Hindawi
Security and Communication Networks
Volume 2021, Article ID 9988939, 10 pages
https://doi.org/10.1155/2021/9988939

Research Article

An Improved Group Signature Scheme with VLR over Lattices

Yanhua Zhang,[1] **Ximeng Liu**,[2] **Yupu Hu**,[3] **Huiwen Jia**,[4] **and Qikun Zhang**[5]

[1]*Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China*
[2]*College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China*
[3]*School of Telecommunications Engineering, Xidian University, Xi'an 710071, China*
[4]*School of Information Science, Guangzhou University, Guangzhou 510006, China*
[5]*College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450001, China*

Correspondence should be addressed to Yanhua Zhang; yhzhang@email.zzuli.edu.cn

Received 13 March 2021; Accepted 17 September 2021; Published 21 October 2021

Academic Editor: Helena Rifà-Pous

For group signatures (GS) supporting membership revocation, verifier-local revocation (VLR) mechanism is the most flexible choice. As a post-quantum secure cryptographic counterpart of classical schemes, the first dynamic GS-VLR scheme over lattices was put forward by Langlois et al. at PKC 2014; furthermore, a corrected version was shown at TCS 2018. However, both designs are within Bonsai trees and featuring bit-sizes of group public-key and member secret signing key proportional to $\log N$ where N is the group size; therefore, both schemes are not suitable for a large group. In this paper, we provide an improved dynamic GS-VLR over lattices, which is efficient by eliminating a $\mathcal{O}(\log N)$ factor for both sizes. To realize the goal, we adopt a more efficient and compact identity-encoding technique. At the heart of our new construction is a new Stern-type statistical zero-knowledge argument of knowledge protocol which may be of some independent cryptographic interest.

1. Introduction

Group signatures (GS), first formalized by Chaum and Heyst [1], allow the members to issue signatures on behalf of the group without leaking their identity. A tracing authority could link any valid message-signature pair to the real signer. The *anonymity* and *traceability* are of especial importance for GS, and to construct GS schemes with different security, efficiency, and hardness, they have been brought (see, e.g., [2–9]) over the last quarter-century.

Up to now, there are five schemes supporting dynamic GS over lattices. At PKC 2014, Langiois et al. [10] introduced the first GS over lattices to support membership revocation with verifier-local revocation (VLR) mechanism. Because of an improper design, there is a flaw of [10], this mistake is completely fixed, and a secure scheme [11] was provided. As an orthogonal problem of membership revocation, enrollment is also noteworthy, and this problem was first resolved by Libert et al. [12]. Later, Ling et al. [13] introduced the first fully dynamic GS over lattices. Recently, Ling et al. [14] proposed the first constant-size and partially dynamic GS over lattices, and Sun and Liu [15] proposed the first lattice-based fully dynamic GS without NIZK.

Membership revocation is also noteworthy for GS, and the VLR mechanism is the most flexible choice in the mobile network that allows anonymous authentication. After the first GS-VLR over lattices was given by Langlois et al. [10], some new constructions are proposed [11, 16, 17]. However, all schemes are within Bonsai trees [18] and featuring bit-sizes of group public-key and member secret signing key proportional to $\log N$; therefore, these schemes are not suitable for certain large group, the only two exceptions [19, 20]. However, the constructions of [19, 20] are not free of public-key encryptions. Therefore, these unsatisfactory situations naturally lead a challenging topic on how to design a more efficient GS-VLR over lattices?

1.1. Our Construction and Techniques. In this work, we will reply positively to the above problem, and we introduced an improved GS-VLR scheme over lattices. Here, by "improved," we mean that our construction eliminates a $\mathcal{O}(\log N)$ factor for the sizes of group public-key and member secret signing key. Furthermore, the free of any public-key encryptions also brings reasonable selecting for cryptographic parameters and a clearer proof idea. A detailed comparison between the proposed scheme and previous GS-VLR over lattices is shown in Table 1.

Our scheme is proven secure under the shortest independent vectors problem (SIVP). We adopt an efficient identity-encoding technique [23]. The group is of $N = 2^\ell$ members, and the member is marked as $i\ d = (d_1, \ldots, d_\ell) \in \{0,1\}^\ell$, a binary representation of his index $i \in \{0, 1, \ldots, N-1\}$, i.e., $i\ d = \mathrm{Bin}(i) \in \{0,1\}^\ell$ where $\mathrm{Bin}(i)$ is i's binary decomposition. In this paper, n is a security parameter and the group public-key Gpk includes a uniform $u \in \mathbb{Z}_q^n$ and $A_0, A_1, A_2 \in \mathbb{Z}_q^{n\times m}$. For $i \in \{0, 1, \ldots, N-1\}$, not as that in [23] to generate a trapdoor basis matrix as member's secret-key, we sample a nonzero short vector $e_i = (e_{i,0}, e_{i,1}) \in \mathbb{Z}^{2m}$ which satisfies $A_i \cdot e_i = u \bmod q$ and $0 < \|e_i\|_\infty \leq \beta$, where $A_i = [A_0 | A_1 + iA_2] \in \mathbb{Z}_q^{n\times 2m}$ and the member i's revocation token is created by A_0 and $e_{i,0}$, i.e., $\mathrm{grt}_i = A_0 \cdot e_{i,0} \bmod q$.

The main challenge is how to prove these two core relations with a secure NIZK protocol: (a) $[A_0|A_1 + iA_2] \cdot e_i = u \bmod q$ and (b) $A_{1i} = A_0 \cdot e_{i,0} \bmod q$. For (b), we first sample a uniformly random $B \in \mathbb{Z}_q^{n\times m}$ (a matrix in an oracle), and a short random $e \in \mathbb{Z}^m$ (a vector in a learning with errors (LWE) distribution), and let $b = B^T \cdot \mathrm{grt}_i + e \bmod \mathrm{grt}$ as in [11]. For (a), because e_i is an affirmative answer to $(A_i = [A_0| A_1 + iA_2], u)$, an instance of the inhomogeneous short integer solution (ISIS), a simple method to prove i's validity is to perform a Stern-type statistical zero-knowledge argument of knowledge (ZKAoK) as in [25]. However, the detailed structure of A_i cannot be given to keep i's anonymity. How to realize a zero-knowledge proof without leaking A_i and e_i? First, A_i is transformed into A' which owns a new shape and is irrelevant to index i, i.e., $A' = [A_0|A_1|g_\ell \otimes A_2] \in \mathbb{Z}_q^{n\times(2\ell+2)m}$ where $g_\ell = (1, 2, 2^2, \ldots, 2^{\ell-1})$, and thus $i = g_\ell^T \cdot \mathrm{Bin}(i)$, and $\otimes$ is defined in Section 3. Correspondingly, the short vector $e_i = (e_{i,0}, e_{i,1})$ is transformed to $e_i' = (e_{i,0}, e_{i,1}, \mathrm{Bin}(i) \otimes e_{i,1}) \in \mathbb{Z}^{(\ell+2)m}$. Thus, to argue the above relation $A_i \cdot e_i = u \bmod q$, we instead show that $A' \cdot e_i' = u \bmod q$.

In a nutshell, by creatively improving an identity-encoding technique and designing a Stern-type zero-knowledge proof protocol, we introduce a more efficient GS-VLR over lattices. Our scheme satisfies the selfless-anonymity and enjoys the low bit-sizes. In addition, the innovative idea in our new construction must be of independent cryptographic interest.

1.2. Related Works. In the study by Regev [26] and Gentry et al. [27], GS over lattices have been extensively studied. The first GS over lattices were proposed by Gordon et al. [6], which are with linear sizes of group public-key and signature. Camenisch el al. [7] showed an improvement of public-key for [6]. In 2013, Laguillaumie et al. [24] introduced the first GS with logarithmic signature size over lattices. Later, Ling et al. [28] and Libert et al. [29] provided efficient GS constructions. Libert et al. [21] described the first GS over lattices not requiring trapdoors. Furthermore, GS over lattices with the message-dependent opening, forward-secure, and without noninteractive zero-knowledge (NIZK) were, respectively, shown by Libert et al. [21], Ling et al. [22], Canard et al. [30], and Katsumata and Yamada [31]. For the above GS schemes, all can only support static groups (i.e., no candidate member could join or leave once the group was established).

Table 1: Comparison of GS-VLR schemes over lattices ($N = 2^\ell = \mathrm{poly}(n)$).

Scheme	$\|Gpk\|$	$\|gsk\|$	$\|\sigma\|$	Free of encryptions
[20]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	Yes
[21]	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	$\widetilde{\mathcal{O}}(n+\ell)$	No
[22]	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	$\widetilde{\mathcal{O}}(n+\ell)$	No
[23]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	Yes
[24]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	No
Ours	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	Yes

1.3. Remark. This article is the improved version of [32], published in the proceedings of ISC 2019. Obviously, this article is a following work of [32] which is implied but not given clearly. And after [32], a series of rich contents of Zhang et al. [33–35] has developed our protocol to design a GS-VLR over lattices supporting explicit traceability and two new protocols for GS-VLR over lattices with improved anonymity.

1.4. Organization. We recall knowledge on GS-VLR and lattices in Section 2. Section 3 describes the main techniques utilized in our GS-VLR construction. Our scheme is finally designed and analysed in Section 4.

2. Preliminaries

2.1. Notations. Table 2 refers to the notations used in our work.

2.2. GS-VLR

2.2.1. Syntax of GS-VLR. There are three polynomial-time algorithms:

KeyGen$(1^n, N)$: taking the security parameter n and group size N as input, this PPT algorithm will output group public-key Gpk, members secret signing keys $\mathrm{Gsk} = (\mathrm{gsk}_0, \mathrm{gsk}_1, \ldots, \mathrm{gsk}_{N-1})$, and members revocation tokens $\mathrm{Grt} = (\mathrm{grt}_0, \mathrm{grt}_1, \ldots, \mathrm{grt}_{N-1})$.

Sign$(\mathrm{Gpk}, \mathrm{gsk}_i, m)$: taking Gpk and gsk_i of member $i\ d$ with index $i \in \{0, 1, \ldots, N-1\}$ and message $m \in \{0,1\}^*$ as input, this PPT algorithm will output a signature σ.

Verify$(\mathrm{Gpk}, RL, \sigma, m)$: taking Gpk a subset of tokens $RL \subseteq \mathrm{Grt}$, σ and $m \in \{0,1\}^*$ as input, this deterministic algorithm will output either 0 or 1. 1 means that σ is valid, and the real signer has not been revoked from the group.

Table 2: Notations of our work.

Notation	Definition
$\mathcal{S}_k$	All permutation of k elements
$\leftarrow_R$	Sampling uniformly at random
$\|\cdot\|$, or $\|\cdot\|_\infty$	Euclidean norm ℓ_2 or the infinity norm ℓ_∞
$\text{Parse}(e, k_1, k_2)$	$(e_{k_1}, e_{k_1+1}, \ldots, e_{k_2}) \in \mathbb{R}^{k_2-k_1+1}$, $e = (e_1, e_2, \ldots, e_n) \in \mathbb{R}^n$, $1 \le k_1 \le k_2 \le n$
$\log e$	Logarithm of e with base 2
PPT	Probabilistic polynomial-time

Correctness and security of GS-VLR: here, there are three main requirements: correctness, selfless-anonymity, and traceability.

Correctness: for all (Gpk, Gsk, Grt) outputted by KeyGen, any member $i \in \{0, 1, \ldots, N-1\}$, all $gsk_i \in$ Gsk, $RL \in$ Grt, and $m \in \{0,1\}^*$, we have the conditions:

$$\text{Verify}(\text{Gpk}, RL, \text{Sign}(\text{Gpk}, gsk_i, m), m) = 1 \Leftrightarrow \text{grt}_i \notin RL. \quad (1)$$

Selfless-anonymity: in the following game, the goal of adversary $\mathcal{A}$ is to determine which of the two adaptively chosen members id_0 with an index i_0 and id_1 with an index i_1 generated σ^*. $\mathcal{A}$ is not given either secret-key.

Setup: the challenger $\mathcal{C}$ runs KeyGen to obtain (Gpk, Gsk, Grt) and provides Gpk to $\mathcal{A}$.

Queries: $\mathcal{A}$ can adaptively make the following queries:

(i) Corruption: taking i as input, $\mathcal{C}$ returns gsk_i.
(ii) Signing: taking i and $m \in \{0,1\}^*$ as input, $\mathcal{C}$ returns $\sigma \longleftarrow \text{Sign}(\text{Gpk}, \text{gsk}_i, m)$.
(iii) Revocation: take i as input, $\mathcal{C}$ returns grt_i.

Challenge: $\mathcal{A}$ outputs a message $m \in \{0,1\}^*$ and two distinct members id_0 with an index i_0 and id_1 with an index i_1. $\mathcal{A}$ should not make corruption query or revocation query at either member. $\mathcal{C}$ chooses a bit $b \longleftarrow_R \{0,1\}$, computes $\sigma^* \longleftarrow \text{Sign}(\text{Gpk}, \text{gsk}_{i_b}, m^*)$ as a valid signature on m^*, and returns it to $\mathcal{A}$.

Restrictedqueries: once the challenge σ^* is obtained, $\mathcal{A}$ can make queries as before without the rights to do the corruption or revocation query for id_0 or id_1 or opening query for (m^*, σ^*).

Output: $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$ and wins if $b' = b$.

$\text{Adv}_{\mathcal{A}}^{\text{self-anon}} = |\Pr[b' = b] - 1/2|$ is defined as $\mathcal{A}$'s advantage in winning the above game. Thus, a GS-VLR satisfies the *selfless-anonymity* if $\text{Adv}_{\mathcal{A}}^{\text{self-anon}}$ is negligible.

Traceability: in the following game, the goal of $\mathcal{A}$ is to forge a signature that cannot be traced to any member in its collation.

Setup: $\mathcal{C}$ runs KeyGen to obtain (Gpk, Gsk, Grt) and provides (Gpk, Grt) to $\mathcal{A}$. Let initial corruption set Corr = ∅.

Queries: $\mathcal{A}$ can adaptively make the corruption and signing queries as in selfless-anonymity and $\mathcal{C}$ additionally adds $i\ d$ with its index i to Corr.

Forgery: $\mathcal{A}$ outputs a message $m^* \in \{0,1\}^*$, a set of members revocation tokens $RL^* \subseteq$ Grt and a signature σ^*. $\mathcal{A}$ wins if

(i) $\text{Verify}(\text{Gpk}, RL^*, \sigma^*, m^*) = 1$.
(ii) The implicit-tracing does not succeed or returns a member not included in Corr/RL^*.
(iii) σ^* is not obtained by a query on m^*.

$\text{Adv}_{\mathcal{A}}^{\text{trace}} = \text{SuccPT}_{\mathcal{A}}$ is defined as $\mathcal{A}$'s advantage in winning the above game. Thus, a GS-VLR scheme satisfies the *traceability* if $\text{Adv}_{\mathcal{A}}^{\text{trace}}$ is negligible.

2.3. Background on Lattices. Ajtai [36] first showed a strategy to generate statistically close to uniform $A \in \mathbb{Z}_q^{n\times m}$ together with low norm trapdoor basis of $\Lambda_q^{\perp}(A) = \{e \in \mathbb{Z}^m | A \cdot e = 0 \bmod q\}$. Subsequently, two new algorithms were given by [37, 38].

Lemma 1 (see [36–38]). *Define $n \ge 1$, $q \ge 2$, and $m = 2n\lceil \log q \rceil$. A PPT algorithm TrapGen(q, n, m) outputs A and R_A, such that $A \in \mathbb{Z}_q^{n\times m}$ is statistically close to uniform and R_A is a trapdoor for $\Lambda_q^{\perp}(A)$.*

Gentry et al. [27] first introduced a method to sample short vector from some discrete Gaussian distribution, and then an improved algorithm was introduced in [38].

Lemma 2 (see [27, 38]). *Let $n \ge 1$, $q \ge 2$, and $m = 2n\lceil \log q \rceil$. Given $A \in \mathbb{Z}_q^{n\times m}$, a trapdoor R_A of $\Lambda_q^{\perp}(A)$, a parameter $s = \omega(\sqrt{n \log q \log n})$, and $u \in \mathbb{Z}_q^n$. A PPT algorithm SamplePre(A, R_A, u, s) will output a short $e \in \Lambda_q^{u}(A)$ sampled from a distribution close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(A),s}$.*

The short integer solution (SIS), ISIS (both in ℓ_∞ norm), and LWE problems are described as follows.

Definition 1 (SIS and ISIS). Given a random $A \in \mathbb{Z}_q^{n\times m}$, a random syndrome $u \in \mathbb{Z}_q^n$, and a real β,

(i) SIS: to return a vector $e \in \mathbb{Z}^m$ satisfying that $A \cdot e = 0 \bmod q$, $0 \ne \|\mathbf{e}\|_\infty \le \beta$
(ii) ISIS: to return a vector $e \in \mathbb{Z}^m$ satisfying that $A \cdot e = u \bmod q$, $\|\mathbf{e}\|_\infty \le \beta$

Lemma 3 (see [27, 39]). *For $m, \beta = poly(n)$, $q \ge \beta \cdot \widetilde{\mathcal{O}}(\sqrt{n})$, the average-case (I)SIS problems are at least as hard as the SIVP$_\gamma$ problem in the worst-case to within $\gamma = \beta \cdot \widetilde{\mathcal{O}}(\sqrt{nm})$ factor.*

Definition 2 (LWE). Given a random $s \in \mathbb{Z}_q^n$, a probability distribution $\chi \in \mathbb{Z}$, define $\mathcal{A}_{\mathbf{s},\chi}$ by sampling $A \in \mathbb{Z}_q^{n\times m}$, $e \longleftarrow_R \chi^m$, outputting $(A, A^T s + e)$, to make distinguish between $\mathcal{A}_{\mathbf{s},\chi}$ and $\mathcal{U} \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$. Define $\beta \ge \sqrt{n} \cdot \omega(\log n)$, $q = p^e$ where p is a prime, $e \in \mathbb{Z}$, and $\chi = \mathcal{D}_{\mathbb{Z}^m,s}$, the LWE problem is as hard as SIVP$_{\widetilde{\mathcal{O}}(nq/\beta)}$.

Lemma 4 (see [40]). *Let $n \ge 1$ and prime $q \ge 2$, assume that $m > (n+1)\log n + \omega(\log n)$. Matrices $A, B \longleftarrow_R \mathbb{Z}_q^{n\times m}$ and $R \longleftarrow_R \{-1, 1\}^{m\times m}$. Thus, $(A, AR, R^T e)$ is close to $(A, B, R^T e)$ where $e \in \mathbb{Z}_q^m$.*

Lemma 5 (see [40]). *Let* $R \longleftarrow_R \{-1,1\}^{m\times m}$*; thus,* $\Pr[\|\mathbf{Re}\|_\infty > \|\mathbf{e}\|_\infty \cdot \omega(\sqrt{\log m})] < negl(m)$ *where* $e \in \mathbb{R}^m$.

Lemma 6 (see [40]). *Let* $q \geq 3$, $A, B \longleftarrow_R \mathbb{Z}_q^{n\times m}$, *and* $s \geq \|\widetilde{R}_\mathbf{B}\| \cdot \sqrt{m} \cdot \omega(\log m)$. *Given a trapdoor* R_B *of* $\Lambda_q^\perp(B)$, $R \in \{-1,1\}^{m\times m}$, *and* $u \in \mathbb{Z}_q^n$. *A PPT algorithm SampleR* (A, B, R, R_B, u, s) *will output* $e \in \mathbb{Z}^{2m}$ *distributed statistically close to* $\mathscr{D}_{\Lambda_q^\mathbf{u}([\mathbf{A}|\mathbf{AR}+\mathbf{B}]),s}$.

3. Preparations

3.1. The Improved Identity-Encoding Technique. The matrix $B \in \mathbb{Z}_q^{n\times m}$ of [23] is replaced by a random vector $u \in \mathbb{Z}_q^n$, i.e., Gpk $= (A_0, A_1, A_2, u)$, and i's secret signing key is a short vector $e_i = (e_{i,0}, e_{i,1}) \in \mathbb{Z}^{2m}$ that is in a coset of $\Lambda_q^\perp(A_i)$, i.e., $\Lambda_q^u(A_i) = \{e_i \in \mathbb{Z}^m | A_i \cdot e_i = u \bmod q\}$, and i's revocation token is created by A_0 and $e_{i,0}$, i.e., $\text{grt}_i = A_0 \cdot e_{i,0} \bmod q \in \mathbb{Z}_q^n$.

To construct a secure Stern-type ZKAoK protocol, we transform the identity-encoding matrix $A_i = [A_0|A_1 + iA_2] \in \mathbb{Z}_q^{n\times 2m}$ for i into a new shape. We first give two new notations (we restate that the group is of $N = 2^\ell$ members):

(i) $g_\ell = (1, 2, 2^2, \ldots, 2^{\ell-1})$: a power-of-two vector, for integer $i \in \{0, \ldots, N-1\}$, $i = g_\ell^T \cdot \text{Bin}(i)$, where $\text{Bin}(i) \in \{0,1\}^\ell$ is i's binary decomposition.

(ii) $\otimes$: given $A \in \mathbb{Z}_q^{n\times m}$, $e = (e_1, e_2, \ldots, e_\ell) \in \mathbb{Z}_q^\ell$, and $e' \in \mathbb{Z}_q^m$, we define

$$e \otimes e' = (e_1 e', e_2 e', \ldots, e_\ell e') \in \mathbb{Z}_q^{m\ell}, \qquad e \otimes A = [e_1 A | e_2 A | \ldots | e_\ell A] \in \mathbb{Z}_q^{n\times m\ell}. \tag{2}$$

Thus, A_i is transformed into some public A' that is irrelevant to index i and

$$A' = [A_0 | A_1 | A_2 | \pi | \cdots | 2^{\ell-1} A_2] = [A_0 | A_1 | g_\ell \otimes A_2] \in \mathbb{Z}_q^{n\times(\ell+2)m}. \tag{3}$$

Correspondingly, $e_i = (e_{i,0}, e_{i,1})$ is transformed to $e_i' = (e_{i,0}, e_{i,1}, \text{Bin}(i) \otimes e_{i,1}) \in \mathbb{Z}^{(\ell+2)m}$.

Therefore, $A_i \cdot e_i = u \bmod q$ is transformed into a new shape, $(r.1)$ $A_i \cdot e_i = A' \cdot e_i' = u \bmod q$.

As for revocation mechanism, as that in [11], the signer's grt_i is bound to an LWE function, $(r.2)$ $b = B^T \cdot \text{grt}_i + e = (B^T A_0) \cdot e_{i,0} + e \bmod q$, $B \in \mathbb{Z}_q^{n\times m}$ is from an oracle, and $e \longleftarrow_R \chi^m$.

In a nutshell, by creatively putting the transformation ideas and the Stern-extension argument system showed by Ling et al. [25] together, we will design a secure zero-knowledge protocol to prove $(r.1)$ and $(r.2)$.

3.2. A New Stern-Type Zero-Knowledge Proof Protocol. In our new underlying Stern-type ZKP protocol, the decomposition (Dec), extension (Ext), and matrix-extension (Mat-Ext) techniques are adopted. Specific sets are as follows: $B_{2\ell}$, B_{3m}, $\text{Sec}_\beta(i\ d)$, and $\text{SecExt}(id^*)$; permutations such as $\pi, \varphi \in \mathcal{S}_{3m}$ and $\tau \in \mathcal{S}_{2\ell}$ and a composition $\mathcal{T}$ are also used. We omit these duplicate concepts, and the detailed definitions can be found in literatures [10, 11, 25]. In addition, we define a series of integers: $k = \lfloor \log \beta \rfloor + 1, \beta_1 = \lceil \beta/2 \rceil, \beta_2 = \lceil (\beta - \beta_1)/2 \rceil, \ldots, \beta_k = 1$.

The underlying ZKP protocol between a prover $\mathscr{P}$ and any verifier $\mathscr{V}$ is as follows:

(1) The inputs include $A' = [A_0|A_1|g_\ell \otimes A_2] \in \mathbb{Z}_q^{n\times(\ell+2)m}$, $B \in \mathbb{Z}_q^{n\times m}$, $u \in \mathbb{Z}_q^n$, and $b \in \mathbb{Z}_q^m$.

(2) $\mathscr{P}$'s witnesses include $e' = (e_0', e_1', \text{Bin}(i) \otimes e_1') \in \text{Sec}_\beta(i\ d)$ corresponding to a secret identity index $i \in \{0, 1, \ldots, N-1\}$ and a vector $e \in \mathbb{Z}^m$, an LWE error.

(3) $\mathscr{P}$ tries to convince $\mathscr{V}$:

(3.1) $A' \cdot e' = u \bmod q$ where $e' \in \text{Sec}_\beta(i\ d)$, while keeping $i\ d = \text{Bin}(i) \in \{0,1\}^\ell$ secret.

(3.2) $b = (B^T A_0) \cdot e_0' + e \bmod q$, where $0 < \|\mathbf{e}_0'\|_\infty$, $|\pi|_\infty \leq \beta$.

For membership mechanism, i.e., $\mathscr{P}$'s goal is shown in 3.1. As in [32], $\mathscr{P}$ does as follows:

(1) Parse $A' = [A_0|A_1|g_\ell \otimes A_2] = [A_0|A_1|A_2|\cdots|\ 2^{\ell-1}\ A_2]$, and use Mat-Ext technique to extend it to $A^* = [A_0 | 0^{n\times 2m} |\ A_1 | 0^{n\times 2m} | A_2 | 0^{n\times 2m} | \cdots | 2^{\ell-1} A_2 | 0^{n\times 2m} | 0^{n\times 3m\ell}]$.

(2) Parse $i\ d = \text{Bin}(i) = (d_1, d_2, \ldots, d_\ell)$, and extend it to $id^* = (d_1, d_2, \ldots, d_\ell, d_{\ell+1}, \ldots, d_{2\ell}) \in B_{2\ell}$.

(3) Parse $e' = (e_0', e_1', \text{Bin}(i) \otimes e_1') = (e_0', e_1', d_1 e_1', \ldots, d_\ell e_1')$, and use Dec-Ext techniques extending $\mathbf{e}_0'$ and $\mathbf{e}_1'$ to k vectors $e_{0,1}', e_{0,2}', \ldots, e_{0,k}' \in B_{3m}$ and k vectors $e_{1,1}', e_{1,2}', \ldots, e_{1,k}' \in B_{3m}$, respectively. Thus, for $j \in \{1, 2, \ldots, k\}$, we define $e_j' = (e_{0,j}', e_{1,j}', d_1 e_{1,j}', \ldots, d_\ell e_{1,j}')$ and then $e_j' \in \text{SecExt}(id^*)$.

$\mathscr{P}'s$ goal is transformed into $(r.3)$ $A^* \cdot (\sum_{j=1}^k \beta_j e_j') = u \bmod q$ and $e_j' \in \text{SecExt}(id^*)$.

To prove $(r.3)$, as in [32], we take the following 2 steps:

(1) Sample k uniform $r_1', r_2', \ldots, r_k' \longleftarrow_R \mathbb{Z}_q^{(2\ell+2)3m}$ to mask $e_1', e_2', \ldots, e_k'$; thus,

$$A^* \cdot \left(\sum_{j=1}^k \beta_j (e_j' + r_j')\right) - u = A^* \cdot \left(\sum_{j=1}^k \beta_j r_j'\right) \bmod q. \tag{4}$$

(2) Sample $\pi, \varphi \in \mathcal{S}_{3m}$, $\tau \in \mathcal{S}_{2\ell}$; thus, for $j \in \{1, 2, \ldots, k\}$, $\mathcal{T}_{\pi,\varphi,\tau}(e_j') \in \text{SecExt}(\tau(id^*))$.

For revocation mechanism, i.e., $\mathscr{P}$'s goal is shown in 3.2. $\mathscr{P}$ does as follows:

(1) Let $B' = B^T A_0 \bmod q \in \mathbb{Z}_q^{m\times m}$ and $e_{j,0}' = \text{Parse}(e_j', 1, m)$

(2) Parse $e = (e_1, e_2, \ldots, e_m)$, and use Dec-Ext techniques to extend $\mathbf{e}$ to k vectors $e_1, e_2, \ldots, e_k \in B_{3m}$

(3) Define $B^* = [B' | I_m | 0^{n\times 2m}]$

$\mathscr{P}'s$ goal is transformed into $(r.4)$:

$$e_j \in B_{3m},$$

$$\begin{aligned} b^* &= B' \cdot \left(\sum_{j=1}^{k} \beta_j e'_{j,o} \right) + \left[I_m | 0^{n \times 2m} \right] \cdot \left(\sum_{j=1}^{k} \beta_j e_j \right) \\ &= B^* \cdot \left(\sum_{j=1}^{k} \beta_j \left(e'_{j,0} + e_j \right) \right) \bmod q. \end{aligned} \quad (5)$$

To prove (r.4), we take the following 3 steps:

(1) Let $r_{j,0} = \text{Parse}(r'_j, 1, m)$.

(2) Sample k random $r_1, r_2, \ldots, r_k \longleftarrow_R \mathbb{Z}_q^{3m}$ to mask $e_1, e_2, \ldots, e_k$; thus,

$$\begin{aligned} &B^* \cdot \left(\sum_{j=1}^{k} \beta_j \left(e'_{j,0} + r'_{j,0}, e_j + r_j \right) \right) - b \\ &= B^* \cdot \left(\sum_{j=1}^{k} \beta_j \left(r'_{j,0}, r_j \right) \right) \bmod q. \end{aligned} \quad (6)$$

(3) Sample $\phi \in \mathcal{S}_{3m}$; thus, for $j \in \{1, 2, \ldots, k\}$, $\phi(e_j) \in B_{3m}$.

In our GS-VLR construction, we also adopt a statistically hiding and computationally blinding commitment scheme COM proposed in [41]. The randomness of COM is omitted.

(1) Commitments: $\mathcal{P}$ samples some objects as follows:

$$\begin{aligned} r'_1, r'_2, \ldots, r'_k &\longleftarrow_R \mathbb{Z}_q^{(2\ell+2)3m}; \\ r_1, r_2, \ldots, r_k &\longleftarrow_R \mathbb{Z}_q^{3m}; \\ \pi_1, \ldots, \pi_k, \varphi_1, \ldots, \varphi_k, \phi_1, \ldots, \phi_k &\in \mathcal{S}_{3m}; \\ \tau &\in \mathcal{S}_{2\ell}. \end{aligned} \quad (7)$$

Let $r'_{j,0} = \text{Parse}(r'_j, 1, m)$, $j \in \{1, 2, \ldots, k\}$. $\mathcal{P}$ sends CMT $= (c_1, c_2, c_3)$ to $\mathcal{V}$.

$$\begin{cases} c_1 = \text{COM}\left(\left\{ \pi_j, \varphi_j, \phi_j \right\}_{j=1}^{k}; \tau; A^* \cdot \left(\sum_{j=1}^{k} \beta_j r'_j \right); B^* \cdot \left(\sum_{j=1}^{k} \beta_j \cdot \left(r'_{j,0}, r_j \right) \right) \right), \\ c_2 = \text{COM}\left(\left\{ \mathcal{T}_{\pi_j, \varphi_j, \tau}\left(r'_j \right), \phi_j\left(r_j \right) \right\}_{j=1}^{k} \right), \\ c_3 = \text{COM}\left(\left\{ \mathcal{T}_{\pi_j, \varphi_j, \tau}\left(e'_j + r'_j \right), \phi_j\left(e_j + r_j \right) \right\}_{j=1}^{k} \right). \end{cases} \quad (8)$$

(2) Challenge: $\mathcal{V}$ samples a challenge $Ch \longleftarrow_R \{1, 2, 3\}$ and transfers to $\mathcal{P}$.

(3) Response: $\mathcal{P}$ does as follows:

(i) $Ch = 1$. For $j \in \{1, 2, \ldots, k\}$, let $v'_j = \mathcal{T}_{\pi_j, \varphi_j, \tau}(e'_j)$, $w'_j = \mathcal{T}_{\pi_j, \varphi_j, \tau}(r'_j)$, $v_j = \phi_j(e_j)$, $w_j = \phi_j(r_j)$, and $t_{i\,d} = \tau(id^*)$, define RSP $= (\{v'_j, w'_j, v_j, w_j\}_{j=1}^{k}, t_{i\,d})$

(ii) $Ch = 2$. For $j \in \{1, 2, \ldots, k\}$, let $\widehat{\pi}_j = \pi_j, \widehat{\varphi}_j = \varphi_j$, $\widehat{\phi}_j = \phi_j$, $\widehat{\tau} = \tau$, $x'_j = e'_j + r'_j$, and $x_j = e_j + r_j$, define RSP $= (\left\{ \widehat{\pi}_j, \widehat{\varphi}_j, \widehat{\phi}_j, x'_j, x_j \right\}_{j=1}^{k}, \widehat{\tau})$

(iii) $Ch = 3$. For $j \in \{1, 2, \ldots, k\}$, let $\widetilde{\pi}_j = \pi_j, \widetilde{\varphi}_j = \varphi_j$, $\widetilde{\phi}_j = \phi_j$, $\widetilde{\tau} = \tau$, $h'_j = r'_j$, and $h_j = r_j$, define RSP $= (\{\widetilde{\pi}_j, \widetilde{\varphi}_j, \widetilde{\phi}_j, h'_j, h_j\}_{j=1}^{k}, \widetilde{\tau})$

(4) Verification: $\mathcal{V}$ does as follows:

(i) $Ch = 1$. Check that $t_{i\,d} \in B_{2\ell}$, $v'_j \in \text{SecExt}(t_{i\,d})$, $v_j \in B_{3m}$, and

$$\begin{cases} c_2 = \text{COM}\left(\left\{ w'_j, w_j \right\}_{j=1}^{k} \right), \\ c_3 = \text{COM}\left(\left\{ v'_j + w'_j, v_j + w_j \right\}_{j=1}^{k} \right). \end{cases} \quad (9)$$

(ii) $Ch = 2$. Let $x'_j = \text{Parse}(x'_j, 1, m)$, check

$$\begin{cases} c_1 = \text{COM}\left(\left\{ \widehat{\pi}_j, \widehat{\varphi}_j, \widehat{\phi}_j \right\}_{j=1}^{k}; \widehat{\tau}; A^* \cdot \left(\sum_{j=1}^{k} \beta_j x'_j \right) - u; B^* \cdot \left(\sum_{j=1}^{k} \beta_j \left(x'_{j,0}, x_j \right) \right) \right) - b, \\ c_3 = \text{COM}\left(\left\{ \mathcal{T}_{\widehat{\pi}_j, \widehat{\varphi}_j, \widehat{\tau}}\left(x'_j \right), \widehat{\phi}_j\left(x_j \right) \right\}_{j=1}^{k} \right). \end{cases} \quad (10)$$

(iii) $Ch = 3$. Let $h_{j,0}' = \text{Parse}(h_{j,0}', 1, m)$, check

$$\begin{cases} c_1 = \text{COM}\left(\left\{\widetilde{\pi}_j, \widetilde{\varphi}_j, \widetilde{\phi}_j\right\}_{j=1}^{k}; \widetilde{\tau}; A^* \cdot \left(\sum_{j=1}^{k} \beta_j h_j'\right); B^* \cdot \left(\sum_{j=1}^{k} \beta_j \left(h_{j,0}', h_j\right)\right)\right), \\ c_3 = \text{COM}\left(\left\{\mathcal{T}_{\widetilde{\pi}_j, \widetilde{\varphi}_j, \widetilde{\tau}}\left(h_j'\right), \widetilde{\phi}_j\left(h_j\right)\right\}_{j=1}^{k}\right). \end{cases} \tag{11}$$

If all the conditions hold, $\mathcal{V}$ outputs 1. The relation $\mathcal{R}(n, k, \ell, q, m, \beta)$ is defined as follows:

$$\mathcal{R} = \left\{ \begin{array}{l} A_0, A_1, A_2, B \in \mathbb{Z}_q^{n\times m}, u \in \mathbb{Z}_q^n, b \in \mathbb{Z}_q^m, id = \text{Bin}(i), e \in \mathbb{Z}^m \\ e' = \left(e_0', e_1', \text{Bin}(i) \otimes e_1'\right) \in \text{Sec}_\beta(id); \text{s.t. } 0 < \left\|e'\right\|_\infty, \|e\|_\infty \le \beta \\ b = \left(B^T \cdot A_0\right) \cdot e_0' + e\text{mod}q, \left[A_0 | A_1 | g_\ell \otimes A_2\right] \cdot e' = u\text{mod}q \end{array} \right\}. \tag{12}$$

3.3. Analysis of the Protocol

Theorem 1. *If COM enjoys the properties as in [41], then the proposed protocol is a statistical ZKAoK for $\mathcal{R}(n, k, \ell, q, m, \beta)$, its every whole interaction has perfect completeness, soundness error 2/3, argument of knowledge property, and communication cost $\ell \cdot \widetilde{\mathcal{O}}(n)$.*

Proof. The details were given in [32], published in the proceedings of ISC 2019. The readers can refer to [32] directly; therefore, we omit them here. □

4. Our Improved GS-VLR over Lattices

4.1. Description of the Scheme

4.1.1. KeyGen $(1^n, N)$. Take a security parameter n and the group size N as input. Define the prime $q = \omega(n^2 \log n) > N$, dimension $m = 2n\lceil \log q \rceil$, parameter $s = \omega(\sqrt{n \log q \log n})$, and integer bound $\beta = \lceil s \cdot \log m \rceil$ satisfying that $(4\beta + 1)^2 \le q$. This algorithm does as follows:

(1) Run TrapGen(q, n, m) to get $A_0 \in \mathbb{Z}_q^{n\times m}$ and trapdoor R_{A_0}.

(2) Choose $A_1, A_2 \longleftarrow_R \mathbb{Z}_q^{n\times m}$ and $u \longleftarrow_R \mathbb{Z}_q^n$.

(3) As in [23], for $i \in \{0, 1, \ldots, N-1\}$, let $A_i = [A_0 | A_1 + iA_2] \in \mathbb{Z}_q^{n\times 2m}$ and proceed as follows:

(3.1) Choose $e_{i,1} \longleftarrow_R \mathcal{D}_{\mathbb{Z}^m, s}$, let $u_i = (A_1 + iA_2) \cdot e_{i,1}$. Run SamplePre$(A_0, R_{A_0}, u - u_i, s)$ to obtain $e_{i,0} \in \mathbb{Z}^m$.

(3.2) Let $\mathbf{e}_i = (\mathbf{e}_{i,0}, \mathbf{e}_{i,1}) \in \mathbb{Z}^{2m}$. Thus, $A_i \cdot e_i = u\text{mod}q$ and $0 < \|\mathbf{e}\|_{i\infty} \le \beta$.

(3.3) Let i's secret signing key be $\text{gsk}_i = e_i$ and its token be $\text{grt}_i = A_0 \cdot e_{i,0} \text{mod}\, q$.

(4) Output Gpk $= (A_0, A_1, A_2, u)$, Gsk $= (\text{gsk}_0, \text{gsk}_1, \ldots, \text{gsk}_{N-1})$, and Grt $= (\text{grt}_0, \text{grt}_1, \ldots, \text{grt}_{N-1})$.

4.1.2. Sign $(\text{Gpk}, \text{gsk}_i, m)$. Choose hash functions: $\mathcal{H}$: $\{0,1\}^* \longrightarrow \{1,2,3\}^{\omega(\log n)}$, $\mathcal{G}$: $\{0,1\}^* \longrightarrow \mathbb{Z}_q^{n\times m}$, and a $\beta -$ *boun de d* distribution $\chi \in \mathbb{Z}$. Take Gpk, $m \in \{0,1\}^*$ as input, a member i with secret-key $gsk_i = \mathbf{e}_i$ proceeds as follows:

(1) Choose $v \longleftarrow_R \{0,1\}^n$, let $B = \mathcal{G}(A_0, A_1, A_2, u, m, v) \in \mathbb{Z}_q^{n\times m}$.

(2) Choose $e \longleftarrow_R \chi^m$, let $b = B^T \cdot \text{grt}_i + e = (B^T \ A_0) \cdot e_{i,0} + e\text{mod}\, q$.

(3) Design a ZKP protocol to prove that the signer is a valid member which is achieved by repeating $\omega(\log n)$ times the underlying protocol as in Section 3.2 with (A_0, A_1, A_2, B, u, b) and a witness ($i\ d$, gsk_i, e), and then make it noninteractive as $\Pi = (\{\text{CMT}_j\}_{j\in\{1,2,\ldots,k\}}$, CH, $\{\text{RSP}_j\}_{j\in\{1,2,\ldots,k\}})$ where CH $= \{Ch_j\}_{j\in\{1,2,\ldots,k\}} = \mathcal{H}(m, A_0, A_1, A_2, u, B, b, \{\text{CMT}_j\}_{j\in\{1,2,\ldots,k\}})$.

(4) Output $\sigma = (m, \Pi, v, b)$.

4.1.3. Verify $(\text{Gpk}, RL, \sigma, m)$. Taking Gpk, (m, σ), and $RL = \{grt_{i'}\}_{0 \le i' \le N-1} \subseteq$ Grt as input, the verifier proceeds as follows:

(1) Parse $\sigma = (m, \Pi, v, b)$

(2) Check that whether CH $= \{Ch_j\}_{j\in\{1,2,\ldots,k\}} = \mathcal{H}(m, A_0, A_1, A_2, u, B, b, \{\text{CMT}_j\}_{j\in\{1,2,\ldots,k\}})$

(3) Run step 4 of the protocol in Section 3.2 to check the validity of RSP_j w.r.t. CMT_j and Ch_j

(4) Define $B = \mathcal{G}(A_0, A_1, A_2, u, m, v)$, for $\text{grt}_{i'} \in RL$, compute $e_{i'} = b - B^T \text{grt}_{i'} \text{mod}\, q$, and check that whether $\|e_{i'}\|_\infty > \beta$

(5) If all are satisfied, output 1 and accept σ; otherwise 0

4.2. Analysis of the Scheme

4.2.1. Efficiency. For our new scheme, three public matrices are needed for identity-encoding; thus, the bit-sizes of Gpk, gsk, and σ are $\widetilde{\mathcal{O}}(n^2)$, $\widetilde{\mathcal{O}}(n)$, and $\log N \cdot \widetilde{\mathcal{O}}(n)$, respectively. Compared with previous GS-VLR schemes over lattices, the $\mathcal{O}(\log N)$ factor for the bit-sizes of Gpk and gsk in the new construction is eliminated; meanwhile, it is also free of any encryptions.

Theorem 2. *With an overwhelming probability, the scheme in Section 4.1 is correct.*

Proof. A member i owning a valid witness $(e_i', e) \in \mathrm{Sec}_\beta(id) \times \chi^m$ can return a signature meeting the first three steps of *Verify*. As for step 4, the vector $\mathbf{e}_{i'}$ can be expressed as follows:

$$\begin{aligned} e_{i'} &= b - B^T \mathrm{grt}_i = B^T \mathrm{grt}_i + e - B^T \mathrm{grt}_{i'} \\ &= B^T \cdot \left(\mathrm{grt}_i - \mathrm{grt}_{i'}\right) + e \bmod q. \end{aligned} \tag{13}$$

(1) To prove that $\mathrm{grt}_i \notin RL \Rightarrow \mathrm{Verify}(\mathrm{Gpk}, RL, \mathrm{Sign}(\mathrm{Gpk}, \mathrm{gsk}_i, m), m) = 1$.

Suppose that $\mathrm{grt}_i \notin RL$; to prove that with an overwhelming probability, step 4 is satisfied, i.e., $\|e_{i'}\|_\infty > \beta$ and $\mathrm{Verify}(\mathrm{Gpk}, RL, \mathrm{Sign}(\mathrm{Gpk}, \mathrm{gsk}_i, m), m) = 1$. For all $\mathrm{grt}_{i'} \in RL$, the following is the establishment: $B^T(\mathrm{grt}_i - \mathrm{grt}_{i'}) = e_{i'} - e \bmod q$. Defining $s_{i'} = \mathrm{grt}_i - \mathrm{grt}_{i'} \bmod q$, we have that $\|B^T s_{i'}\|_\infty \le \|e_{i'}\|_\infty + \|e\|_\infty \le \|e_{i'}\|_\infty + \beta$. In addition, according to [11], $\|B^T s_{i'}\|_\infty > 2\beta$ with an overwhelming probability; thus, $\|e_{i'}\|_\infty > 2\beta - \beta = \beta$.

(2) To prove that $\mathrm{Verify}(\mathrm{Gpk}, RL, \mathrm{Sign}(\mathrm{Gpk}, \mathrm{gsk}_i, m), m) = 1 \Rightarrow \mathrm{grt}_{i'} \in RL$.

Suppose that $\mathrm{Verify}(\mathrm{Gpk}, RL, \mathrm{Sign}(\mathrm{Gpk}, \mathrm{gsk}_i, m), m) = 1$. For every $\mathrm{grt}_{i'} \in RL$, we have that $\|e_{i'}\|_\infty > \beta$. Therefore, if there is index i' satisfying that $\mathrm{grt}_i = \mathrm{grt}_{i'}$, we have that $e_{i'} = e$. Thus, $\|e_{i'}\|_\infty = |\pi|_\infty \le \beta$ and σ fails the step 4 of *Verify*. So, it is obviously a conflict. This concludes the correctness proof. ☐

Theorem 3. *If COM enjoys the property of statistically hiding as in [41], the proposed scheme is selfless-anonymous in the random oracle model.*

Proof. A series of games is established as follows:

Game 0: $\mathscr{C}$ proceeds as follows:

(1) Run KeyGen to get $\mathrm{Gpk} = (A_0, A_1, A_2, u)$, $\mathrm{Gsk} = (\mathrm{gsk}_0, \ldots, \mathrm{gsk}_{N-1})$, and $\mathrm{Grt} = (\mathrm{grt}_0, \ldots, \mathrm{grt}_{N-1})$. Set $RL = \varnothing$ and $\mathrm{Corr} = \varnothing$, and send Gpk to $\mathscr{A}$
(2) For $\mathscr{A}$'s corruption queries for a member i, $\mathscr{C}$ sets $\mathrm{Corr} = \mathrm{Corr} \cup \{i\}$ and returns gsk_i; for $\mathscr{A}$'s signing queries on m for i, $\mathscr{C}$ outputs $\sigma \longleftarrow \mathrm{Sign}(\mathrm{Gpk}, \mathrm{gsk}_i, m)$; for $\mathscr{A}$'s revocation queries for i, $\mathscr{C}$ sets $RL = RL \cup \{\mathrm{grt}_i\}$ and outputs gsk_i to $\mathscr{A}$
(3) $\mathscr{A}$ outputs a message $m \in \{0,1\}^*$, members i_0 and i_1, for $b \in \{0,1\}$, $i_b \notin \mathrm{Corr}$ and $\mathrm{grt}_{i_b} \notin RL$
(4) $\mathscr{C}$ chooses $b \longleftarrow_R \{0,1\}$, generates $\sigma^* \longleftarrow \mathrm{Sign}(\mathrm{Gpk}, \mathrm{gsk}_{i_b}, m^*) = (m^*, \Pi, v, b)$, and outputs it
(5) $\mathscr{A}$ makes queries as before without the rights to ask for gsk_{i_b} or grt_{i_b} for each $b \in \{0,1\}$
(6) Finally, $\mathscr{A}$ outputs a bit $b' \in \{0,1\}$

Game 1: $\mathscr{C}$ simulates step 4 of *Sign* by programming the oracle:

(1) Choose $v \longleftarrow_R \{0,1\}^n$ and $e \longleftarrow_R \chi^m$; let $B = \mathscr{G}(A_0, A_1, A_2, u, m, v)$ and $b = B^T \cdot \mathrm{grt}_{i_b} + e \bmod q$
(2) Program $\mathscr{H}(m^*, A_0, A_1, A_2, u, B, b, \{\mathrm{CMT}_j\}_{j\in\{1,2,\ldots,k\}}) = \{Ch_j\}_{j\in\{1,\ldots,k\}}$; other algorithms are as in the proof of Theorem 1
(3) Output $\widehat{\sigma}^* = (m^*, \Pi^*, v, b)$

Game 2: $\mathscr{C}$ defines $b = B^T \cdot r + e \bmod q$, so b is close to the one in Game 1, and thus Game 2 is statistically indistinguishable with Game 1.

Game 3: $\mathscr{C}$ defines $(B, b) \longleftarrow_R \mathscr{U}$, so (B, b) is close to the one in Game 2. Thus, Games 3 and 2 are computationally indistinguishable. Furthermore, the advantage $\mathrm{Adv}_{\mathscr{A}}^{\text{self-anon}}$ is 0.

According to the indistinguishability of Games 1, 2, and 3, the advantage $\mathrm{Adv}_{\mathscr{A}}^{\text{self-anon}}$ in Game 1 is negligible; therefore, our new scheme satisfies the definition of selfless-anonymity. ☐

Theorem 4. *Suppose* SIS *within $\beta' = poly(m)$ factor is hard, the proposed scheme is traceable.*

Proof. Suppose with an advantage ε, a forger $\mathscr{F}$ breaks the scheme. By using $\mathscr{F}$, we construct an efficient $\mathscr{A}$ to solve a SIS instance $\widehat{A} \in \mathbb{Z}_q^{n\times m}$ within $\beta' = 2\beta \cdot (1 + \omega(\sqrt{\log m}))$ factor. ☐

4.2.2. Setup. $\mathscr{A}$ proceeds as follows:

(1) Choose $e_0^*, e_1^* \longleftarrow_R \mathscr{D}_{\mathbb{Z}^m, s}$, $R \longleftarrow_R \{-1,1\}^{m\times m}$, and $i^* \in \{0, 1, \ldots, N-1\}$
(2) Run TrapGen to get $A_2 \in \mathbb{Z}_q^{n\times m}$ and a trapdoor R_{A_2}
(3) Define $A_0 = \widehat{A}$, $A_1 = A_0 \cdot R - i^* A_2 \bmod q$, and $u = A_0 \cdot (e_0^* + R \cdot e_1^*) \bmod q$
(4) For $i = i^*$, let $\mathrm{gsk}_{i^*} = (e_0^*, e_1^*)$ and $\mathrm{grt}_{i^*} = A_0 \cdot e_0^* \bmod q$
(5) For $i \in \{0, 1, \ldots, N-1\}/\{i^*\}$, let $A_i = [A_0 | A_1 + i \cdot A_2]$, run $\mathrm{Sample}R(A_0, A_2, R, R_{A_2}, u, s)$ to obtain $e_i = (e_{i,0}, e_{i,1}) \in \mathbb{Z}^{2m}$, and let $\mathrm{gsk}_i = e_i$, $\mathrm{grt}_i = A_0 \cdot e_{i,0} \bmod q$
(6) Let $\mathrm{Gpk} = (A_0, A_1, A_2, u)$, $\mathrm{Gsk} = (\mathrm{gsk}_0, \ldots, \mathrm{gsk}_{N-1})$, and $\mathrm{Grt} = (\mathrm{grt}_0, \ldots, \mathrm{grt}_{N-1})$, transfer Gsk and Grt to $\mathscr{F}$

4.2.3. Queries. $\mathcal{F}$ proceeds as follows:

(1) *Corruption*. Taking i as input, $\mathcal{A}$ outputs grt_i and adds i to Corr.

(2) *Signing*. Taking i and $m \in \{0,1\}^*$ as input, $\mathcal{A}$ outputs $\sigma \longleftarrow \mathrm{Sign}(\mathrm{Gpk}, gsk_i, m)$. In particular, the values in $\{1,2,3\}^{\omega(\log n)}$ are sampled as responses to $\mathcal{H}$. Let r_d be a reply to the d-th ($d \le q_{\mathcal{H}}$) query (here, $q_{\mathcal{H}}$ is the whole number of oracle queries for $\mathcal{H}$).

4.2.4. Forgery. $\mathcal{F}$ returns $m^* \in \{0,1\}^*$, $RL^* \subseteq \mathrm{Grt}$, and a forged $\sigma^* = (m^*, \Pi^*, v^*, b^*)$ which satisfies the following:

(1) $\mathrm{Verify}(\mathrm{Gpk}, RL^*, \sigma^*, m^*) = 1$

(2) The implicit-tracing does not succeed or returns a member not included in Corr/RL^*

$\mathcal{F}$ proceeds as in [11]; let $B = \mathcal{G}(A_0, A_1, A_2, u, m^*, v^*) \in \mathbb{Z}_q^{n\times m}$. $\mathcal{A}$ obtains a 3-fork involving $\Delta = (m^*, A_0, A_1, A_2, u, B^*, b^*, \{\mathrm{CMT}_j\}_{j\in\{1,\dots,k\}})$ after at most $32 \cdot q_{\mathcal{H}}/(\varepsilon - 3^{-k})$ operations of $\mathcal{F}$.

With the help of an extractor $\mathcal{K}$ in the proof of Theorem 1, we get a valid

$$\begin{aligned} \text{witness} &= \Big(id = \mathrm{Bin}(i) \in \{0,1\}^{\ell}, e_i \\ &= \big(e_{i,0}, e_{i,1}\big) \in \mathbb{Z}^{2m}, e^* \in \mathbb{Z}^m\Big), \end{aligned} \tag{14}$$

such that

(1) $[A_0 | A_1 + iA_2] \cdot e_i = u \bmod q$ and $e_i \in \mathrm{Sec}_\beta(i\ d)$

(2) $b^* = (B^{*T} \cdot A_0) \cdot e_{i,0} + e^* \bmod q$ and $0 < \|e^*\|_\infty \le \beta$

In the following, we show two cases:

(1) If $i \ne i^*$ (the probability is at most $(N-1)/N$), $\mathcal{A}$ aborts.

(2) If $i = i^*$, $\mathcal{A}$ returns $\widehat{e} = (e_0^* - e_{i^*,0}) + R \cdot (e_1^* - e_{i^*,1})$. Thus, we have that

$$\begin{aligned} \widehat{A} \cdot \widehat{e} &= A_0 \cdot \big(e_0^* - e_{i^*,0} + R \cdot \big(e_1^* - e_{i^*,1}\big)\big) \\ &= \underbrace{A_0 \cdot \big(e_0^* + R \cdot e_1^*\big)}_{u} - \underbrace{A_0 \cdot \big(e_{i^*,0} + R \cdot e_{i^*,1}\big)}_{u} \\ &= 0 \bmod q. \end{aligned} \tag{15}$$

In the followings, we show that with a high probability, $\widehat{e} \ne 0 \bmod q$ and $\|\widehat{e}\|_\infty \le \mathrm{poly}(m)$.

(1) $\|\widehat{e}\|_\infty \le \mathrm{poly}(m)$: for $j \in \{0,1\}$, $\|\mathbf{e}_i^*\|_\infty, \|\mathbf{e}_{i^*,j}\|_\infty \le \beta$ and $R \longleftarrow_R \{-1,1\}^{m\times m}$; thus, we have that

$$\|\widehat{e}\|_\infty \le \big(1 + \omega\big(\sqrt{\log m}\big)\big) \cdot 2\beta = \mathrm{poly}(m). \tag{16}$$

(2) $\widehat{e} \ne 0 \bmod q$: since $\sigma^* = (m^*, \Pi^*, v^*, b^*)$ is a forged signature, the implicit-tracing does not succeed or returns a member not included in Corr/RL^*.

(2.1) If the implicit-tracing will not succeed, $\mathrm{Verify}(\mathrm{Gpk}, \mathrm{grt}_{i^*}, \sigma^*, m^*) = 1$ will indicate that

$$\begin{aligned} A_0 \cdot e_{i^*,0} \bmod q \ne grt_{i^*} &= A_0 \cdot e_0^* \bmod q \\ e_{i^*,0} &\ne e_0^*. \end{aligned} \tag{17}$$

(2.2) If the implicit-tracing returns a member not included in $j^* \notin \mathrm{Corr}/RL^*$, we have that $\mathrm{Verify}(\mathrm{Gpk}, \mathrm{grt}_{j^*}, \sigma^*, m^*) = 0$ and $\mathrm{Verify}(\mathrm{Gpk}, RL^*, \sigma^*, m^*) = 1$. Thus, we get the conclusions as follows:

(2.2.1) $\mathrm{grt}_{j^*} \ne RL^*$; thus, $j^* \in \mathrm{Corr}$.

(2.2.2) Since $\|b - B^{*T} \cdot \mathrm{grt}_{j^*}\|_\infty = \|B^{*T} \cdot (A_0 \cdot e_{i^*,0} - \mathrm{grt}_{j^*}) + e^*\|_\infty \le \beta$, $\|\mathbf{e}^*\|_\infty \le \beta$. So, $\|B^{*T} \cdot (A_0 \cdot e_{i^*,0} - grt_{j^*}) + e^*\|_\infty \le 2\beta$, and based on [23], we come to the conclusion that with an overwhelming probability, $\mathrm{grt}_{j^*} = A_0 \cdot e_{i^*,0} \bmod q$.
Next, we consider the following:

(2.2.3) If $\mathcal{F}$ has never requested gsk_{i^*}, (e_0^*, e_1^*) will not be known to $\mathcal{F}$; thus, we have that $(e_0^*, e_1^*) \ne (e_{i^*,0}, e_{i^*,1})$ with overwhelming probability.

(2.2.4) If $\mathcal{F}$ has requested gsk_{i^*}, we have that $i^* \in \mathrm{Corr}$, $i^* \ne j^*$, $\mathrm{grt}_{i^*} \ne \mathrm{grt}_{j^*}$, and $e_0^* \ne e_{i^*,0}$.

According to the previous analysis, the same as in [32], for the different cases in 2.1 and 2.2.4 (suppose $e_1^* = e_{i^*,1}$) and in 2.1, 2.2.3, and 2.2.4 (suppose $e_1^* \ne e_{i^*,1}$), we have the conclusion that with probability $1 - \exp^{-\mathcal{O}(n)}$, $\widehat{e} \ne 0 \bmod q$. Therefore, based on the above analysis, we come to the conclusion that with a probability $\varepsilon\prime \ge \varepsilon/(2N) \cdot (1 - (7/9)^k) \cdot (1 - \exp^{-\mathcal{O}(n)})$, $\widehat{e}$ will satisfy $\widehat{A} \cdot \widehat{e} = 0 \bmod q$ and $0 \ne \|\widehat{e}\|_\infty \le 2\beta \cdot (1 + \omega(\sqrt{\log m})) = \beta\prime = \mathrm{poly}(m)$.

5. Conclusion

In this work, we introduced an improved GS-VLR scheme over lattices. By adopting a compact identity-encoding technique and a corresponding Stern -type statistical ZKP protocol, the group public-key and member secret signing key in our new construction enjoy the shorter bit-sizes; furthermore, the new design is free of any public-key encryptions, and thus it is more flexible to allow anonymous authentication in the mobile network, especially, for a group with a mass of members. Achieving a stronger security (e.g., almost-full anonymity or full anonymity) for GS-VLR over lattices is our future work.

Data Availability

No data were used to support the findings of this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by National Natural Science Foundation of China (No. 61802075), Guangxi Key Laboratory of Cryptography and Information Security (No.

GCIS201907), and Natural Science Foundation of Henan Province (No. 202300410508).

References

[1] D. Chaum and E. V. Heyst, "Group Signatures," in *Proceedings of the EUROCRYPT: International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 257–265, Springer, Brighton, UK, April 1991.

[2] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions," in *Proceedings of the EUROCRYPT: International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 614–629, Springer, Warsaw, Poland, May 2003.

[3] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proceedings of the 11th ACM Conference on Computer and Communications Security 2004*, pp. 168–177, Washington, DC, USA, October 2004.

[4] M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: the case of dynamic groups," in *Proceedings of the CT-RSA*, pp. 136–153, San Francisco, CA, USA, February 2005.

[5] A. Kiayias and M. Yung, "Secure scalable group signature with dynamic joins and separable authorities," *International Journal of Security and Networks*, vol. 1, no. 1/2, pp. 24–45, 2006.

[6] S. D. Gordon, J. Katz, and V. Vaikuntanathan, "A group signature scheme from lattice assumptions," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security Asiacrypt*, pp. 395–412, Singapore, December 2010.

[7] J. Camenisch, G. Neven, and M. Rückert, "Fully anonymous attribute tokens from lattices," in *Proceedings of the International Conference on Security and Cryptography for Networks SCN*, pp. 57–75, Amalfi, Italy, September 2012.

[8] J. Bootle, A. Cerulli, and P. Chaidos, "Foundations of fully dynamic group signatures," in *Proceedings of the International Conference on Applied Cryptography and Network Security ACNS*, pp. 117–136, Guildford, UK, June 2016.

[9] A. Ishida, Y. Sakai, and K. Emura, "Fully anonymous group signature with verifier-local revocation," in *Proceedings of the International Conference on Security and Cryptography for Networks SCN*, pp. 23–42, Amalfi, Italy, September 2018.

[10] A. Langlois, S. Ling, and K. Nguyen, "Lattice-based group signature scheme with verifier-local revocation," in *Proceedings of the International Workshop on Public Key Cryptography PKC*, pp. 345–361, Buenos Aires, Argentina, March 2014.

[11] S. Ling, K. Nguyen, A. L. Roux, and H. Wang, "A lattice-based group signature scheme with verifier-local revocation," *Theoretical Computer Science*, vol. 730, pp. 1–20, 2018.

[12] B. Libert, S. Ling, and F. Mouhartem, "Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security Asiacrypt*, pp. 373–403, Hanoi, Vietnam, December 2016.

[13] S. Ling, K. Nguyen, and H. Wang, "Lattice-based group signatures: achieving full dynamicity with ease," in *Proceedings of the International Conference on Applied Cryptography and Network Security ACNS*, pp. 293–312, Kanazawa, Japan, July 2017.

[14] S. Ling, K. Nguyen, and H. Wang, "Constant-size group signatures from lattices," in *Proceedings of the International Workshop on Public Key Cryptography PKC*, pp. 58–88, Rio de Janeiro, Brazil, March 2018.

[15] Y. Sun and Y. Liu, "A lattice-based fully dynamic group signatures without NIZK," in *Proceedings of the Inscrypt*, pp. 359–367, Guangzhou, China, December 2020.

[16] M. N. S. Perera and T. Koshiba, "Zero-knowledge proof for lattice-based group signature schemes with verifier-local revocation," in *Proceedings of the International Conference on Network-Based Information Systems NBIS*, pp. 772–782, Bratislava, Slovakia, September 2018.

[17] M. N. S. Perera and T. Koshiba, "Achieving strong security and verifier-local revocation for dynamic group signatures from lattice assumptions," in *Proceedings of the International Workshop on Security and Trust Management STM*, pp. 3–19, Barcelona, Spain, September 2018.

[18] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques Eurocrypt*, pp. 523–552, French Riviera, France, May 2010.

[19] Y. Zhang, Y. Hu, W. Gao, and M. Jiang, "Simpler efficient group signature scheme with verifier-local revocation from lattices," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 1, pp. 414–430, 2016.

[20] W. Gao, Y. Hu, Y. Zhang, and B. Wang, "Lattice-based group signature with verifier-local revocation," *Journal of Shanghai Jiaotong University (Science)*, vol. 22, no. 3, pp. 313–321, 2017.

[21] B. Libert, F. Mouhartem, and K. Nguyen, "A lattice-based group signature scheme with message-dependent opening," in *Proceedings of the Applied Cryptography and Network Security*, pp. 137–155, Guildford, UK, June 2016.

[22] S. Ling, K. Nguyen, H. Wang, and Y. Xu, "Forward-secure group signatures from lattices," in *Proceedings of the International Conference on Post-Quantum Cryptography PQCrypto*, pp. 44–64, Chongqing, China, May 2019.

[23] P. Q. Nguyen, J. Zhang, and Z. Zhang in *Proceedings of the International Workshop on Public Key Cryptography PKC*, pp. 401–426, Gaithersburg, MD, USA, March 2015.

[24] F. Laguillaumie, A. Langlois, B. Libert, and D. Stehlé, "Lattice-based group signatures with logarithmic signature size," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security Asiacrypt*, pp. 41–61, Bengaluru, India, December 2013.

[25] S. Ling, K. Nguyen, and D. Stehlé, "Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications," in *Proceedings of the Public-Key Cryptography - PKC 2013*, pp. 107–124, Nara, Japan, February 2013.

[26] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the Annual ACM Symposium on Theory of Computing STOC*, pp. 84–93, Baltimore, MD, USA, May 2005.

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

[28] S. Ling, K. Nguyen, and H. Wang, "Group signatures from lattices: simpler, tighter, shorter, ring-based," in *Proceedings of the International Workshop on Public Key Cryptography PKC*, pp. 427–449, Gaithersburg, MD, USA, March 2015.

[29] B. Libert, S. Ling, and K. Nguyen, "Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors," in

Proceedings of the Advances in Cryptology - EUROCRYPT 2016, pp. 1–31, Vienna, Austria, May 2016.
[30] S. Canard, A. Georgescu, G. Kaim, A. R. Langlois, and J. Traoré, "Constant-size lattice-based group signature with forward security in the standard model," *Provable and Practical Security*, Springer, Berlin, Germany, pp. 24–44, 2020.
[31] S. Katsumata and S. Yamada, "Group signatures without NIZK: from lattices in the standard model," in *Proceedings of the Advances in Cryptology-EUROCRYPT 2019*, pp. 312–344, Darmstadt, Germany, May 2019.
[32] Y. Zhang, Y. Hu, and Q. Zhang, "On new zero-knowledge proofs for lattice-based group signatures with verifier-local revocation," in *Proceedings of the ISC Conference*, pp. 190–208, New York City, NY, USA, September 2019.
[33] Y. Zhang, X. Liu, and Y. Hu, "Lattice-based group signatures with verifier-local revocation: achieving shorter key-sizes and explicit traceability with ease," in *Proceedings of the Cryptology and Network Security*, pp. 120–140, Fuzhou, China, October 2019.
[34] Y. Zhang, Y. Yin, and X. Liu, "Zero-knowledge proofs for improved lattice-based group signature scheme with verifier-local revocation," in *Proceedings of the International Conference on Frontiers in Cyber Security*, pp. 107–127, Xi'an, China, November 2019.
[35] Y. Zhang, X. Liu, and Y. Yin, "On new zero-knowledge proofs for fully anonymous lattice-based group signature scheme with verifier-local revocation," in *Proceedings of the ACNS workshops*, pp. 381–399, Rome, Italy, October 2020.
[36] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the Annual ACM Symposium on Theory of Computing STOC*, pp. 257–265, Philadelphia, PA, USA, May 1996.
[37] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," *Theory of Computing Systems*, vol. 48, no. 3, pp. 535–553, 2011.
[38] D. Micciancio and C. Peikert, "Trapdoors for lattices: simpler, tighter, faster, smaller," in *Proceedings of the Advances in Cryptology-EUROCRYPT 2012*, pp. 700–718, Cambridge, UK, April 2012.
[39] D. Micciancio and C. Peikert, "Hardness of SIS and LWE with small parameters," in *Proceedings of the Advances in Cryptology-CRYPTO 2013*, pp. 21–39, Santa Barbara, CA, USA, August 2013.
[40] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H)IBE in the standard model," in *Proceedings of the Advances in Cryptology-EUROCRYPT 2010*, pp. 553–572, French Riviera, France, May 2010.
[41] A. Kawachi, K. Tanaka, and K. Xagawa, "Concurrently secure identification schemes based on the worst-case hardness of lattice problems," in *Proceedings of the Advances in Cryptology - ASIACRYPT 2008*, pp. 372–389, Melbourne, Australia, December 2008.