Lattice-Based Group Signatures with Verifier-Local Revocation: Achieving Shorter Key-Sizes and Explicit Traceability with Ease

Yanhua Zhang[1(✉)], Ximeng Liu[2], Yupu Hu[3], Qikun Zhang[1], and Huiwen Jia[4]

[1] Zhengzhou University of Light Industry, Zhengzhou 450002, China
{yhzhang,qkzhang}@zzuli.edu.cn
[2] Fuzhou University, Fuzhou 350108, China
snbnix@gmail.com
[3] Xidian University, Xi'an 710071, China
yphu@mail.xidian.edu.cn
[4] Guangzhou University, Guangzhou 510006, China
hwjia@gzhu.edu.cn

Abstract. For lattice-based group signatures (GS) with verifier-local revocation (VLR), it only requires the verifiers to possess up-to-date group information (i.e., a revocation list, RL, consists of a series of revocation tokens for revoked members), but not the signers. The first such scheme was introduced by Langlois et al. in 2014, and subsequently, a full and corrected version (to fix a flaw in the original revocation mechanism) was proposed by Ling et al. in 2018. However, both constructions are within the structure of a *Bonsai Tree*, and thus features bit-sizes of the group public-key and the member secret-key proportional to $\log N$, where N is the maximum number of group members. On the other hand, the tracing algorithm for both schemes runs in a linear time in N (i.e., one by one, until the real signer is traced). Therefore for a large group, the tracing algorithm of conventional GS-VLR is not convenient and both lattice-based constructions are not that efficient.

In this work, we propose a much more efficient lattice-based GS-VLR, which is efficient by saving the $\mathcal{O}(\log N)$ factor for both bit-sizes of the group public-key and the member secret-key. Moreover, we achieve this result in a relatively simple manner. Starting with Nguyen et al.'s efficient and compact *identity-encoding technique* in 2015 - which only needs a constant number of matrices to encode the member's identity, we develop an improved identity-encoding function, and introduce an efficient Stern-type statistical zero-knowledge argument of knowledge (ZKAoK) protocol corresponding to our improved identity-encoding function, which may be of independent cryptographic interest.

Furthermore, we demonstrate how to equip the obtained lattice-based GS-VLR with explicit traceability (ET) in some simple way. This attractive functionality, only satisfied in the non-VLR constructions, can enable the tracing authority in lattice-based GS-VLR to determine the signer's real identity in a constant time, independent of N. In the whole

Y. Mu et al. (Eds.): CANS 2019, LNCS 11829, pp. 120–140, 2019.
https://doi.org/10.1007/978-3-030-31578-8_7

process, we show that the proposed scheme is proven secure in the random oracle model (ROM) based on the hardness of the Short Integer Solution (SIS) problem, and the Learning With Errors (LWE) problem.

Keywords: Lattice-based group signatures · Verifier-local revocation · Stern-type zero-knowledge proofs · Identity-encoding technique · Explicit traceability

1 Introduction

Group signature (GS), put forward by Chaum and van Heyst [10], is a fundamental privacy-preserving primitive which allows any member to issue signatures on behalf of the whole group without compromising his/her identity information, and given a valid message-signature pair, the tracing authority (i.e., an opener) can find out the signer's real identity. These two properties, called *anonymity* and *traceability* respectively, allow GS to find several real-life applications. To construct such valid scheme is a interesting and challenging work for the research community, and over the last quarter-century, various GS constructions with different security requirements, different levels of efficiency, and based on different hardness assumptions have been proposed (e.g., [4–7,13,16] $\cdots$).

LATTICE-BASED GROUP SIGNATURES. Lattice-based cryptography, believed to be the most promising candidate for post-quantum cryptography (PQC), possesses several noticeable advantages over conventional number-theoretic cryptography: conjectured resistance against quantum computers, faster arithmetic operations and provable security under the *worst-case* hardness assumptions. Since the creative works of Ajtai [2], Regev [34], Micciancio and Regev [28], and Gentry et al. [12], lattice-based cryptography has attracted significant interest by the research community and become an exciting cryptographic research field. In recent ten years, lattice-based GS has been paid greet attention along with other primitives. The first construction was put forth by Gordon et al. [13], while their solution only obtains a low running efficiency, due to the linear-size of public-key and signature (i.e., linear in the security parameter n, and the maximum number of group members N). Camenisch et al. [8] introduced a variant of [13] to achieve the improvements with a shorter public-key and stronger anonymity while the signature size is still linear in N. The linear-size barrier problem is eventually overcome by Laguillaumie et al. [17], who provided the first logarithmic lattice-based GS scheme with relatively large parameters. Ling et al. [24] and Nguyen et al. [31] constructed more efficient schemes with $\mathcal{O}(\log N)$ signature size respectively. More recently, Libert et al. [20] developed a lattice-based accumulator from Merkle trees and based on which they designed the first lattice-based GS not requiring any GPV trapdoors. The first lattice-based GS realizations with message-dependent opening (MDO), forward-secure (FS), and without NIZK in the standard model (SM) were then proposed by Libert et al. [21], Ling et al. [26], and Katsumata and Yamada [14], respectively. For the lattice-based GS schemes mentioned above, all are designed for the static groups and analyzed in the security model of Bellare et al. [4], where no candidate member is allowed to join or leave after the whole group's preliminary setup.

For lattice-based GS schemes with dynamic features, member enrollment was firstly token into account by Libert et al. [19] and a dynamic construction in the model of Kiayias and Yong [16] and Bellare et al. [5] was introduced. Ling et al. [27] added some dynamic ingredients into a static accumulator constructed in [20] to construct the first lattice-based GS scheme with full dynamicity (i.e., candidate members can join and leave the group at will) in the model of Bootle et al. [7]. Recently, Ling et al. [25] introduced a constant-size lattice-based GS scheme (i.e., signature size is independent of N), meanwhile supporting dynamic member enrollments.

As an orthogonal problem of member enrollment, the support for membership revocation is also a desirable functionality of lattice-based GS. The verifier-local revocation (VLR) mechanism, which only requires the verifiers to possess some up-to-date group information (i.e., a revocation list, RL, consists of a series of revocation tokens for the revoked members), but not the signers, is more efficient than the accumulators, especially when considering a large group. The first such scheme was introduced by Langlois et al. [18] in 2014, and subsequently, a full and corrected version (to fix a flaw in original revocation mechanism) was proposed by Ling et al. [22], and two more schemes achieving different security notions were proposed by Perera and Koshiba [32,33] in 2018. However, all constructions are within the structure of a *Bonsai Tree* of hard random lattices [9], and thus features bit-sizes of the group public-key and the member secret-key proportional to $\log N$. The only two exceptions are [11,35] which adopt a identity-encoding function as introduced in [31] to encode the member's identity index and save a $\mathcal{O}(\log N)$ factor for both bit-sizes. However, the latter two constructions both involve a series of sophisticated encryption operations and zero-knowledge proof protocols in the signing phase, and on the other hand, the tracing algorithm for [11,18,22,35] runs in a linear time in N (i.e., one by one for all members, until the real signer is traced). For a large group, the tracing algorithm of conventional GS-VLR is not so convenient and almost of all lattice-based constructions are not that efficient. Thus these somewhat unsatisfactory state-of-affairs highlights the challenge of designing a simpler and more efficient lattice-based GS scheme with VLR, which can be more suitable for a large group.

Our results and main techniques. In this work, we reply positively to the problems discussed above. Specifically, we propose a new lattice-based GS-VLR achieving shorter key-sizes and explicit traceability. Here, by "shorter key-sizes", we mean saving a $\mathcal{O}(\log N)$ factor for both bit-sizes of the group public-key and the member secret-key; by "explicit traceability", we mean the tracing authority determining the signer's real identity in a constant time, independent of N. The proposed scheme is proven secure in the random oracle model (ROM) based on the hardness of the Short Integer Solution (SIS) problem, and the Learning With Errors (LWE) problem.

The comparisons between our scheme and previous works, in terms of asymptotic efficiency (i.e., key-sizes, explicit traceability), functionality (i.e., static or not) and anonymity, are shown in Table 1 (the security parameter is n, time period $T = 2^d$ and group size $N = 2^\ell = \mathsf{poly}(n)$).

Our construction operates in the model of Boneh and Shacham [6] for VLR, which enjoys the implicit traceability, and additionally, the explicit traceability is also obtained. Furthermore, we declare that the "shorter key-sizes" and "explicit traceability" can be obtained in a relatively simple manner, thanks to three main techniques discussed below.

Table 1. Comparisons of known lattice-based GS schemes.

Scheme	Group public-key size	Signer secret-key size	Explicit traceability	Functionality	Anonymity
GKV [13]	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	yes	static	CPA
CNR [8]	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	yes	static	CCA
LLLS [17]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	yes	static	CPA
LLNW [18]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	no	VLR	Selfless
LNW [24]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	yes	static	CCA
NZZ [31]	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n^2)$	yes	static	CCA
LLNW [20]	$\widetilde{\mathcal{O}}(n^2 + n \cdot \ell)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	yes	static	CCA
LMN [21]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	yes	MDO	CCA
LLMNW [19]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	yes	enrollment	CCA
ZHGJ [35]	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	no	VLR	Selfless
LNWX [27]	$\widetilde{\mathcal{O}}(n^2 + n \cdot \ell)$	$\widetilde{\mathcal{O}}(n) + \ell$	yes	fully-dynamic	CCA
GHZW [11]	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	no	VLR	Selfless
LNWX [26]	$(\ell + d) \cdot \widetilde{\mathcal{O}}(n^2)$	$(\ell+d)^2 \cdot d \cdot \widetilde{\mathcal{O}}(n^2)$	yes	FS	CCA
LNLW [22]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	no	VLR	Selfless
KP [33]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\ell \cdot \widetilde{\mathcal{O}}(n)$	yes	VLR	almost-CCA
KP [32]	$\ell \cdot \widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	yes	fully-dynamic	almost-CCA
LNWX [25]	$\widetilde{\mathcal{O}}(n)$	$\widetilde{\mathcal{O}}(n)$	yes	enrollment	CCA
KY [14]	$N \cdot \widetilde{\mathcal{O}}(n^2)$	$N \cdot \widetilde{\mathcal{O}}(n^2)$	yes	static	Selfless
Ours	$\widetilde{\mathcal{O}}(n^2)$	$\widetilde{\mathcal{O}}(n)$	yes	VLR	Selfless

Firstly, as we discussed earlier, adopting a *Bonsai Tree* structure to construct lattice-based GS-VLR results in a larger bit-sizes of the group public-key and the member secret-key. To realize a more efficient lattice-based GS-VLR with shorter key-sizes, we further need an efficient mechanism to encode the member's identity information, and a simpler zero-knowledge protocol to prove the signer's validity as a certified group member.

Towards the goal described as above, we utilize a compact *identity-encoding technique* introduced in [31] which only needs a constant number of matrices to encode the member's identity index. We consider the group of $N = 2^\ell$ members and each member is identified by a ℓ-bits string $\mathsf{id} = (d_1, d_2, \cdots, d_\ell) \in \{0,1\}^\ell$ which is a binary representation of his/her identity index $i \in \{1, \cdots, N\}$, that is, $\mathsf{id} = \mathsf{bin}(i) \in \{0,1\}^\ell$. Throughout this paper, let n be the security parameter, and other parameters N, m, q, β, s are the function of n and will be determined later (see Sect. 4). In our new VLR scheme, the group public-key only consists of a random vector $\mathbf{u} \in \mathbb{Z}_q^n$ and 4 random matrices $\mathbf{A}_0$, $\mathbf{A}_1^1$, $\mathbf{A}_2^2$ (used for identity-encoding) and $\mathbf{A}_3^3$ (only used for explicit traceability) over $\mathbb{Z}_q^{n\times m}$. For member i, instead of generating a trapdoor basis matrix for a hard random lattice as the signing secret-key for i as in [31], we sample some short $2m$-dimensional vector $\mathbf{e}_i = (\mathbf{e}_{i,1}, \mathbf{e}_{i,2}) \in \mathbb{Z}^{2m}$ satisfying $0 < \|\mathbf{e}_i\|_\infty \le \beta$, and $\mathbf{A}_i \cdot \mathbf{e}_i = \mathbf{u} \bmod q$, where $\mathbf{A}_i = [\mathbf{A}_0|\mathbf{A}_1^1 + i\mathbf{A}_2^2] \in \mathbb{Z}_q^{n\times 2m}$. Furthermore, for the VLR feature, the revocation token of i is constructed by $\mathbf{A}_0$ and $\mathbf{e}_{i,1} \in \mathbb{Z}^m$, that is, $\mathsf{grt}_i = \mathbf{A}_0 \cdot \mathbf{e}_{i,1} \bmod q$.

Secondly, the implicit tracing algorithm of conventional lattice-based GS-VLR runs in a linear time in N, and thus it is not so convenient, resulting in a low efficiency. To realize an efficient construction with explicit traceability, we further need an efficient mechanism to encrypt the identity index of member i (in our actual construction, it's to encrypt $\mathsf{bin}(i) \in \{0,1\}^\ell$) to obtain a ciphertext $\mathbf{c}$, and design a zero-knowledge argument to prove: $\mathbf{c}$ is a correct encryption of $\mathsf{bin}(i)$, namely, a lattice-based verifiable encryption protocol. Besides the public matrix $\mathbf{A}_0$, $\mathbf{A}_1^1$, and $\mathbf{A}_2^2$ for identity-encoding, a fourth matrix $\mathbf{A}_3^3$ is required to encrypt $\mathsf{bin}(i)$ using the dual LWE cryptosystem [12]. This relation can be expressed as $\mathbf{c} = (\mathbf{c}_1 = \mathbf{A}_3^{3\top}\mathbf{s} + \mathbf{e}_1 \bmod q,\ \mathbf{c}_2 = \mathbf{G}^\top\mathbf{s} + \mathbf{e}_2 + \lfloor q/2 \rfloor \mathsf{bin}(i) \bmod q)$ where $\mathbf{G}$ is a random matrix, and $\mathbf{s}$, $\mathbf{e}_1$, $\mathbf{e}_2$ are random vectors having certain specific norm.

Thirdly, the major challenge for our construction lies in how to design a simpler and efficient zero-knowledge proof protocol to prove the following relations: (a) $[\mathbf{A}_0|\mathbf{A}_1^1 + i\mathbf{A}_2^2] \cdot \mathbf{e}_i = \mathbf{u} \bmod q$; (b) $\mathsf{grt}_i = \mathbf{A}_0 \cdot \mathbf{e}_{i,1} \bmod q$; (c) $\mathbf{c} = (\mathbf{c}_1 = \mathbf{A}_3^{3\top}\mathbf{s} + \mathbf{e}_1 \bmod q,\ \mathbf{c}_2 = \mathbf{G}^\top\mathbf{s} + \mathbf{e}_2 + \lfloor q/2 \rfloor \mathsf{bin}(i) \bmod q)$. For relation (b), we utilize a creative idea introduced by Ling et al. [22] by drawing a matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$ from a random oracle and a vector $\mathbf{e}_0 \in \mathbb{Z}^m$ from the LWE error distribution, define $\mathbf{b} = \mathbf{B}^\top \mathsf{grt}_i + \mathbf{e}_0 = (\mathbf{B}^\top\mathbf{A}_0) \cdot \mathbf{e}_{i,1} + \mathbf{e}_0 \bmod q$, thus the member i's token grt_i is bound to a one-way and injective LWE function. For relation (c), we utilize a creative idea of Ling et al. [24] by constructing a matrix $\mathbf{P} \in \mathbb{Z}_q^{(m+\ell)\times(n+m+\ell)}$ (obtained from the public matrices $\mathbf{A}_3^3$ and $\mathbf{G}$, see Sect. 3 for details), and a vector $\mathbf{e} = (\mathbf{s}, \mathbf{e}_1, \mathbf{e}_2) \in \mathbb{Z}^{n+m+\ell}$, then let $\mathbf{c} = \mathbf{P}\mathbf{e} + (\mathbf{0}^m, \lfloor q/2 \rfloor \mathsf{bin}(i)) \bmod q$, thus the identity index i is now bound to this new form which is easy to construct a Stern-type statistical zero-knowledge proof protocol.

For relation (a), since $\mathbf{e}_i \in \mathbb{Z}^{2m}$ is a valid short solution to the Inhomogeneous Short Integer Solution (ISIS) instance $(\mathbf{A}_i, \mathbf{u})$ where $\mathbf{A}_i = [\mathbf{A}_0|\mathbf{A}_1^1 + i\mathbf{A}_2^2]$, a direct way for member i to prove his/her validity as a certified group member without leaking $\mathbf{e}_i$ just by performing a Stern-type statistical zero-knowledge argument of knowledge (ZKAoK) as in [23]. However, in order to protect the anonymity of i, the structure of $\mathbf{A}_i$ should not be given explicitly. How to realize a Stern-type zero-knowledge proof without leaking $\mathbf{A}_i$ and $\mathbf{e}_i$ simultaneously? To solve this open problem, we transform matrix $\mathbf{A}_i$ to $\mathbf{A}'$ which enjoys a new form and is independent of the identity index i, i.e., $\mathbf{A}' = [\mathbf{A}_0|\mathbf{A}_1^1|\mathbf{g}_\ell \otimes \mathbf{A}_2^2] \in \mathbb{Z}_q^{n\times(\ell+2)m}$, where $\mathbf{g}_\ell = (1, 2, 2^2, \cdots, 2^{\ell-1})$ is a power-of-two vector, and the identity index i can be rewritten as $i = \mathbf{g}_\ell^\top \cdot \mathsf{bin}(i)$, the notation $\otimes$ denotes a concatenation with vectors or matrices, and the detailed definition will be given later (see Sect. 3). As a corresponding change to the member i's signing secret-key, $\mathbf{e}_i = (\mathbf{e}_{i,1}, \mathbf{e}_{i,2})$ is now transformed to $\mathbf{e}'_i = (\mathbf{e}_{i,1}, \mathbf{e}_{i,2}, \mathsf{bin}(i) \otimes \mathbf{e}_{i,2}) \in \mathbb{Z}^{(\ell+2)m}$. Thus, to argue the relation $\mathbf{A}_i \cdot \mathbf{e}_i = \mathbf{u} \bmod q$, we instead show that $\mathbf{A}' \cdot \mathbf{e}'_i = \mathbf{u} \bmod q$.

Putting the above transformations ideas and the versatility of the Stern-type argument system introduced by Ling et al. [23] together, we can construct an efficient Stern-type interactive protocol for the relations (a), (b) and (c).

To summarize, by incorporating the compact *identity-encoding technique* and the corresponding efficient Stern-type statistical ZKAoK into a lattice-based GS, we design a more efficient lattice-based GS-VLR. The proposed scheme obtains the shorter bit-sizes for the group public-key and the group member secret-key, furthermore, the explicit traceability, and thus, is more suitable for a large group. In addition, we believe that the innovative ideas and design approaches in our whole constructions may be of independent interest.

Organization. In the forthcoming sections, we first recall some background on GS-VLR and lattice-based cryptography in Sect. 2. Section 3 turns to develop an improved identity-encoding technique, an explicit traceability mechanism and the corresponding new Stern-type statistical ZKAoK protocol that will be used in our construction. Our scheme is constructed and analyzed in Sect. 4.

2 Preliminaries

Notations. Assume that all vectors are in a column form. $\mathcal{S}_k$ denotes the set of all permutations of k elements, and $\xleftarrow{\$}$ denotes that sampling elements from a given distribution uniformly at random. Let $\|\cdot\|_\infty$ denote the infinity norm (ℓ_∞) of a vector. Given $\boldsymbol{e} = (e_1, e_2, \cdots, e_n) \in \mathbb{R}^n$, $\mathsf{Parse}(\boldsymbol{e}, k_1, k_2)$ denotes the vector $(e_{k_1}, e_{k_1+1}, \cdots, e_{k_2}) \in \mathbb{R}^{k_2-k_1+1}$ for $1 \le k_1 \le k_2 \le n$. $\log a$ denotes the logarithm of a with base 2. The acronym PPT stands for "probabilistic polynomial-time".

2.1 Group Signatures with VLR

A conventional GS-VLR scheme involves two entities: a group manager (also is a tracing authority) and a sets of group members. In order to support an explicit traceability we add an Open algorithm to conventional GS-VLR.

Syntax of GS-VLR with Explicit Traceability. A GS-VLR with the explicit traceability (GS-VLR-ET) consists of 4 polynomial-time algorithms: KeyGen, Sign, Verify, Open. Because of the page limitation, we omit the detailed definition, if any necessary, please contact the corresponding author for the full version.

Correctness and Security of GS-VLR-ET. As put forward by Boneh and Shacham [6], A conventional GS-VLR scheme should satisfy correctness selfless-anonymity, and traceability. Thus for GS-VLR-ET, these 3 requirements also should be satisfied. Due to the limited space, the details are presented in the full paper.

2.2 Background on Lattices

Ajtai [2] first introduced how to obtain a statistically close to uniform matrix $\mathbf{A}$ together with a low Gram-Schmidt norm basis for $\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m \mid \mathbf{A} \cdot \mathbf{e} = \mathbf{0} \bmod q\}$, then two improved algorithms were investigated by [3,30].

Lemma 1 **([2,3,30]).** *Let integers $n \geq 1$, $q \geq 2$, and $m = 2n\lceil \log q \rceil$. There exists a* PPT *algorithm* $\mathsf{TrapGen}(q, n, m)$ *that outputs* $\mathbf{A}$ *and* $\mathbf{R_A}$*, such that* $\mathbf{A}$ *is statistically close to a uniform matrix in* $\mathbb{Z}_q^{n\times m}$ *and* $\mathbf{R_A}$ *is a trapdoor for* $\Lambda_q^{\perp}(\mathbf{A})$*.*

Lemma 2 **([12,30]).** *Let integers $n \geq 1$, $q \geq 2$, and $m = 2n\lceil \log q \rceil$, given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a trapdoor $\mathbf{R_A}$ for $\Lambda_q^{\perp}(\mathbf{A})$, a parameter $s = \omega(\sqrt{n \log q \log n})$ and a vector $\boldsymbol{u} \in \mathbb{Z}_q^n$, there is a* PPT *algorithm* $\mathsf{SamplePre}(\mathbf{A}, \mathbf{R_A}, \mathbf{u}, s)$ *that returns a short vector $\mathbf{e} \in \Lambda_q^{\mathbf{u}}(\mathbf{A})$ sampled from a distribution statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),s}$.*

We recall 3 *average-case* lattices problems: ISIS, SIS (in the ℓ_∞ norm), LWE.

Definition 1. *The* $(\mathsf{I})\mathsf{SIS}^{\infty}_{n,m,q,\beta}$ *problems are: Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a random syndrome vector $\boldsymbol{u} \in \mathbb{Z}_q^n$ and a real $\beta > 0$,*

- $\mathsf{SIS}^{\infty}_{n,m,q,\beta}$*: to find a non-zero $\mathbf{e} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{e} = \mathbf{0} \bmod q$, $\|\mathbf{e}\|_\infty \leq \beta$.*
- $\mathsf{ISIS}^{\infty}_{n,m,q,\beta}$*: to find a vector $\mathbf{e} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{e} = \mathbf{u} \bmod q$, $\|\mathbf{e}\|_\infty \leq \beta$.*

Lemma 3 **([12,29]).** *For m, $\beta = \mathsf{poly}(n)$, and $q \geq \beta \cdot \widetilde{\mathcal{O}}(\sqrt{n})$, the average-case* $(\mathsf{I})\mathsf{SIS}^{\infty}_{n,m,q,\beta}$ *problems are at least as hard as the* SIVP_γ *problem in the worst-case to within $\gamma = \beta \cdot \widetilde{\mathcal{O}}(\sqrt{nm})$ factor. In particular, if $\beta = 1$, $q = \widetilde{\mathcal{O}}(n)$ and $m = 2n\lceil \log q \rceil$, then the* $(\mathsf{I})\mathsf{SIS}^{\infty}_{n,m,q,1}$ *problems are at least as hard as* $\mathsf{SIVP}_{\widetilde{\mathcal{O}}(n)}$*.*

Definition 2. *The* $\mathsf{LWE}_{n,q,\chi}$ *problem is: Given a random vector $\mathbf{s} \in \mathbb{Z}_q^n$, a probability distribution χ over $\mathbb{Z}$, let $\mathcal{A}_{\mathbf{s},\chi}$ be the distribution obtained by sampling a matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, a vector $\mathbf{e} \xleftarrow{\$} \chi^m$, and outputting a tuple $(\mathbf{A}, \mathbf{A}^\top\mathbf{s} + \mathbf{e})$, to distinguish $\mathcal{A}_{\mathbf{s},\chi}$ and a uniform distribution $\mathcal{U}$ over $\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$.*

Let $\beta \geq \sqrt{n}\cdot\omega(\log n)$, if q is a prime power, and χ is a β-bounded distribution (e,g., $\chi = \mathcal{D}_{\mathbb{Z}^m,s}$), then the $\mathsf{LWE}_{n,q,\chi}$ *problem is as least as hard as* $\mathsf{SIVP}_{\widetilde{\mathcal{O}}(nq/\beta)}$*.*

Lemma 4 **([1]).** *Let $\mathbf{R}$ be an $m\times m$-matrix chosen at random from $\{-1, 1\}^{m\times m}$, for vectors $\mathbf{e} \in \mathbb{R}^m$, $\Pr[\|\mathbf{R} \cdot \mathbf{e}\|_\infty > \|\mathbf{e}\|_\infty \cdot \omega(\sqrt{\log m})] < \mathsf{negl}(m)$.*

Lemma 5 **([1]).** *Let $q \geq 3$, and $m > n$, $\boldsymbol{A}$, $\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}$ and a real $s \geq \|\widetilde{\boldsymbol{R_B}}\| \cdot \sqrt{m} \cdot \omega(\log m)$. There is a* PPT *algorithm* $\mathit{SampleRight}(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{R}, \boldsymbol{R_B}, \boldsymbol{u}, s)$ *that given a trapdoor $\mathbf{R_B}$ for $\Lambda_q^{\perp}(\mathbf{B})$, a low-norm matrix $\mathbf{R} \in \{-1, 1\}^{m\times m}$, and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, outputs $\mathbf{e} \in \mathbb{Z}^{2m}$ distributed statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}([\mathbf{A}|\mathbf{AR}+\mathbf{B}]),s}$.*

3 Preparations

3.1 The Improved of Identity-Encoding Technique

For an improved of identity-encoding technique, a public random vector $\mathbf{u} \in \mathbb{Z}_q^n$ is required, i.e., $\mathsf{Gpk} = (\mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{A}_3^3, \mathbf{u})$, furthermore, the secret-key of i is not yet a trapdoor basis matrix for $\Lambda_q^{\perp}(\mathbf{A}_i)$, instead of a short $2m$-dimensional vector $\mathbf{e}_i = (\mathbf{e}_{i,1}, \mathbf{e}_{i,2})$ in the coset of $\Lambda_q^{\perp}(\mathbf{A}_i)$, i.e., $\Lambda_q^{\mathbf{u}}(\mathbf{A}_i) = \{\mathbf{e}_i \in \mathbb{Z}^{2m} \mid \mathbf{A}_i \cdot \mathbf{e}_i = \mathbf{u} \bmod q\}$, and thus, the revocation token of i is constructed by $\mathbf{A}_0$ and the first part of its secret-key, i.e., $\mathsf{grt}_i = \mathbf{A}_0 \cdot \mathbf{e}_{i,1} \bmod q$.

In order to design an efficient Stern-type ZKAoK protocol corresponding to the above new variant, we transform $\mathbf{A}_i = [\mathbf{A}_0 | \mathbf{A}_1^1 + i\mathbf{A}_2^2]$ corresponding to i to a new form. Before we do that, we first define 2 notations (we restate, in this paper, the group is of $N = 2^\ell$ members):

- $\mathbf{g}_\ell = (1, 2, \cdots, 2^{\ell-1})$: a power-of-2 vector, for $i \in \{1, 2, \cdots, N\}$, $i = \mathbf{g}_\ell^\top \cdot \mathsf{bin}(i)$ where $\mathsf{bin}(i) \in \{0,1\}^\ell$ denotes a binary representation of i.
- $\otimes$: a concatenation with vectors or matrices, given $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{e}' \in \mathbb{Z}_q^m$, and $\mathbf{e} = (e_1, e_2, \cdots, e_\ell) \in \mathbb{Z}_q^\ell$, define: $\mathbf{e} \otimes \mathbf{e}' = (e_1\mathbf{e}', e_2\mathbf{e}', \cdots, e_\ell\mathbf{e}') \in \mathbb{Z}_q^{m\ell}$, $\mathbf{e} \otimes \mathbf{A} = [e_1\mathbf{A} | e_2\mathbf{A} | \cdots | e_\ell\mathbf{A}] \in \mathbb{Z}_q^{n \times m\ell}$.

Next, we transform $\mathbf{A}_i$ to a public matrix $\mathbf{A}'$ that is independent of the index i, where $\mathbf{A}' = [\mathbf{A}_0 | \mathbf{A}_1^1 | \mathbf{A}_2^2 | 2\mathbf{A}_2^2 | \cdots | 2^{\ell-1}\mathbf{A}_2^2] = [\mathbf{A}_0 | \mathbf{A}_1^1 | \mathbf{g}_\ell \otimes \mathbf{A}_2^2] \in \mathbb{Z}_q^{n \times (\ell+2)m}$.

As a corresponding change to the group secret-key of member i, $\mathbf{e}_i = (\mathbf{e}_{i,1}, \mathbf{e}_{i,2})$ is now transformed to $\mathbf{e}_i'$, a vector with some special structure as for $\mathbf{e}_i$, that is, $\mathbf{e}_i' = (\mathbf{e}_{i,1}, \mathbf{e}_{i,2}, \mathsf{bin}(i) \otimes \mathbf{e}_{i,2}) \in \mathbb{Z}^{(\ell+2)m}$.

Thus, from the above transformations, the relation $\mathbf{A}_i \cdot \mathbf{e}_i = \mathbf{u} \bmod q$ is now transformed to a new form, (i) $\mathbf{A}_i \cdot \mathbf{e}_i = \mathbf{A}' \cdot \mathbf{e}_i' = \mathbf{u} \bmod q$.

For the revocation mechanism, as it was stated in [22], due to a flaw in the revocation mechanism of [18], a corrected technique which realizes revocation by binding signer's token grt_i to an LWE function was proposed, (ii) $\mathbf{b} = \mathbf{B}^\top \mathsf{grt}_i + \mathbf{e}_0 = (\mathbf{B}^\top \mathbf{A}_0) \cdot \mathbf{e}_{i,1} + \mathbf{e}_0 \bmod q$, where $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$ is a uniformly random matrix from a random oracle, $\mathbf{e}_0 \in \mathbb{Z}^m$ is sampled from the LWE error χ^m.

For the explicit traceability mechanism, as it was shown in [24], the lattice-based dual LWE cryptosystem [12] can be used to encrypt the identity index of signer i. In our construction, the string $\mathsf{bin}(i) \in \{0,1\}^\ell$ is treated as the plaintext and the ciphertext can be expressed as $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$, where $\mathbf{c}_1 = \mathbf{A}_3^{3\top}\mathbf{s} + \mathbf{e}_1 \bmod q$, $\mathbf{c}_2 = \mathbf{G}^\top \mathbf{s} + \mathbf{e}_2 + \lfloor q/2 \rfloor \mathsf{bin}(i) \bmod q$). Here, $\mathbf{G} \in \mathbb{Z}_q^{n \times \ell}$ is a random matrix, and $\mathbf{s}$, $\mathbf{e}_1$, $\mathbf{e}_2$ are random vectors sampled from the LWE error χ^n, χ^m, χ^ℓ, respectively. Thus, the above relation can be expressed as (iii) $\mathbf{c} = \mathbf{P} \cdot \mathbf{e} + (\mathbf{0}^m, \lfloor q/2 \rfloor \mathsf{bin}(i))$, where $\mathbf{P} = \left(\begin{array}{c|c} \mathbf{A}_3^{3\top} & \\ \cdots\cdots & \mathbf{I}_{m+\ell} \\ \mathbf{G}^\top & \end{array} \right) \in \mathbb{Z}_q^{(m+\ell) \times (n+m+\ell)}$ and $\mathbf{e} = (\mathbf{s}, \mathbf{e}_1, \mathbf{e}_2) \in \mathbb{Z}^{n+m+\ell}$.

Putting all the above transformations ideas and the versatility of the Stern-extension argument system introduced by Ling et al. [23] together, we can construct an efficient Stern-type statistical ZKAoK protocol to prove the above new relations (i), (ii) and (iii).

3.2 A New Stern-Type Zero-Knowledge Proof Protocol

An efficient Stern-type ZKAoK protocol which allows $\mathcal{P}$ to convince any verifier $\mathcal{V}$ that $\mathcal{P}$ is a group member who signed M will be introduced, namely, $\mathcal{P}$ owns a valid secret-key, his/her token is correctly embedded into an LWE instance and the identity information is correctly hidden with the dual LWE cryptosystem.

Firstly, we recall some specific sets and techniques as in [17,18,22] that will be used in our VLR-ET construction. Due to the limited space, we give them in the full version and the readers can also refer to [17,18,22].

Secondly, we introduce the main building block, a new Stern-type interactive statistical zero-knowledge proof protocol, and we consider the group of $N = 2^\ell$ members and each member is identified by $\mathsf{id} = (d_1, d_2, \cdots, d_\ell) \in \{0,1\}^\ell$ which is a binary representation of the index $i \in \{1, 2, \cdots, N\}$, namely, $\mathsf{id} = \mathsf{bin}(i) \in \{0,1\}^\ell$. The underlying new Stern-type statistical ZKAoK protocol between $\mathcal{P}$ and $\mathcal{V}$ can be summarized as follows:

1. The public inputs include $\mathbf{A}' = [\mathbf{A}_0|\mathbf{A}_1^1|\mathbf{g}_\ell \otimes \mathbf{A}_2^2] \in \mathbb{Z}_q^{n\times(\ell+2)m}$, $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{P} = \left(\begin{array}{c|c} \mathbf{A}_3^{3\top} & \\ \cdots\cdots & \mathbf{I}_{m+\ell} \\ \mathbf{G}^\top & \end{array}\right) \in \mathbb{Z}_q^{(m+\ell)\times(n+m+\ell)}$, $\mathbf{u} \in \mathbb{Z}_q^n$, $\mathbf{b} \in \mathbb{Z}_q^m$, $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$.
2. $\mathcal{P}$'s witnesses include $\mathbf{e}' = (\mathbf{e}_1', \mathbf{e}_2', \mathsf{bin}(i) \otimes \mathbf{e}_2') \in \mathsf{Sec}_\beta(\mathsf{id})$ corresponding to a secret index $i \in \{1, \cdots, N\}$ and 4 short vectors $\mathbf{e}_0$, $\mathbf{s}$, $\mathbf{e}_1$, $\mathbf{e}_2$, the LWE errors.
3. $\mathcal{P}$'s goal is to convince $\mathcal{V}$ in zero-knowledge that:
   a. $\mathbf{A}' \cdot \mathbf{e}' = \mathbf{u} \bmod q$ where $\mathbf{e}' \in \mathsf{Sec}_\beta(\mathsf{id})$, while keeping id secret.
   b. $\mathbf{b} = (\mathbf{B}^\top \mathbf{A}_0) \cdot \mathbf{e}_1' + \mathbf{e}_0 \bmod q$ where $0 < \|\mathbf{e}_1'\|_\infty, \|\mathbf{e}_0\|_\infty \le \beta$.
   c. $\mathbf{c} = \mathbf{P}\mathbf{e} + (\mathbf{0}^m, \lfloor q/2 \rfloor \mathsf{bin}(i)) \bmod q$, where $\mathbf{e} = (\mathbf{s}, \mathbf{e}_1, \mathbf{e}_2)$, $0 < \|\mathbf{e}\|_\infty \le \beta$, while keeping $\mathsf{bin}(i) \in \{0,1\}^\ell$ secret.

Firstly, we sketch Group Membership Mechanism, i.e., $\mathcal{P}$ is a certified member and its goal is shown in a. $\mathcal{P}$ does as follows:

1. Parse $\mathbf{A}' = [\mathbf{A}_0|\mathbf{A}_1^1|\mathbf{A}_2^2|\cdots|2^{\ell-1}\mathbf{A}_2^2]$, use Matrix-Ext technique to extend it to $\mathbf{A}^* = [\mathbf{A}_0|\mathbf{0}^{n\times 2m}|\mathbf{A}_1^1|\mathbf{0}^{n\times 2m}|\cdots|2^{\ell-1}\mathbf{A}_2^2|\mathbf{0}^{n\times 2m}|\mathbf{0}^{n\times 3m\ell}]$.
2. Parse $\mathsf{id} = \mathsf{bin}(i) = (d_1, d_2, \cdots, d_\ell)$, extend it to $\mathsf{id}^* = (d_1, d_2, \cdots, d_{2\ell}) \in \mathsf{B}_{2\ell}$.
3. Parse $\mathbf{e}' = (\mathbf{e}_1', \mathbf{e}_2', \mathsf{bin}(i) \otimes \mathbf{e}_2') = (\mathbf{e}_1', \mathbf{e}_2', d_1\mathbf{e}_2', d_2\mathbf{e}_2', \cdots, d_\ell\mathbf{e}_2')$, use Dec, Ext techniques extending $\mathbf{e}_1'$ and $\mathbf{e}_2'$ to k vectors $\mathbf{e}_{1,1}', \mathbf{e}_{1,2}', \cdots, \mathbf{e}_{1,k}' \in \mathsf{B}_{3m}$, and k vectors $\mathbf{e}_{2,1}', \mathbf{e}_{2,2}', \cdots, \mathbf{e}_{2,k}' \in \mathsf{B}_{3m}$. For each $j \in \{1, 2, \cdots, k\}$, we define $\mathbf{e}_j' = (\mathbf{e}_{1,j}', \mathbf{e}_{2,j}', d_1\mathbf{e}_{2,j}', d_2\mathbf{e}_{2,j}', \cdots, d_{2\ell}\mathbf{e}_{2,j}')$, it can be checked that $\mathbf{e}_j' \in \mathsf{SecExt}(\mathsf{id}^*)$.

So $\mathcal{P}$'s goal in a is transformed to: $\mathbf{A}^*(\sum_{j=1}^k \beta_j \mathbf{e}_j') = \mathbf{u} \bmod q$, $\mathbf{e}_j' \in \mathsf{SecExt}(\mathsf{id}^*)$. To prove this new structure in zero-knowledge, we take 2 steps as follows:

1. Pick k random vectors $\mathbf{r}_1', \cdots, \mathbf{r}_k' \xleftarrow{\$} \mathbb{Z}_q^{(2\ell+2)3m}$ to mask $\mathbf{e}_1', \cdots, \mathbf{e}_k'$, then it can be checked that, $\mathbf{A}^* \cdot (\sum_{j=1}^k \beta_j(\mathbf{e}_j' + \mathbf{r}_j')) - \mathbf{u} = \mathbf{A}^* \cdot (\sum_{j=1}^k \beta_j \mathbf{r}_j') \bmod q$.
2. Pick two permutations π, $\varphi \in \mathcal{S}_{3m}$, one permutation $\tau \in \mathcal{S}_{2\ell}$, then it can be checked that, $\forall j \in \{1, 2, \cdots, k\}$, $\mathcal{T}_{\pi,\varphi,\tau}(\mathbf{e}_j') \in \mathsf{SecExt}(\tau(\mathsf{id}^*))$, where $\mathsf{id}^* \in \mathsf{B}_{2\ell}$ is an extension of $\mathsf{id} = \mathsf{bin}(i) \in \{0,1\}^\ell$.

Secondly, we sketch $\mathsf{Revocation\ Mechanism}$, i.e., $\mathcal{P}$'s revocation token is correctly embedded in an LWE instance and its goal is shown in b. $\mathcal{P}$ does as follows:

1. Let $\mathbf{B}' = \mathbf{B}^\top \mathbf{A}_0 \bmod q \in \mathbb{Z}_q^{m \times m}$, and $\mathbf{e}'_{j,0} = \mathsf{Parse}(\mathbf{e}'_j, 1, m)$.
2. Parse $\mathbf{e}_0 = (e_1, e_2, \cdots, e_m) \in \mathbb{Z}^m$, use Dec, Ext techniques to extend $\mathbf{e}_0$ to k vectors $\mathbf{e}_1^0, \mathbf{e}_2^0, \cdots, \mathbf{e}_k^0 \in \mathsf{B}_{3m}$.
3. Let $\mathbf{B}^* = [\mathbf{B}'|\mathbf{I}^*]$ where $\mathbf{I}^* = [\mathbf{I}_m|\mathbf{0}^{n\times 2m}]$, $\mathbf{I}_m$ is identity matrix of order m.

So $\mathcal{P}$'s goal in b is transformed to: $\mathbf{b} = \mathbf{B}'(\sum_{j=1}^k \beta_j \mathbf{e}'_{j,0}) + \mathbf{I}^*(\sum_{j=1}^k \beta_j \mathbf{e}_j^0) = \mathbf{B}^* \cdot (\sum_{j=1}^k \beta_j(\mathbf{e}'_{j,0}, \mathbf{e}_j^0)) \bmod q$, $\mathbf{e}_j^0 \in \mathsf{B}_{3m}$. To prove this new structure in zero-knowledge, we take 2 steps as follows:

1. Let $\mathbf{r}'_{j,0} = \mathsf{Parse}(\mathbf{r}'_j, 1, m)$, pick k random vectors $\mathbf{r}_1, \cdots, \mathbf{r}_k \xleftarrow{\$} \mathbb{Z}_q^{3m}$ to mask $\mathbf{e}_1^0, \cdots, \mathbf{e}_k^0$, it can be checked that,

$$\mathbf{B}^* \cdot (\textstyle\sum_{j=1}^k \beta_j(\mathbf{e}'_{j,0} + \mathbf{r}'_{j,0}, \mathbf{e}_j^0 + \mathbf{r}_j)) - \mathbf{b} = \mathbf{B}^* \cdot (\sum_{j=1}^k \beta_j(\mathbf{r}'_{j,0}, \mathbf{r}_j)) \bmod q$$

2. Pick $\phi \in \mathcal{S}_{3m}$, then it can be checked that, $\forall j \in \{1, 2, \cdots, k\}$, $\phi(\mathbf{e}_j^0) \in \mathsf{B}_{3m}$.

Thirdly, we sketch $\mathsf{Explicit\ Traceability\ Mechanism}$, i.e., $\mathcal{P}$'s index is correctly embedded in a LWE cryptosystem and its goal is shown in c. $\mathcal{P}$ does as follows:

1. Let $\mathbf{P}^* = [\mathbf{P}|\mathbf{0}^{(m+\ell)\times 2(n+m+\ell)}]$ and $\mathbf{Q} = \left(\begin{array}{c|c} \mathbf{0}^{m\times\ell} & \mathbf{0}^{m\times\ell} \\ \cdots\cdots & \cdots\cdots \\ \lfloor q/2 \rfloor \mathbf{I}_\ell & \mathbf{0}^{\ell\times\ell} \end{array}\right)$, where $\mathbf{I}_\ell$ is an identity matrix of order ℓ.
2. Parse $\mathbf{e} = (\mathbf{s}, \mathbf{e}_1, \mathbf{e}_2) \in \mathbb{Z}^{n+m+\ell}$, use Dec, Ext techniques to extend $\mathbf{e}$ to k vectors $\mathbf{e}^{(1)}, \mathbf{e}^{(2)}, \cdots, \mathbf{e}^{(k)} \in \mathsf{B}_{3(n+m+\ell)}$.
3. Let $\mathsf{id}^* = \mathsf{bin}(i)^* \in \mathsf{B}_{2\ell}$ be an extension of $\mathsf{id} = \mathsf{bin}(i) \in \{0,1\}^\ell$.

So $\mathcal{P}$'s goal in c is transformed to: $\mathbf{c} = \mathbf{P}^* \cdot (\sum_{j=1}^k \beta_j \mathbf{e}^{(j)}) + \mathbf{Q} \cdot \mathsf{id}^* \bmod q$, $\mathbf{e}^{(j)} \in \mathsf{B}_{3(n+m+\ell)}$, $\mathsf{bin}(i)^* \in \mathsf{B}_{2\ell}$. To prove this new structure in zero-knowledge, we take 2 steps as follows:

1. Pick a random vector $\mathbf{r}_{\mathsf{id}^*} \xleftarrow{\$} \mathbb{Z}_q^{2\ell}$ to mask $\mathsf{id}^* = \mathsf{bin}(i)^*$, k random vectors $\mathbf{r}''_1, \cdots, \mathbf{r}''_k \xleftarrow{\$} \mathbb{Z}_q^{3(n+m+\ell)}$ to mask $\mathbf{e}^{(1)}, \cdots, \mathbf{e}^{(k)}$, it can be checked that,

$$\mathbf{P}^* \cdot (\textstyle\sum_{j=1}^k \beta_j(\mathbf{e}^{(j)} + \mathbf{r}''_j)) + \mathbf{Q} \cdot (\mathsf{id}^* + \mathbf{r}_{\mathsf{id}^*}) - \mathbf{c} = \mathbf{P}^* \cdot (\sum_{j=1}^k \beta_j \mathbf{r}''_j) + \mathbf{Q} \cdot \mathbf{r}_{\mathsf{id}^*} \bmod q$$

2. Pick $\rho \in \mathcal{S}_{3(n+m+\ell)}$, then it can be checked that, $\forall j \in \{1, 2, \cdots, k\}$, $\rho(\mathbf{e}^{(j)}) \in \mathsf{B}_{3(n+m+\ell)}$ and $\tau(\mathsf{id}^*) \in \mathsf{B}_{2\ell}$, where τ has been picked in the proof of group membership mechanism.

Putting the above techniques together, we can obtain a new Stern-type interactive statistical zero-knowledge proof protocol, the details will be given bellow.

In our $\mathsf{VLR\text{-}ET}$ construction, we utilize a statistically hiding, computationally blinding commitment scheme (COM) as proposed in [15]. For simplicity, we omit the randomness of COM. $\mathcal{P}$ and $\mathcal{V}$ interact as follows:

1. Commitments: $\mathcal{P}$ randomly samples the following random objects:

$$\begin{cases} \mathbf{r}'_1, \cdots, \mathbf{r}'_k \xleftarrow{\$} \mathbb{Z}_q^{(2\ell+2)3m};\ \mathbf{r}_1, \cdots, \mathbf{r}_k \xleftarrow{\$} \mathbb{Z}_q^{3m};\ \mathbf{r}''_1, \cdots, \mathbf{r}''_k \xleftarrow{\$} \mathbb{Z}_q^{3(n+m+\ell)}; \\ \pi_1, \cdots, \pi_k \xleftarrow{\$} \mathcal{S}_{3m};\ \varphi_1, \cdots, \varphi_k \xleftarrow{\$} \mathcal{S}_{3m};\ \phi_1, \cdots, \phi_k \xleftarrow{\$} \mathcal{S}_{3m}; \\ \rho_1, \cdots, \rho_k \xleftarrow{\$} \mathcal{S}_{3(n+m+\ell)};\ \tau \xleftarrow{\$} \mathcal{S}_{2\ell};\ \mathbf{r}_{\mathsf{id}^*} \xleftarrow{\$} \mathbb{Z}_q^{2\ell}. \end{cases}$$

Let $\mathbf{r}'_{j,0} = \mathsf{Parse}(\mathbf{r}'_j, 1, m)$, $j \in \{1, \cdots, k\}$, $\mathcal{P}$ sends $\mathsf{CMT} = (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$ to $\mathcal{V}$,

$$\begin{cases} \mathbf{c}_1 = \mathsf{COM}(\{\pi_j, \varphi_j, \phi_j, \rho_j\}_{j=1}^k, \tau, \mathbf{A}^* \cdot (\sum_{j=1}^k \beta_j \mathbf{r}'_j), \mathbf{B}^* \cdot (\sum_{j=1}^k \beta_j (\mathbf{r}'_{j,0}, \mathbf{r}_j)), \\ \qquad\qquad \mathbf{P}^* \cdot (\sum_{j=1}^k \beta_j \mathbf{r}''_j) + \mathbf{Q} \cdot \mathbf{r}_{\mathsf{id}^*}), \\ \mathbf{c}_2 = \mathsf{COM}(\{\mathcal{T}_{\pi_j, \varphi_j, \tau}(\mathbf{r}'_j), \phi_j(\mathbf{r}_j), \rho_j(\mathbf{r}''_j)\}_{j=1}^k, \tau(\mathbf{r}_{\mathsf{id}^*})), \\ \mathbf{c}_3 = \mathsf{COM}(\{\mathcal{T}_{\pi_j, \varphi_j, \tau}(\mathbf{e}'_j + \mathbf{r}'_j), \phi_j(\mathbf{e}_j^0 + \mathbf{r}_j), \rho_j(\mathbf{e}^{(j)} + \mathbf{r}''_j)\}_{j=1}^k, \tau(\mathsf{id}^* + \mathbf{r}_{\mathsf{id}^*})). \end{cases}$$

2. Challenge: $\mathcal{V}$ chooses a challenge $\mathsf{CH} \xleftarrow{\$} \{1, 2, 3\}$ and sends it to $\mathcal{P}$.
3. Response: Depending on CH, $\mathcal{P}$ replies as follows:
   - $\mathsf{CH} = 1$. For $j \in \{1, 2, \cdots, k\}$, let $\mathbf{v}'_j = \mathcal{T}_{\pi_j, \varphi_j, \tau}(\mathbf{e}'_j)$, $\mathbf{w}'_j = \mathcal{T}_{\pi_j, \varphi_j, \tau}(\mathbf{r}'_j)$, $\mathbf{v}_j = \phi_j(\mathbf{e}_j^0)$, $\mathbf{w}_j = \phi_j(\mathbf{r}_j)$, $\mathbf{v}^{(j)} = \rho_j(\mathbf{e}^{(j)})$, $\mathbf{w}''_j = \rho_j(\mathbf{r}''_j)$, $\mathbf{t}_{\mathsf{id}} = \tau(\mathsf{id}^*)$ and $\mathbf{v}_{\mathsf{id}} = \tau(\mathbf{r}_{\mathsf{id}^*})$, define $\mathsf{RSP} = (\{\mathbf{v}'_j, \mathbf{w}'_j, \mathbf{v}_j, \mathbf{w}_j, \mathbf{v}^{(j)}, \mathbf{w}''_j\}_{j=1}^k, \mathbf{t}_{\mathsf{id}}, \mathbf{v}_{\mathsf{id}})$.
   - $\mathsf{CH} = 2$. For $j \in \{1, 2, \cdots, k\}$, let $\hat{\pi}_j = \pi_j$, $\hat{\varphi}_j = \varphi_j$, $\hat{\phi}_j = \phi_j$, $\hat{\rho}_j = \rho_j$, $\hat{\tau} = \tau$, $\mathbf{x}'_j = \mathbf{e}'_j + \mathbf{r}'_j$, $\mathbf{x}_j = \mathbf{e}_j^0 + \mathbf{r}_j$, $\mathbf{x}''_j = \mathbf{e}^{(j)} + \mathbf{r}''_j$ and $\mathbf{x}_{\mathsf{id}} = \mathsf{id}^* + \mathbf{r}_{\mathsf{id}^*}$, define $\mathsf{RSP} = (\{\hat{\pi}_j, \hat{\varphi}_j, \hat{\phi}_j, \hat{\rho}_j, \mathbf{x}'_j, \mathbf{x}_j, \mathbf{x}''_j\}_{j=1}^k, \hat{\tau}, \mathbf{x}_{\mathsf{id}})$.
   - $\mathsf{CH} = 3$. For $j \in \{1, 2, \cdots, k\}$, let $\tilde{\pi}_j = \pi_j$, $\tilde{\varphi}_j = \varphi_j$, $\tilde{\phi}_j = \phi_j$, $\tilde{\rho}_j = \rho_j$, $\tilde{\tau} = \tau$, $\mathbf{h}'_j = \mathbf{r}'_j$, $\mathbf{h}_j = \mathbf{r}_j$, $\mathbf{h}''_j = \mathbf{r}''_j$ and $\mathbf{h}_{\mathsf{id}} = \mathbf{r}_{\mathsf{id}^*}$, define $\mathsf{RSP} = (\{\tilde{\pi}_j, \tilde{\varphi}_j, \tilde{\phi}_j, \tilde{\rho}_j, \mathbf{h}'_j, \mathbf{h}_j, \mathbf{h}''_j\}_{j=1}^k, \tilde{\tau}, \mathbf{h}_{\mathsf{id}})$.
4. Verification: Receiving RSP, $\mathcal{V}$ checks as follows:
   - $\mathsf{CH} = 1$. Check that $\mathbf{t}_{\mathsf{id}} \in \mathsf{B}_{2\ell}$, for each $j \in \{1, 2, \cdots, k\}$, $\mathbf{v}'_j \in \mathsf{SecExt}(\mathbf{t}_{\mathsf{id}})$, $\mathbf{v}_j \in \mathsf{B}_{3m}$, $\mathbf{v}^{(j)} \in \mathsf{B}_{3(n+m+\ell)}$, and that,

$$\begin{cases} \mathbf{c}_2 = \mathsf{COM}(\{\mathbf{w}'_j, \mathbf{w}_j, \mathbf{w}''_j\}_{j=1}^k, \mathbf{t}_{\mathsf{id}}), \\ \mathbf{c}_3 = \mathsf{COM}(\{\mathbf{v}'_j + \mathbf{w}'_j, \mathbf{v}_j + \mathbf{w}_j, \mathbf{v}^{(j)} + \mathbf{w}''_j\}_{j=1}^k, \mathbf{t}_{\mathsf{id}} + \mathbf{v}_{\mathsf{id}}). \end{cases}$$

   - $\mathsf{CH} = 2$. For $j \in \{1, 2, \cdots, k\}$, let $\mathbf{x}'_{j,0} = \mathsf{Parse}(\mathbf{x}'_j, 1, m)$, and check that,

$$\begin{cases} \mathbf{c}_1 = \mathsf{COM}(\{\hat{\pi}_j, \hat{\varphi}_j, \hat{\phi}_j, \hat{\rho}_j\}_{j=1}^k, \hat{\tau}, \mathbf{A}^* \cdot (\sum_{j=1}^k \beta_j \mathbf{x}'_j) - \mathbf{u}, \\ \qquad \mathbf{B}^* \cdot (\sum_{j=1}^k \beta_j (\mathbf{x}'_{j,0}, \mathbf{x}_j) - \mathbf{b}), \mathbf{P}^* \cdot (\sum_{j=1}^k \beta_j \mathbf{x}''_j) + \mathbf{Q}^* \cdot \mathbf{x}_{\mathsf{id}} - \mathbf{c}), \\ \mathbf{c}_3 = \mathsf{COM}(\{\mathcal{T}_{\hat{\pi}_j, \hat{\varphi}_j, \hat{\tau}}(\mathbf{x}'_j), \hat{\phi}_j(\mathbf{x}_j), \hat{\rho}_j(\mathbf{x}''_j)\}_{j=1}^k, \hat{\tau}(\mathbf{x}_{\mathsf{id}})). \end{cases}$$

   - $\mathsf{CH} = 3$. For $j \in \{1, 2, \cdots, k\}$, let $\mathbf{h}'_{j,0} = \mathsf{Parse}(\mathbf{h}'_j, 1, m)$, and check that,

$$\begin{cases} \mathbf{c}_1 = \mathsf{COM}(\{\tilde{\pi}_j, \tilde{\varphi}_j, \tilde{\phi}_j, \tilde{\rho}_j\}_{j=1}^k, \tilde{\tau}, \mathbf{A}^* \cdot (\sum_{j=1}^k \beta_j \mathbf{h}'_j), \\ \qquad\qquad \mathbf{B}^* \cdot (\sum_{j=1}^k \beta_j (\mathbf{h}'_{j,0}, \mathbf{h}_j)), \mathbf{P}^* \cdot (\sum_{j=1}^k \beta_j \mathbf{h}''_j) + \boldsymbol{Q}^* \cdot \mathbf{h}_{\mathsf{id}}), \\ \mathbf{c}_2 = \mathsf{COM}(\{\mathcal{T}_{\tilde{\pi}_j, \tilde{\varphi}_j, \tilde{\tau}}(\mathbf{h}'_j), \tilde{\phi}_j(\mathbf{h}_j), \tilde{\rho}_j(\mathbf{h}''_j)\}_{j=1}^k, \tilde{\tau}(\mathbf{h}_{\mathsf{id}})). \end{cases}$$

The verifier $\mathcal{V}$ outputs 1 iff all the above conditions hold, otherwise 0.

The associated relation $\mathcal{R}(n, k, \ell, q, m, \beta)$ in the above protocol is defined as:

$$\mathcal{R} = \left\{ \begin{array}{l} \mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{B} \in \mathbb{Z}_q^{n\times m}, \mathbf{P} \in \mathbb{Z}_q^{(m+\ell)\times(n+m+\ell)}, \mathbf{u} \in \mathbb{Z}_q^n, \mathbf{b} \in \mathbb{Z}_q^m, \\ \mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^\ell, \mathsf{id} = \mathsf{bin}(i) \in \{0,1\}^\ell, \mathbf{e}_0 \in \mathbb{Z}^m, \\ \mathbf{e}' = (\mathbf{e}_1', \mathbf{e}_2', \mathsf{bin}(i) \otimes \mathbf{e}_2') \in \mathsf{Sec}_\beta(\mathsf{id}), \mathbf{e} \in \mathbb{Z}^{n+m+\ell};\ s.t. \\ 0 < \|\mathbf{e}'\|_\infty, \|\mathbf{e}_0\|_\infty, \|\mathbf{e}\|_\infty \le \beta, \mathbf{c} = \mathbf{P}\mathbf{e} + (\mathbf{0}^m, \lfloor q/2 \rfloor \mathsf{id}) \bmod q, \\ \mathbf{b} = (\mathbf{B}^\top \mathbf{A}_0) \cdot \mathbf{e}_1' + \mathbf{e}_0 \bmod q, [\mathbf{A}_0 | \mathbf{A}_1^1 | \mathbf{g}_\ell \otimes \mathbf{A}_2^2] \cdot \mathbf{e}' = \mathbf{u} \bmod q. \end{array} \right\}$$

3.3 Analysis of the Protocol

The following theorem gives a detailed analysis of the above interactive protocol.

Theorem 1. *Let* COM *(as proposed in [15]) be a statistically hiding and computationally binding commitment scheme, for a given commitment* CMT*, 3 valid responses* RSP_1*,* RSP_2 *and* RSP_3 *with respect to 3 different challenges* CH_1*,* CH_2 *and* CH_3*, the proposed protocol is a statistical zero-knowledge argument of knowledge for* $\mathcal{R}(n, k, \ell, q, m, \beta)$*, where each round has perfect completeness, soundness error* $2/3$*, argument of knowledge property and communication cost* $\widetilde{\mathcal{O}}(\ell n \log \beta)$*.*

Proof. The proof employs a list of standard techniques for Stern-type protocol as in [15,18,23]. Due to the limited space, the proof is presented in the full version.

4 The Lattice-Based GS-VLR-ET Scheme

4.1 Description of the Scheme

– $\mathsf{KeyGen}(1^n, N)$: On input security parameter n, group size $N = 2^\ell = \mathsf{poly}(n)$. The prime modulus $q = \omega(n^2 \log n) > N$, dimension $m = 2n\lceil \log q \rceil$, Gaussian parameter $s = \omega(\sqrt{n \log q \log n})$, and the norm bound $\beta = \lceil s \cdot \log m \rceil$ such that $(4\beta + 1)^2 \le q$. This algorithm specifies the following steps:

1. Run $\mathsf{TrapGen}(q, n, m)$ to generate $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times m}$ and a trapdoor $\mathbf{R}_{\mathbf{A}_0}$.
2. Sample two matrices $\mathbf{A}_1^1, \mathbf{A}_2^2 \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ and a vector $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$.
3. Run $\mathsf{TrapGen}(q, n, m)$ to generate $\mathbf{A}_3^3 \in \mathbb{Z}_q^{n\times m}$ and a trapdoor $\mathbf{R}_{\mathbf{A}_3^3}$.
4. As in [31], for group member with index $i \in \{1, 2, \cdots, N\}$, define a matrix $\mathbf{A}_i = [\mathbf{A}_0 | \mathbf{A}_1^1 + i\mathbf{A}_2^2] \in \mathbb{Z}_q^{n\times 2m}$, and do the followings:
   - 4.1. Sample $\mathbf{e}_{i,2} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m, s}$ and let $\mathbf{u}_i = (\mathbf{A}_1^1 + i\mathbf{A}_2^2) \cdot \mathbf{e}_{i,2} \bmod q$. Then run $\mathsf{SamplePre}(\mathbf{A}_0, \mathbf{R}_{\mathbf{A}_0}, \mathbf{u} - \mathbf{u}_i, s)$ to obtain $\mathbf{e}_{i,1} \in \mathbb{Z}^m$.
   - 4.2. Let $\boldsymbol{e}_i = (\boldsymbol{e}_{i,1}, \boldsymbol{e}_{i,2}) \in \mathbb{Z}^{2m}$. Thus $\mathbf{A}_i \cdot \mathbf{e}_i = \mathbf{u} \bmod q$, $0 < \|\mathbf{e}_i\|_\infty \le \beta$.
   - 4.3. Let the member i's group secret-key be $\mathsf{gsk}_i = \mathbf{e}_i$, and its revocation token be $\mathsf{grt}_i = \mathbf{A}_0 \cdot \mathbf{e}_{i,1} \bmod q$.

5. Output $(\mathsf{Gpk}, \mathsf{Gmsk}, \mathsf{Gsk}, \mathsf{Grt})$ where $\mathsf{Gpk} = (\mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{A}_3^3, \mathbf{u})$, $\mathsf{Gmsk} = \mathbf{R}_{\mathbf{A}_3^3}$, $\mathsf{Gsk} = (\mathsf{gsk}_1, \mathsf{gsk}_2, \cdots, \mathsf{gsk}_N)$, $\mathsf{Grt} = (\mathsf{grt}_1, \mathsf{grt}_2, \cdots, \mathsf{grt}_N)$.

– $\mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_i, M)$: Let $\mathcal{H} : \{0,1\}^* \to \{1,2,3\}^{\kappa=\omega(\log n)}$, $\mathcal{G} : \{0,1\}^* \to \mathbb{Z}_q^{n\times m}$ be two hash functions, modeled as random oracles. Let χ be a β-bounded distribution as in Definition 2. On input Gpk and a message $M \in \{0,1\}^*$, the member i with secret-key $\mathsf{gsk}_i = \boldsymbol{e}_i$ specifies the following steps:

1. Sample $\mathbf{v} \xleftarrow{\$} \{0,1\}^n$ and define $\mathbf{B} = \mathcal{G}(\mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{u}, M, \boldsymbol{v}) \in \mathbb{Z}_q^{n\times m}$.
2. Sample $\mathbf{e}_0 \xleftarrow{\$} \chi^m$ and define $\mathbf{b} = \mathbf{B}^\top \mathsf{grt}_i + \mathbf{e}_0 = (\mathbf{B}^\top \mathbf{A}_0) \cdot \mathbf{e}_{i,1} + \mathbf{e}_0 \bmod q$.
3. Sample $\mathbf{G} \xleftarrow{\$} \mathbb{Z}_q^{n\times \ell}$, $\mathbf{s} \xleftarrow{\$} \chi^n$, $\mathbf{e}_1 \xleftarrow{\$} \chi^m$, $\mathbf{e}_2 \xleftarrow{\$} \chi^\ell$, define $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^\ell$ where $\mathbf{c}_1 = \mathbf{A}_3^{3\top}\mathbf{s} + \mathbf{e}_1 \bmod q$, $\mathbf{c}_2 = \mathbf{G}^\top \mathbf{s} + \mathbf{e}_2 + \lfloor q/2 \rfloor \mathsf{bin}(i) \bmod q$,
4. Generate a zero-knowledge proof that the signer is indeed a group member who owns a valid secret-key, and has signed the message $M \in \{0,1\}^*$, and its revocation token is correctly embedded in $\mathbf{b}$, and its identity is correctly embedded in $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$ constructed as above. This can be achieved by repeating $\kappa = \omega(\log n)$ times the Stern-type interactive protocol as in Sect. 3.3 with the public tuple $(\mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{P}, \mathbf{u}, \mathbf{B}, \mathbf{b}, \mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2))$ and a witness $(\mathsf{id}, \mathsf{gsk}_i, \mathbf{e}_0, \mathbf{e})$, then making it non-interactive via the Fiat-Shamir heuristic as a triple $\Pi = (\{\mathsf{CMT}_j\}_{j\in\{1,\cdots,\kappa\}}, \mathsf{CH}, \{\mathsf{RSP}_j\}_{j\in\{1,\cdots,\kappa\}})$ where $\mathsf{CH} = \{\mathsf{CH}_j\}_{j\in\{1,\cdots,\kappa\}} = \mathcal{H}(M, \mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{P}, \mathbf{u}, \mathbf{B}, \mathbf{b}, \mathbf{c}, \{\mathsf{CMT}_j\}_{j\in\{1,\cdots,\kappa\}})$.
5. Output the signature $\Sigma = (M, \Pi, \mathbf{v}, \mathbf{b}, \mathbf{G}, \mathbf{c})$.

– $\mathsf{Verify}(\mathsf{Gpk}, \mathsf{RL}, M, \Sigma)$: On input Gpk, a signature Σ on $M \in \{0,1\}^*$, a set of tokens $\mathsf{RL} = \{\mathsf{grt}_{i'}\}_{i'\leq N} \subseteq \mathsf{Grt}$, the verifier specifies the following steps:

1. Parse the signature $\Sigma = (M, \Pi, \mathbf{v}, \mathbf{b}, \mathbf{G}, \mathbf{c})$.
2. Let $\mathbf{P} = \left(\begin{array}{c|c} \mathbf{A}_3^{3\top} & \\ \cdots\cdots & \mathbf{I}_{m+\ell} \\ \mathbf{G}^\top & \end{array} \right)$, and check that if $\mathsf{CH} = \{\mathsf{CH}_1, \mathsf{CH}_2, \cdots, \mathsf{CH}_\kappa\} = \mathcal{H}(M, \mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{P}, \mathbf{u}, \mathbf{B}, \mathbf{b}, \mathbf{c}, \{\mathsf{CMT}_j\}_{j\in\{1,2,\cdots,\kappa\}})$.
3. For $j \in \{1,2,\cdots,\kappa\}$, run the verification steps of the protocol from Sect. 3.3 to check the validity of RSP_j with respect to CMT_j and CH_j.
4. Let $\mathbf{B} = \mathcal{G}(\mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{u}, M, \mathbf{v}) \in \mathbb{Z}_q^{n\times m}$, and for each $\mathsf{grt}_{i'} \in \mathsf{RL}$, compute $\mathbf{e}_{i'} = \mathbf{b} - \mathbf{B}^\top \mathsf{grt}_{i'} \bmod q$, and check that if $\|\mathbf{e}_{i'}\|_\infty > \beta$.
5. If the above are all satisfied, output 1 and accept Σ, otherwise reject it.

– $\mathsf{Open}(\mathsf{Gpk}, \mathsf{Gmsk}, M, \Sigma)$: On input Gpk, $\mathsf{Gmsk} = \mathbf{R}_{\mathbf{A}_3^3}$, a group signature Σ on $M \in \{0,1\}^*$, the tracing authority specifies the following steps:

1. Parse $\Sigma = (M, \Pi, \mathbf{v}, \mathbf{b}, \mathbf{G}, \mathbf{c})$, in particular, $\mathbf{G} = [\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_\ell]$.
2. For $i \in \{1,2,\cdots,\ell\}$, run $\mathsf{SamplePre}(\mathbf{A}_3, \mathbf{R}_{\mathbf{A}_3^3}, \mathbf{g}_i, s)$ to obtain $\mathbf{f}_i \in \mathbb{Z}^m$, and define $\mathbf{F} = [\mathbf{f}_1, \mathbf{f}_2, \cdots, \mathbf{f}_\ell] \in \mathbb{Z}_q^{m\times \ell}$.
3. Compute $\mathsf{id}' = (d_1', d_2', \cdots, d_\ell') = \mathbf{c}_2 - \mathbf{F}^\top \mathbf{c}_1 \bmod q$. For $i \in \{1,2,\cdots,\ell\}$, if d_i' is closer to 0 than to $\lfloor q/2 \rfloor$, define $d_i = 1$; otherwise, $d_i = 0$.
4. Let $\mathsf{id} = (d_1, d_2, \cdots, d_\ell)$ and output $i = \mathbf{g}_\ell^\top \cdot \mathsf{id}$.

4.2 Analysis of the Scheme

Efficiency and Correctness: For our lattice-based GS-VLR-ET, it only needs 3 public matrices for identity-encoding, and one more matrix for explicit traceability, thus the group public-key has bit-size $\widetilde{\mathcal{O}}(n^2)$, the member secret-key has bit-size $\widetilde{\mathcal{O}}(n)$ and the signature has bit-size $\ell \cdot \widetilde{\mathcal{O}}(n) = \log N \cdot \widetilde{\mathcal{O}}(n)$. Compared with the existing lattice-based GS-VLR constructions, our scheme saves a $\mathcal{O}(\log N)$ factor for both bit-sizes of the group public-key and the member secret-key, meanwhile, supporting the explicit traceability, thus is more suitable for a large group.

Theorem 2. *The proposed scheme is correct with overwhelming probability.*

Proof. To prove that for all Gpk, Gsk, Gmsk, Grt generated by KeyGen, all indexes $i \in \{1, 2, \cdots, N\}$, and all messages $M \in \{0,1\}^*$, the following holds true:

$$\mathsf{Verify}(\mathsf{Gpk}, \mathsf{RL}, \mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_i, M), M) = 1 \Leftrightarrow \mathsf{grt}_i \notin \mathsf{RL}.$$
$$\mathsf{Open}(\mathsf{Gpk}, \mathsf{Gmsk}, \mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_i, M), M) = i.$$

For the first 3 steps of Verify, a member i owning $(\mathbf{e}', \mathbf{e}_0) \in \mathsf{Sec}_\beta(\mathsf{id}) \times \chi^m$ can always generate a signature satisfying them. For step 4, $\mathbf{e}_{i'}$ can be expressed as $\mathbf{e}_{i'} = \mathbf{b} - \mathbf{B}^\top \mathsf{grt}_{i'} = \mathbf{B}^\top \mathsf{grt}_i + \mathbf{e}_0 - \mathbf{B}^\top \mathsf{grt}_{i'} = \mathbf{B}^\top(\mathsf{grt}_i - \mathsf{grt}_{i'}) + \mathbf{e}_0 \bmod q$.

1. To prove that, $\mathsf{grt}_i \notin \mathsf{RL} \Rightarrow \mathsf{Verify}(\mathsf{Gpk}, \mathsf{RL}, \mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_i, M), M) = 1$.
   Assume that $\mathsf{grt}_i \notin \mathsf{RL}$, we prove that, the step 4 is satisfied with overwhelming probability, namely, the infinity norm of vector $\mathbf{e}_{i'}$ is lager than β, and $\mathsf{Verify}(\mathsf{Gpk}, \mathsf{RL}, \mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_i, M), M) = 1$. For all $\mathsf{grt}_{i'} \in \mathsf{RL}$, we have that $\mathbf{B}^\top \cdot (\mathsf{grt}_i - \mathsf{grt}_{i'}) = \mathbf{e}_{i'} - \mathbf{e}_0 \bmod q$.
   Let $\mathbf{s}_{i'} = \mathsf{grt}_i - \mathsf{grt}_{i'}$, we have that $\|\mathbf{B}^\top \mathbf{s}_{i'}\|_\infty \leq \|\mathbf{e}_{i'}\|_\infty + \|\mathbf{e}_0\|_\infty \leq \|\mathbf{e}_{i'}\|_\infty + \beta$. According to Lemma 4 of [22], $\|\mathbf{B}^\top \mathbf{s}_{i'}\|_\infty > 2\beta$ with overwhelming probability, thus $\|\mathbf{e}'_i\|_\infty > 2\beta - \beta = \beta$.
2. To prove that, $\mathsf{Verify}(\mathsf{Gpk}, \mathsf{RL}, \mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_i, M), M) = 1 \Rightarrow \mathsf{grt}_i \notin \mathsf{RL}$.
   Assume that $\mathsf{Verify}(\mathsf{Gpk}, \mathsf{RL}, \mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_i, M), M) = 1$. Thus for all $\mathsf{grt}_{i'} \in \mathsf{RL}$, we have $\|\mathbf{e}_{i'}\|_\infty > \beta$. Therefore, if there is an index i' satisfying $\mathsf{grt}_i = \mathsf{grt}_{i'}$, then we have $\mathbf{e}_{i'} = \mathbf{e}_0$, thus $\|\mathbf{e}_{i'}\|_\infty = \|\mathbf{e}_0\|_\infty \leq \beta$, the signature cannot pass the verification of step 4, therefore, a contradiction appears.
3. To prove that, $\mathsf{Open}(\mathsf{Gpk}, \mathsf{Gmsk}, \mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_i, M), M) = i$ with overwhelming probability.
   We set the parameters so that the lattice-based dual LWE cyrptosystem is correct and a tracing authority owning the trapdoor for $\Lambda_q^\perp(\mathbf{A}_3^3)$ can compute an identity index belonging to the collection $\{1, 2, \cdots, N\}$ effectively, or a special symbol $\perp$ denoting the opening failure, which implies that our Open algorithm is also correct. This concludes the correctness proof.

Theorem 3. *If* COM *(as proposed in [15]) is a statistically hiding commitment scheme, then the proposed scheme is selfless-anonymous in* ROM*.*

Proof. To proof this theorem, we define a list of games as follows:
Game 0. It is the original selfless-anonymity game. $\mathcal{C}$ honestly does as follows:

1. Run KeyGen to obtain Gpk, Gmsk, Gsk, Grt. Set $\mathsf{RL} = \varnothing$, $\mathsf{Corr} = \varnothing$, and send Gpk to adversary $\mathcal{A}$.
2. If $\mathcal{A}$ queries the group secret-key of member i, $\mathcal{C}$ sets $\mathsf{Corr} = \mathsf{Corr} \cup \{i\}$ and returns gsk_i; if $\mathcal{A}$ queries the group signature on $M \in \{0,1\}^*$ of member i, $\mathcal{C}$ returns $\Sigma \leftarrow \mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_i, M)$; if $\mathcal{A}$ queries the revocation token of member i, $\mathcal{C}$ sets $\mathsf{RL} = \mathsf{RL} \cup \{\mathsf{grt}_i\}$ and returns it to $\mathcal{A}$.
3. $\mathcal{A}$ outputs a message $M^* \in \{0,1\}^*$, two members i_0 and i_1, and for each $b \in \{0,1\}$, $i_b \notin \mathsf{Corr}$ and $\mathsf{grt}_{i_b} \notin \mathsf{RL}$.
4. $\mathcal{C}$ chooses $b \xleftarrow{\$} \{0,1\}$, and generates a valid $\mathsf{VLR\text{-}ET}$ group signature, $\Sigma^* = \mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_{i_b}, M^*) = (M^*, \Pi, \mathbf{v}, \mathbf{b}, \mathbf{G}, \mathbf{c})$ and returns it to $\mathcal{A}$.
5. $\mathcal{A}$ can make queries as before, but it is not allowed to ask for gsk_{i_b} or grt_{i_b} for each $b \in \{0,1\}$.
6. Finally, $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$.

$\mathsf{Game\ 1}$: $\mathcal{C}$ does the same as that in $\mathsf{Game\ 0}$, except that it simulates the signature generation in step 4 of $\mathsf{Game\ 0}$ by programming the random oracle:

1. For the first 2 steps of algorithm Sign, work in the honest process, namely, sample $\mathbf{v} \xleftarrow{\$} \{0,1\}^n$, $\mathbf{e}_0, \mathbf{e}_1 \xleftarrow{\$} \chi^m$, $\mathbf{G} \xleftarrow{\$} \mathbb{Z}_q^{n\times\ell}$, $\mathbf{s} \xleftarrow{\$} \chi^n$, $\mathbf{e}_2 \xleftarrow{\$} \chi^\ell$. Let $\mathbf{B} = \mathcal{G}(\mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{u}, M, \mathbf{v})$, $\mathbf{b} = \mathbf{B}^\top \mathsf{grt}_{i_b} + \mathbf{e}_0 \bmod q$, and $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$, where $\mathbf{c}_1 = \mathbf{A}_3^{3\top}\mathbf{s} + \mathbf{e}_1 \bmod q$, $\mathbf{c}_2 = \mathbf{G}^\top \mathbf{s} + \mathbf{e}_2 + \lfloor q/2 \rfloor \mathsf{bin}(i) \bmod q$.
2. The simulation algorithm does as in the proof of Theorem 1 and will be repeated $\kappa = \omega(\log n)$ times. $\mathcal{C}$ programs the random oracle $\mathcal{H}(M^*, \mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{P}, \mathbf{u}, \mathbf{B}, \mathbf{b}, \mathbf{c}, \mathsf{CMT}_1, \cdots, \mathsf{CMT}_\kappa) = (\mathsf{CH}_1, \cdots, \mathsf{CH}_\kappa)$ and due to the statistically zero-knowledge of underlying argument of knowledge, the distribution of Π^* is statistically close to Π.
3. Finally, $\mathcal{C}$ outputs the simulated signature $\widehat{\Sigma}^* = (M^*, \Pi^*, \mathbf{v}, \mathbf{b}, \mathbf{G}, \mathbf{c})$.

$\mathsf{Game\ 2}$: $\mathcal{C}$ does the same as that in $\mathsf{Game\ 1}$, except that it computes the vector $\mathbf{b} = \mathbf{B}^\top \mathbf{r} + \mathbf{e}_0 \bmod q$. In $\mathsf{Game\ 1}$, $\mathbf{b}$ is generated by the revocation token grt_{i_b}, which is unknown to $\mathcal{A}$ and statistically close to a uniform vector $\mathbf{r} \in \mathbb{Z}_q^n$. Thus the distribution of $\mathbf{b}$ is statistically close to that in $\mathsf{Game\ 1}$, and $\mathsf{Game\ 2}$ and 1 are statistically indistinguishable.

$\mathsf{Game\ 3}$: $\mathcal{C}$ does the same as that in $\mathsf{Game\ 2}$, except that it generates $(\mathbf{B}, \mathbf{b}) \xleftarrow{\$} \mathcal{U}$. In $\mathsf{Game\ 2}$, $(\mathbf{B}, \mathbf{b})$ is generated by an $\mathsf{LWE}_{n,q,\chi}$ instance, and according to Definition 2, this distribution is computationally close to a uniform distribution $\mathcal{U}$ over $\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$. Thus $\mathsf{Game\ 3}$ and 2 are computationally indistinguishable.

$\mathsf{Game\ 4}$: $\mathcal{C}$ does the same as that in $\mathsf{Game\ 3}$, except that it obtains $\mathbf{A}_3^3 \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$. According to Lemma 1, $\mathbf{A}_3^3$ is statistically close to a uniform matrix in $\mathbb{Z}_q^{n\times m}$. Thus $\mathsf{Game\ 4}$ and 3 are statistically indistinguishable.

$\mathsf{Game\ 5}$: $\mathcal{C}$ does the same as that in $\mathsf{Game\ 4}$, except that it generates $\mathbf{c} = (\mathbf{c}_1^*, \mathbf{c}_2^*)$, where $\mathbf{c}_1^* = \mathbf{z}_1$, $\mathbf{c}_2^* = \mathbf{z}_2 + \lfloor q/2 \rfloor \mathsf{bin}(i)$, here $\mathbf{z}_1 \xleftarrow{\$} \mathbb{Z}_q^m$, $\mathbf{z}_2 \xleftarrow{\$} \mathbb{Z}_q^\ell$. According to Definition 2, the hardness of $\mathsf{LWE}_{n,q,\chi}$ problem implies that $\mathsf{Game\ 5}$ and 4 are computationally indistinguishable.

Game 6: $\mathcal{C}$ does the same as that in Game 5, except that it generates $\mathbf{c} = (\mathbf{c}_1^*, \mathbf{c}_2^*)$, where $\mathbf{c}_1^* = \mathbf{z}_1'$, $\mathbf{c}_2^* = \mathbf{z}_2'$, where $\mathbf{z}_1' \xleftarrow{\$} \mathbb{Z}_q^m$ and $\mathbf{z}_2' \xleftarrow{\$} \mathbb{Z}_q^\ell$. Thus it is easy to see Game 6 and 5 are statistically indistinguishable. Furthermore, Game 6 is independent of the bit b, thus the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{self\text{-}anon}}$ of $\mathcal{A}$ in Game 6 is 0.

According to a series of Games 1 to 6 defined as above, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{self\text{-}anon}}$ in Game 1 is negligible, namely, the proposed scheme is selfless-anonymous.

Theorem 4. *If the* $\mathsf{SIS}^{\infty}_{n,m,q,2\beta\cdot(1+\omega(\sqrt{\log m}))}$ *problem is hard, then the proposed scheme is traceable in* ROM.

Proof. Without loss of generality (WLOG), we first assume that the commitment COM, mentioned in [15], is computationally binding.

Assume that there is a PPT forger $\mathcal{F}$ against our construction with advantage ϵ, we can use $\mathcal{F}$ to construct an algorithm $\mathcal{A}$ to solve the $\mathsf{SIS}^{\infty}_{n,m,q,2\beta\cdot(1+\omega(\sqrt{\log m}))}$ problem with non-negligible probability.

Given a SIS instance $\hat{\mathbf{A}} \in \mathbb{Z}_q^{n\times m}$, $\mathcal{A}$ is required to output a shorter non-zero vector $\hat{\mathbf{e}} \in \mathbb{Z}^m$ satisfying $\hat{\mathbf{A}} \cdot \hat{\mathbf{e}} = \mathbf{0} \bmod q$, and $0 < \|\hat{\mathbf{e}}\|_\infty \leq \mathsf{poly}(m)$.
Setup: $\mathcal{A}$ does as follows:

1. Sample $\mathbf{e}_1^{1*}, \mathbf{e}_2^{2*} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,s}$, $\mathbf{R} \xleftarrow{\$} \{-1,1\}^{m\times m}$, an index $i^* \in \{1,2,\cdots,N\}$.
2. Run $\mathsf{TrapGen}(q,n,m)$ to generate $\mathbf{A}_2^2 \in \mathbb{Z}_q^{n\times m}$ and a trapdoor $\mathbf{R}_{\mathbf{A}_2^2}$.
3. Define $\mathbf{A}_0 = \hat{\mathbf{A}}$, $\mathbf{A}_1^1 = \mathbf{A}_0 \cdot \mathbf{R} - i^*\mathbf{A}_2^2 \bmod q$.
4. Run $\mathsf{TrapGen}(q,n,m)$ to generate $\mathbf{A}_3^3 \in \mathbb{Z}_q^{n\times m}$ and a trapdoor $\mathbf{R}_{\mathbf{A}_3^3}$.
5. Define $\mathbf{u} = \mathbf{A}_0 \cdot (\mathbf{e}_1^{1*} + \mathbf{R}_0 \cdot \mathbf{e}_2^{2*}) \bmod q$.
6. For $i = i^*$, let $\mathsf{gsk}_{i^*} = (\mathbf{e}_1^{1*}, \mathbf{e}_2^{2*})$, $\mathsf{grt}_{i^*} = \mathbf{A}_0 \cdot \mathbf{e}_1^{1*} \bmod q$.
7. For $i \in \{1,2,\cdots,N\} \setminus \{i^*\}$, define $\mathbf{A}_i = [\mathbf{A}_0|\mathbf{A}_1^1 + i\mathbf{A}_2^2] \in \mathbb{Z}_q^{n\times 2m}$, and run $\mathsf{SampleRight}(\mathbf{A}_0, (i-i^*)\mathbf{A}_2^2, \mathbf{R}, \mathbf{R}_{\mathbf{A}_2^2}, \mathbf{u}, s)$ to obtain $\mathbf{e}_i = (\mathbf{e}_{i,1}, \mathbf{e}_{i,2}) \in \mathbb{Z}^{2m}$ and let $\mathsf{gsk}_i = \mathbf{e}_i$, $\mathsf{grt}_i = \mathbf{A}_0 \cdot \mathbf{e}_{i,1} \bmod q$.
8. Let $\mathsf{Gpk} = (\mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{A}_3^3, \mathbf{u})$, $\mathsf{Gmsk} = \mathbf{R}_{\mathbf{A}_3^3}$, $\mathsf{Gsk} = (\mathsf{gsk}_1, \mathsf{gsk}_2, \cdots, \mathsf{gsk}_N)$, $\mathsf{Grt} = (\mathsf{grt}_1, \mathsf{grt}_2, \cdots, \mathsf{grt}_N)$, then send $(\mathsf{Gpk}, \mathsf{Gmsk}, \mathsf{Grt})$ to $\mathcal{F}$.

Queries: $\mathcal{F}$ can make a polynomially bounded number of queries as follows:

1. Corruption: Request for secret-key of i, $\mathcal{A}$ adds i to Corr, and returns gsk_i.
2. Signing: Request for a signature on $M \in \{0,1\}^*$ of member i. $\mathcal{A}$ returns $\Sigma \leftarrow \mathsf{Sign}(\mathsf{Gpk}, \mathsf{gsk}_i, M)$. For queries to oracle $\mathcal{H}$, uniformly random values in $\{1,2,3\}^{\kappa=\omega(\log n)}$ are returned. Assume that $q_{\mathcal{H}}$ is the number of queries to $\mathcal{H}$, for any $d \leq q_{\mathcal{H}}$, let r_d denote the answer to the d-th query.

Forgery: $\mathcal{F}$ outputs a message $M^* \in \{0,1\}^*$, a set of revocation tokens $\mathsf{RL}^* \subseteq \mathsf{Grt}$ and a non-trivial forged group signature $\Sigma^* = (M^*, \Pi^*, \mathbf{v}^*, \mathbf{b}^*, \mathbf{G}^*, \mathbf{c}^*)$, where $\Pi^* = (\{\mathsf{CMT}_j, \mathsf{CH}_j, \mathsf{RSP}_j\}_{j\in\{1,2,\cdots,\kappa\}})$, which satisfies the followings:

1. $\mathsf{Verify}(\mathsf{Gpk}, \mathsf{RL}^*, \Sigma^*, M^*) = 1$.
2. The tracing algorithm (no matter the implicit or explicit tracing) fails, or traces to a member outside of the coalition $\mathsf{Corr}\backslash\mathsf{RL}^*$.

$\mathcal{A}$ exploits the above forgery as follows:

1. Let $\mathbf{B}^* = \mathcal{G}(\mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{u}, M^*, \mathbf{v}^*) \in \mathbb{Z}_q^{n\times m}$.
2. $\mathcal{A}$ must queried $\mathcal{H}$ on $(M^*, \mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{P}, \mathbf{u}, \mathbf{B}^*, \mathbf{b}^*, \mathbf{c}^*, \{\mathsf{CMT}_j\}_{j\in\{1,\cdots,\kappa\}})$, since otherwise, the probability that $(\mathsf{CH}_1, \cdots, \mathsf{CH}_\kappa) = \mathcal{H}(M^*, \mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{P}, \mathbf{u}, \mathbf{B}^*, \mathbf{b}^*, \mathbf{c}^*, \{\mathsf{CMT}_j\}_{j\in\{1,\cdots,\kappa\}})$ is at most $3^{-\kappa}$. Thus, there exists $d' \le q_{\mathcal{H}}$ such that the d'-th hash query involves $(M^*, \mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{P}, \mathbf{u}, \mathbf{B}^*, \mathbf{b}^*, \mathbf{c}^*, \{\mathsf{CMT}_j\}_{j\in\{1,\cdots,\kappa\}})$ with probability at least $\epsilon - 3^{-\kappa}$.
3. Let d' be the target point. $\mathcal{A}$ replays $\mathcal{F}$ many times with the same random tape and input as in the original execution. $\mathcal{F}$ is given the same answers to the first $d' - 1$ queries as in the original execution. From the d'-th query, $\mathcal{A}$ chooses fresh random values $r'_{d'}, \cdots, r'_{q_{\mathcal{H}}} \in \{1, 2, 3\}^\kappa$ as replies.

According to the Improved Forking Lemma of Pointcheval and Vaudenay, with a probability larger than 1/2, algorithm $\mathcal{A}$ can obtain a 3-fork involving the tuple $(M^*, \mathbf{A}_0, \mathbf{A}_1^1, \mathbf{A}_2^2, \mathbf{P}, \mathbf{u}, \mathbf{B}^*, \mathbf{b}^*, \mathbf{c}^*, \{\mathsf{CMT}_j\}_{j\in\{1,2,\cdots,\kappa\}})$ after at most $32 \cdot q_{\mathcal{H}}/(\epsilon - 3^{-\kappa})$ executions of $\mathcal{F}$. Let the answers of $\mathcal{A}$ corresponding to this 3-fork be $r_{d'}^1 = (\mathsf{CH}_1^1, \mathsf{CH}_2^1, \cdots, \mathsf{CH}_\kappa^1), r_{d'}^2 = (\mathsf{CH}_1^2, \mathsf{CH}_2^2, \cdots, \mathsf{CH}_\kappa^2), r_{d'}^3 = (\mathsf{CH}_1^3, \mathsf{CH}_2^3, \cdots, \mathsf{CH}_\kappa^3)$, then $\Pr[\exists i \in \{1, 2, \cdots, \kappa\}\ s.t.\ \{\mathsf{CH}_i^1, \mathsf{CH}_i^2, \mathsf{CH}_i^3\} = \{1, 2, 3\}] = 1 - (7/9)^\kappa$.

Thus, according to the existence of such i, one can parse these 3 forgeries corresponding to the fork to obtain $(\mathsf{RSP}_i^1, \mathsf{RSP}_i^2, \mathsf{RSP}_i^3)$ which are 3 valid responses corresponding to 3 different challenges for the same commitment CMT_i. Further, COM is computationally binding, using the knowledge extractor $\mathcal{K}$ as described in the proof of Theorem 1, one can extract a witness $(\mathsf{id} = \mathsf{bin}(i) \in \{0,1\}^\ell, \boldsymbol{e}_i = (\boldsymbol{e}_{i,1}, \boldsymbol{e}_{i,2}) \in \mathbb{Z}^{2m}, \boldsymbol{e}_0^*, \boldsymbol{e}_1^* \in \mathbb{Z}^m, \boldsymbol{s}^* \in \mathbb{Z}^n, \boldsymbol{e}_2^* \in \mathbb{Z}^\ell)$ such that,

1. $[\mathbf{A}_0|\mathbf{A}_1^1 + i\mathbf{A}_2^2] \cdot \mathbf{e}_i = \mathbf{u} \bmod q$, and $\mathbf{e}_i \in \mathsf{Sec}_\beta(\mathsf{id})$.
2. $\mathbf{b}^* = (\mathbf{B}^{*\top}\mathbf{A}_0) \cdot \mathbf{e}_{i,1} + \mathbf{e}_0^* \bmod q$, and $0 < \|\mathbf{e}_0^*\|_\infty \le \beta$.
3. $\mathbf{c}^* = (\mathbf{c}_1^*, \mathbf{c}_2^*) = (\mathbf{A}_3^{3\top}\mathbf{s}^* + \mathbf{e}_1^* \bmod q, \mathbf{G}^{*\top}\mathbf{s}^* + \mathbf{e}_2^* + \lfloor q/2 \rfloor \mathsf{bin}(i) \bmod q)$.

Now, we consider the following 2 cases:

1. If $i \ne i^*$, this event happens with a probability at most $1 - 1/N$, then $\mathcal{A}$ outputs $\perp$ and aborts.
2. If $i = i^*$, $\mathcal{A}$ returns $\hat{\mathbf{e}} = (\mathbf{e}_1^{1*} - \mathbf{e}_{i^*,1}) + \mathbf{R} \cdot (\mathbf{e}_2^{2*} - \mathbf{e}_{i^*,2})$ as a solution of the given SIS problem. By construction, we have

$$\begin{aligned}\hat{\mathbf{A}} \cdot \hat{\mathbf{e}} &= \mathbf{A}_0 \cdot (\mathbf{e}_1^{1*} - \mathbf{e}_{i^*,1} + \mathbf{R} \cdot (\mathbf{e}_2^{2*} - \mathbf{e}_{i^*,2}))\\ &= \mathbf{A}_0 \cdot (\mathbf{e}_1^{1*} + \mathbf{R} \cdot \mathbf{e}_2^{2*}) - \mathbf{A}_0 \cdot (\mathbf{e}_{i^*,1} + \mathbf{R} \cdot \mathbf{e}_{i^*,2}) = \mathbf{0} \bmod q.\end{aligned}$$

Next, we show that $\hat{\mathbf{e}}$ is with high probability a short non-zero preimage of $\mathbf{0}$ under $\hat{\mathbf{A}}$.

1. $\|\hat{\mathbf{e}}\|_\infty \le \mathsf{poly}(m)$. For $j \in \{1, 2\}$, $\|\mathbf{e}_j^{j*}\|_\infty$, $\|\mathbf{e}_{i^*,j}\|_\infty \le \beta$, $\mathbf{R}$ is a low-norm matrix with coefficients ± 1, thus according to Lemma 4, with overwhelming probability, we have $\|\hat{\mathbf{e}}\|_\infty \le (1 + \omega(\sqrt{\log m})) \cdot 2\beta = \mathsf{poly}(m)$.

2. $\hat{\mathbf{e}} \neq \mathbf{0}$. $\Sigma^* = (M^*, \Pi^*, \mathbf{v}^*, \mathbf{b}^*, \mathbf{G}^*, \mathbf{c}^*)$ is a valid forged signature, thus the tracing algorithm (no matter the implicit or explicit tracing) either fails, or traces to a member outside of the coalition $\mathsf{Corr}\backslash\mathsf{RL}^*$.
   (2.1). If the tracing algorithm fails. $\mathsf{Verify}(\mathsf{Gpk}, \mathsf{grt}_{i^*}, \Sigma^*, M^*) = 1$ implies that $\mathbf{A}_0 \cdot \mathbf{e}_{i^*,1} \neq \mathsf{grt}_{i^*} = \mathbf{A}_0 \cdot \mathbf{e}_1^{1*} \bmod q$, thus $\mathbf{e}_{i^*,1} \neq \mathbf{e}_1^{1*}$.
   (2.2). If the tracing algorithm traces to $j^* \notin \mathsf{Corr}\backslash\mathsf{RL}^*$. Clearly, we have 2 facts: $\mathsf{Verify}(\mathsf{Gpk}, \mathsf{grt}_{j^*}, \Sigma^*, M^*) = 0$, $\mathsf{Verify}(\mathsf{Gpk}, \mathsf{RL}^*, \Sigma^*, M^*) = 1$. Thus, we have the following conclusions:
   a_1. $\mathsf{grt}_{j^*} \notin \mathsf{RL}^*$, thus $j^* \notin \mathsf{Corr}$.
   a_2. Since $\|\mathbf{b}^* - \mathbf{B}^{*\top}\mathsf{grt}_{j^*}\|_\infty = \|\mathbf{B}^{*\top} \cdot (\mathbf{A}_0 \cdot \mathbf{e}_{i^*,1} - \mathsf{grt}_{j^*}) + \mathbf{e}_0^*\|_\infty \leq \beta$, $\|\mathbf{e}_0^*\|_\infty \leq \beta$, thus $\|\mathbf{B}^{*\top} \cdot (\mathbf{A}_0 \cdot \mathbf{e}_{i^*,1} - \mathsf{grt}_{j^*})\|_\infty \leq 2\beta$, furthermore, according to Lemma 4 of [22], we have that $\mathsf{grt}_{j^*} = \mathbf{A}_0 \cdot \mathbf{e}_{i^*,1} \bmod q$ with overwhelming probability.
   Now, considering the following 2 cases:
   b_1. If $\mathcal{F}$ has never requested gsk_{i^*}, then $(\mathbf{e}_1^{1*}, \mathbf{e}_2^{2*})$ cannot be known to $\mathcal{F}$, and thus $(\mathbf{e}_1^{1*}, \mathbf{e}_2^{2*}) \neq (\mathbf{e}_{i^*,1}, \mathbf{e}_{i^*,2})$ with overwhelming probability.
   b_2. If $\mathcal{F}$ has requested gsk_{i^*}, then $i^* \in \mathsf{Corr}$, thus $i^* \neq j^*$, so $\mathsf{grt}_{i^*} \neq \mathsf{grt}_{j^*}$, which means $\mathbf{e}_{i^*,1} \neq \mathbf{e}_1^{1*}$.

Based on the above analysis, for an easy case, in (2.1) and b_2, suppose that $\mathbf{e}_2^{2*} = \mathbf{e}_{i^*,2}$, then we must have $\hat{\mathbf{e}} = \mathbf{e}_1^{1*} - \mathbf{e}_{i^*,1} \neq \mathbf{0}$. On the contrary, in (2.1), b_1 and b_2, $\mathbf{e}_2^{2*} \neq \mathbf{e}_{i^*,2}$, define $\widehat{\mathbf{e}_2} = \mathbf{e}_2^{2*} - \mathbf{e}_{i^*,2}$, in this case, we have $0 \neq \|\widehat{\mathbf{e}_2}\|_\infty \leq 2\beta \ll q$, and thus there must be at least one coordinate of $\widehat{\mathbf{e}_2}$ that is non-zero modulo q. WLOG, let this coordinate be the last one in $\widehat{\mathbf{e}_2}$, and call it $\widehat{e}$. Let $\mathbf{r}$ be the last column of $\mathbf{R}$, the expression of $\hat{\mathbf{e}}$ can be rewritten as $\hat{\mathbf{e}} = \mathbf{r} \cdot \widehat{e} + \hat{\mathbf{e}}'$ where $\hat{\mathbf{e}}'$ does not depends on $\mathbf{r}$. The only information about $\mathbf{r}$ available to $\mathcal{F}$ is just contained in the last column of $\mathbf{A}_1 = \mathbf{A}_0 \cdot \mathbf{R}$. According to the leftover hash or pigeonhole principle, there are $\exp^{\mathcal{O}(m - n\log q) = \widetilde{\mathcal{O}}(n)}$ admissible and equally likely vectors $\mathbf{r}$ that are compatible with the view of $\mathcal{F}$, $\mathcal{F}$ cannot know the value of $\mathbf{r} \cdot \widehat{e}$ with probability exceeding $\exp^{-\widetilde{\mathcal{O}}(n)}$, and at most one such value can result in a cancelation of $\hat{\mathbf{e}}$. Thus, $\hat{\mathbf{e}}$ is non-zero with a high probability $1 - \exp^{-\widetilde{\mathcal{O}}(n)}$.

Therefore, we deduce that $\hat{\mathbf{e}}$ is with a probability larger than $1/(2N) \cdot (1 - (7/9)^\kappa) \cdot (1 - \exp^{-\widetilde{\mathcal{O}}(n)}) \cdot \epsilon$ a short non-zero preimage of $\mathbf{0}$ under $\hat{\mathbf{A}}$, i.e., $\hat{\mathbf{A}} \cdot \hat{\mathbf{e}} = \mathbf{0} \bmod q$, $0 \neq \|\hat{\mathbf{e}}\|_\infty \leq 2\beta \cdot (1 + \omega(\sqrt{\log m})) = \mathsf{poly}(m)$. This concludes the proof.

Acknowledgments. The authors would like to thank the anonymous reviewers of CANS 2019 for their helpful comments and this research is supported by the National Natural Science Foundation of China under Grant 61772477.

References

1. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_28
2. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: STOC, pp. 99–108. ACM (1996). https://doi.org/10.1145/237814.237838

3. Alwen, J., Peikert, C.: Generating shorter bases for hard random lattices. Theory Comput. Syst. **48**(3), 535–553 (2011). https://doi.org/10.1007/s00224-010-9278-3
4. Bellare, M., Micciancio, D., Warinschi, B.: Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 614–629. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-39200-9_38
5. Bellare, M., Shi, H., Zhang, C.: Foundations of group signatures: the case of dynamic groups. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 136–153. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30574-3_11
6. Boneh, D., Shacham, H.: Group signatures with verifier-local revocation. In: CCS, pp. 168–177. ACM (2004). https://doi.org/10.1145/1030083.1030106
7. Bootle, J., Cerulli, A., Chaidos, P., Ghadafi, E., Groth, J.: Foundations of fully dynamic group signatures. In: Manulis, M., Sadeghi, A.-R., Schneider, S. (eds.) ACNS 2016. LNCS, vol. 9696, pp. 117–136. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39555-5_7
8. Camenisch, J., Neven, G., Rückert, M.: Fully anonymous attribute tokens from lattices. In: Visconti, I., De Prisco, R. (eds.) SCN 2012. LNCS, vol. 7485, pp. 57–75. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32928-9_4
9. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 523–552. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_27
10. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991). https://doi.org/10.1007/3-540-46416-6_22
11. Gao, W., Hu, Y., Zhang, Y., Wang, B.: Lattice-Based Group Signature with Verifier-Local Revocation. J. Shanghai JiaoTong Univ. (Sci.) **22**(3), 313–321 (2017). https://doi.org/10.1007/s12204-017-1837-1
12. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoor for hard lattices and new cryptographic constructions. In: STOC, pp. 197–206. ACM (2008) https://doi.org/10.1145/1374376.1374407
13. Gordon, S.D., Katz, J., Vaikuntanathan, V.: A group signature scheme from lattice assumptions. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 395–412. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17373-8_23
14. Katsumata, S., Yamada, S.: Group signatures without NIZK: from lattices in the standard model. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019. LNCS, vol. 11478, pp. 312–344. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17659-4_11
15. Kawachi, A., Tanaka, K., Xagawa, K.: Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 372–389. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89255-7_23
16. Kiayias, A., Yung, M.: Secure scalable group signature with dynamic joins and separable authorities. Int. J. Secur. Netw. **1**(1/2), 24–45 (2006). https://doi.org/10.1504/ijsn.2006.010821
17. Laguillaumie, F., Langlois, A., Libert, B., Stehlé, D.: Lattice-based group signatures with logarithmic signature size. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8270, pp. 41–61. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-42045-0_3

18. Langlois, A., Ling, S., Nguyen, K., Wang, H.: Lattice-based group signature scheme with verifier-local revocation. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 345–361. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54631-0_20
19. Libert, B., Ling, S., Mouhartem, F., Nguyen, K., Wang, H.: Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 373–403. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_13
20. Libert, B., Ling, S., Nguyen, K., Wang, H.: Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 1–31. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_1
21. Libert, B., Mouhartem, F., Nguyen, K.: A lattice-based group signature scheme with message-dependent opening. In: Manulis, M., Sadeghi, A.-R., Schneider, S. (eds.) ACNS 2016. LNCS, vol. 9696, pp. 137–155. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39555-5_8
22. Ling, S., Nguyen, K., Roux-Langlois, A., Wang, H.: A lattice-based group signature scheme with verifier-local revocation. Theor. Comput. Sci. **730**, 1–20 (2018)
23. Ling, S., Nguyen, K., Stehlé, D., Wang, H.: Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 107–124. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36362-7_8
24. Ling, S., Nguyen, K., Wang, H.: Group signatures from lattices: simpler, tighter, shorter, ring-based. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 427–449. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_19
25. Ling, S., Nguyen, K., Wang, H., Xu, Y.: Constant-size group signatures from lattices. In: Abdalla, M., Dahab, R. (eds.) PKC 2018. LNCS, vol. 10770, pp. 58–88. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76581-5_3
26. Ling, S., Nguyen, K., Wang, H., Xu, Y.: Forward-secure group signatures from lattices. In: Ding, J., Steinwandt, R. (eds.) PQCrypto 2019. LNCS, vol. 11505, pp. 44–64. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-25510-7_3
27. Ling, S., Nguyen, K., Wang, H., Xu, Y.: Lattice-based group signatures: achieving full dynamicity with ease. In: Gollmann, D., Miyaji, A., Kikuchi, H. (eds.) ACNS 2017. LNCS, vol. 10355, pp. 293–312. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-61204-1_15
28. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput. **37**(1), 267–302 (2007). https://doi.org/10.1137/s0097539705447360
29. Micciancio, D., Peikert, C.: Hardness of SIS and LWE with small parameters. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 21–39. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_2
30. Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_41
31. Nguyen, P.Q., Zhang, J., Zhang, Z.: Simpler efficient group signatures from lattices. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 401–426. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_18

32. Perera, M.N.S., Koshiba, T.: Achieving strong security and verifier-local revocation for dynamic group signatures from lattice assumptions. In: Katsikas, S.K., Alcaraz, C. (eds.) STM 2018. LNCS, vol. 11091, pp. 3–19. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01141-3_1
33. Perera, M.N.S., Koshiba, T.: Zero-knowledge proof for lattice-based group signature schemes with verifier-local revocation. In: Barolli, L., Kryvinska, N., Enokido, T., Takizawa, M. (eds.) NBiS 2018. LNDECT, vol. 22, pp. 772–782. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-98530-5_68
34. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC, pp. 84–93. ACM (2005). https://doi.org/10.1145/1060590.1060603
35. Zhang, Y., Hu, Y., Gao, W., Jiang, M.: Simpler efficient group signature scheme with verifier-local revocation from lattices. KSII Trans. Internet Inf. Syst. **10**(1), 414–430 (2016). https://doi.org/10.3837/tiis.2016.01.024