera and Koshiba (2018c)'s	$\ell\tilde{\mathcal{O}}(n^2)$	$\ell\tilde{\mathcal{O}}(n)$	$\ell\tilde{\mathcal{O}}(n)$	Fully dynamic	No	No
Zhang et al. (2019a)'s	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	$\ell\tilde{\mathcal{O}}(n)$	VLR	Yes	No
Zhang et al. (2019b)'s	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	$\ell\tilde{\mathcal{O}}(n)$	VLR	No	No
Ours	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	$\ell\tilde{\mathcal{O}}(n)$	VLR	Yes	Yes

|Gpk|: size of the group public-key; |**gsk**|: size of a member's signing secret-key; $|\sigma|$: size of the signature; VLR: verifier-local revocation

Major results

Detailed comparisons

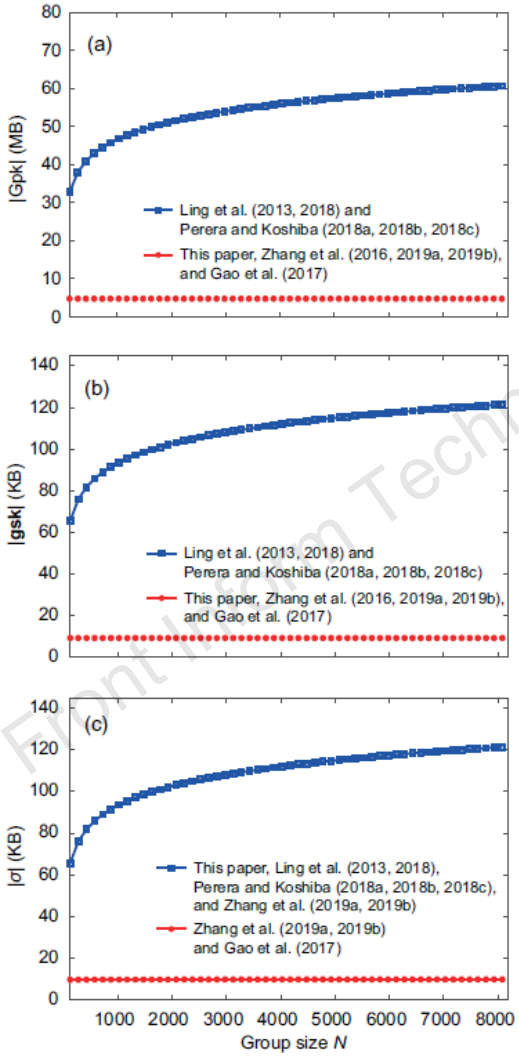

Fig. 1 Comparison of the 10 schemes in terms of |Gpk| (a), |gsk| (b), and $|\sigma|$ (c)

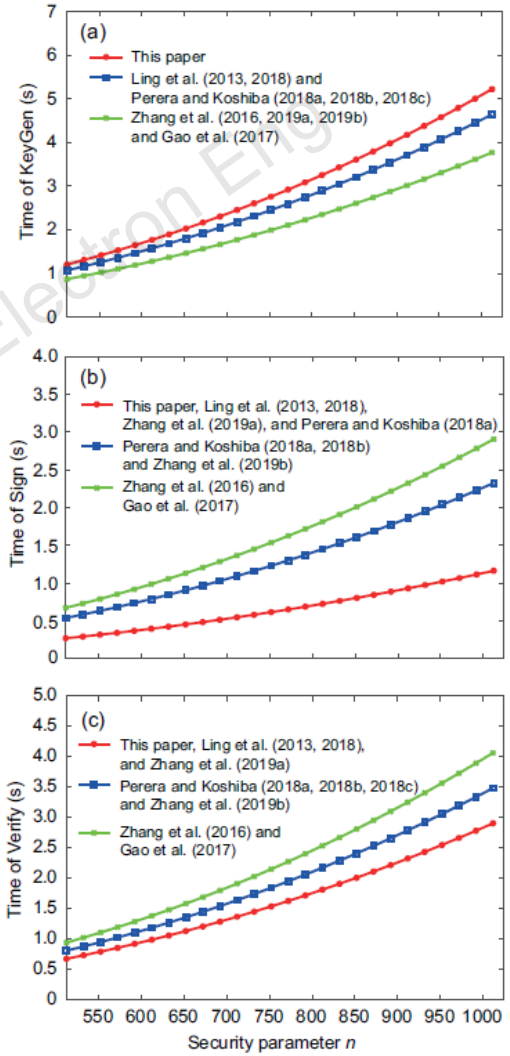

Fig. 2 Comparison of the 10 schemes in terms of KeyGen cost (a), Sign cost (b), and Verify cost (c)

Conclusions

- We proposed the first lattice-based VLR-GS scheme with BU security, and thus resolved a prominent open problem.
- By adopting an injective encoding function with FRD, a compact identity-encoding technique, and the corresponding Stern-type statistical ZKP protocol creatively, the proposed scheme enjoys an $O(\log N)$ factor saving for the bit-sizes of GPK and member's signing secret-key, and is free of any public-key encryption.
- With BU security, the proposed scheme is more suitable for some large groups with better security.