Identity-Based Ring Signature from Lattice Basis Delegation

Jin Wang

Institute for Advanced Study, Tsinghua University, Beijing 100084, China
jimiwang@mail.tsinghua.edu.cn

Abstract. In this paper, we propose a set of ring signature (RS) schemes and identity-based ring signature (IBRS) schemes using the lattice basis delegation technique due to [10,22]. The schemes are unforgeable and hold anonymity in the random oracle model. Using the method in [28,29], we also extend our constructions to obtain RS and IBRS schemes in the standard model. Our proposed ring signature schemes fit with ring trapdoor functions introduced by Brakerski and Kalai [31]. However, their work does not include ring signature in the random oracle model and identity-based ring signature schemes. For the lattice-based ring signature in the standard model, our construction is motivated by Boyen's work [28] and results in shorter signatures than Brakeski-Kalai scheme. [1]

Key words: Ring signature, identity-based ring signature, lattices, basis delegation

1 Introduction

Ring Signature. Ring signature, introduced by Rivest, Shamir and Tauman[23], is a type of group-oriented signatures which provides anonymity in some scenarios. In a ring signature scheme, a message signer forms a ring of any set of possible signers including him/herself. The message signer can then generate a ring signature using his/her secret key and public keys of other ring members. The generated ring signature can convince an arbitrary verifier that the message was signed by one of the ring members without revealing exactly the singer's identity. Ring signature schemes could be used for whistle blowing [23], anonymous membership authentication [7] and many other applications.

Identity-Based Ring Signature. The concept of identity-based ring signature can be seen as the merge of identity-based cryptography and ring signature. Identity-based cryptography was introduced by Shamir [25] to simplify the certificate management process. As in identity-based cryptographic constructions [9,11,14], a user's public key is allowed to be derived from his/her identity information, such as an email address, while the corresponding private key is

[1] Supported by 973 Project (No.2007CB807902), National Natural Science Foundation of China (NSFC Grant No.60910118)

calculated by a trusted authority called Key Generator Center (KGC).The first identity-based ring signature scheme was proposed in [27]. Since then, several construction have been proposed based on pairings [2,12] and Strong RSA assumptions [30] .

Motivations. Up to date, most of the existing ring signature and identity-based ring signature constructions are based on hard number theory assumptions ranging from the Strong RSA [7,23] assumptions and the discrete logarithm problem [1,17] to the bilinear pairings with diffie-hellman problems [26,27]. However, above underlying number theory problems will be solvable if practical quantum computers become reality, so it implies a potential security threat to these schemes. Thus, a natural question one can ask is how to design ring signature systems that are secure in the quantum environment. In recent years, lattices have emerged as a possible alternative to number theory. Lattice-based cryptography began with the seminal work of Ajtai[3], who showed that it is possible to construct families of cryptographic functions in which average-case security provably related to the worst-case complexity of hard lattice problems. Lattice-based constructions also enjoy relatively efficient implementations, as well as great simplicity. In addition, lattice-based cryptography is believed to be secure against quantum computers.

Our Contribution. Following above discussion, in this paper, we focus on constructing ring signature and identity-based ring signature schemes from lattices. The idea behind our construction is based on the lattice delegation method due to [10,22]. In our ring signature scheme, the public/secret key pair of each user is simply a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a corresponding short basis $\mathbf{B} \in \mathbb{Z}^{m \times m}$ for the lattice $\Lambda^{\perp}(\mathbf{A})$. As explored in prior works[3,14], short basis can be treated as a trapdoor for the corresponding lattice. In the ring signature approach, for the ring set R of size l, the singer constructs a public lattice corresponding to the ring set as $\mathbf{A}_R = [\mathbf{A}_1 \| ... \| \mathbf{A}_l]$(for $i \in R, 1 \leq i \leq l$). Following the "hash-and-sign" paradigm as in [16], a message m is hashed to some point $\mathbf{y} = H(m)$. Using the basis delegation technique, each member in R should be able to deduce a signature (short vector $\mathbf{e}$) on m that satisfied $\mathbf{A}_R\mathbf{e} = \mathbf{y} \bmod q$. Since short basis for lattices essentially functions like cryptographic trapdoors, only the ring members in R can generate the signature successfully. The above construction can be generalized to obtain the first identity-based ring signature scheme from lattice. Our ring signature and identity-based ring signature schemes hold anonymity and unforgeability in the random oracle model. Moreover, using the similar technique in [28,29] , we can modify our basic constructions to obtain a ring signature and an identity-based ring signature scheme in the standard model. To the best of author's knowledge, our constructions constitute of the first lattice-based ring signature and identity-based ring signature schemes in the random oracle model and achieve shorter signatures than Brakeski and Kalai's work in the standard model.

1.1 Related Work

Comparing with Brakerski and Kalai's Work. Brakerski and Kalai [31] recently presented a generic framework for constructing ring signature schemes in the standard model, and obtained a corresponding scheme based on SIS assumption. Our proposed ring signature schemes fit with ring trapdoor functions in [31] at a technical level. However, their work does not include ring signature in the random oracle model and identity-based ring signature schemes. For the lattice-based ring signature in the standard model, our construction is motivated by Boyen's work [28] and results in shorter signature than Brakeski-Kalai scheme.

Lattice-based Signature. Our cryptographic constructions is based on the hardness assumption of the Small Integer Solution Problem (SIS)[24]. For reasonable choices of parameters, SIS is as hard as the shortest vector problem (SVP) in lattices. Gentry, Peikert, and Vaikuntanathan [16] constructed a kind of trapdoor primitive called Pre-image Sampling functions that, given a basis of a hard integer lattice, samples lattice points from a *Discrete Gaussian* probability distribution whose standard deviation is essentially the length of the longest *Gram-Schmidt* vector of the basis. As the application of above trapdoors, Gentry et al. [16] constructed "hash and sign" digital signature schemes based on SIS. Another notable recent work is due to Cash et al.[9] who constructed a basis delegation technique that allows one to derive a short basis of a given lattice using a short basis of a related lattice. Using this basis delegation technique, Cash et al.[9] also constructed a stateless signature of lattice-based constructions.

2 Preliminaries

2.1 Notation

For a positive integer d, $[d]$ denotes the set $\{1, ..., d\}$. For an $n \times m$ matrix $\mathbf{A}$, let $\mathbf{A} = [\mathbf{a}_1, ..., \mathbf{a}_m]$, where $\mathbf{a}_i$ denotes the i-th column vector of $\mathbf{A}$. We define $\|\mathbf{a}\|$ for the Euclidean norm of $\mathbf{a}$, and $\|\mathbf{A}\| = \max_{i \in [m]} \|\mathbf{a}_i\|$.

2.2 Lattices

Lattices. Let $\mathbf{B} = \{\mathbf{b}_1, ..., \mathbf{b}_n\} \in \mathbb{R}^n$ consist of n linearly independent vectors. A n-dimensional lattice Λ generated by $\mathbf{B}$ is defined as

$$\Lambda = \mathcal{L}(\mathbf{B}) = \{\mathbf{Bc} : \mathbf{c} \in \mathbb{Z}^n\}$$

Here $\mathbf{B}$ is called a *basis* of the lattice $\Lambda = \mathcal{L}(\mathbf{B})$. For a basis $\mathbf{B} = \{\mathbf{b}_1, ..., \mathbf{b}_n\}$, let $\widetilde{\mathbf{B}}$ denote its *Gram-Schmidt orthogonalization*, defined iteratively as follows: $\widetilde{b_1} = b_1$, and for $i = 2, ..., n$, $\widetilde{b_i}$ is the component of b_i orthogonal to $\text{span}(b_1, ..., b_{i-1})$.

Hard Random Lattices. In this paper our cryptographic constructions will build on a certain family of m-dimensional integer lattices defined by Ajtai [5].

Definition 1. *Given a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *for some integers* q, m, n*, define:*

1 . $\Lambda^{\perp}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{Ae} = 0 \bmod q\}$
2 . $\Lambda^{\perp}_{\mathbf{y}}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{Ae} = \mathbf{y} \bmod q\}$
3 . $\Lambda(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}^T\mathbf{w} \bmod q, \text{ for some } \mathbf{w} \in \mathbb{Z}^n\}$

Observe that $\Lambda^{\perp}_{\mathbf{y}}(\mathbf{A}) = \mathbf{t} + \Lambda^{\perp}(\mathbf{A}) \bmod q$ where $\mathbf{t}$ is an arbitrary solution (over $\mathbb{Z}^m$) of the equation $\mathbf{At} = \mathbf{y} \bmod q$. Thus $\Lambda^{\perp}_{\mathbf{y}}(\mathbf{A})$ is the coset of $\Lambda^{\perp}(\mathbf{A})$.
Discrete Gaussians on Lattices. Here we review Gaussian functions used in lattice based cryptographic constructions. For any $r > 0$ the Gaussian function on $\mathbb{R}^n$ centered at $\mathbf{c}$ with deviation parameter r is defined as

$$\forall\, \mathbf{x} \in \mathbb{R}^n, \rho_{r,\mathbf{c}}(x) = \exp(-\pi\|\mathbf{x} - \mathbf{c}\|^2/r^2)$$

For any $\mathbf{c} \in \mathbb{R}^n$, $r > 0$ and n-dimensional lattice Λ, the discrete gaussian distribution over Λ is defined as

$$\forall\, \mathbf{x} \in \Lambda, D_{\Lambda_{r,\mathbf{c}}}(x) = \frac{\rho_{r,\mathbf{c}}(\mathbf{x})}{\rho_{r,\mathbf{c}}(\Lambda)}$$

For a fixed vector $\mathbf{y} \in \mathbb{Z}_q^n$ in the span of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, define the coset of $\Lambda^{\perp}(\mathbf{A})$ as $\Lambda^{\perp}_y(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{Ae} = \mathbf{y} \bmod q\} = \mathbf{t} + \Lambda^{\perp}(\mathbf{A}) \bmod q$; where $\mathbf{t}$ is an arbitrary solution (over $\mathbb{Z}$) of the equation $\mathbf{At} = \mathbf{y} \bmod q$. The Gaussian on $\Lambda^{\perp}_y(\mathbf{A})$, which is the conditional distribution of $D_{\mathbb{Z}^m,r}$ on $\mathbf{Ae} = \mathbf{y} \bmod q$, is given by

$$\forall\, \mathbf{x} \in \Lambda, D_{\Lambda^{\perp}_{\mathbf{y}}(\mathbf{A}),r}(\mathbf{x}) = \frac{\rho_{r,c}(\mathbf{x})}{\rho_{r,c}(\mathbf{t} + \Lambda^{\perp}(\mathbf{A}))}$$

Small Integer Solution Problem The most well known computational problem on lattices is the *shortest vector problem* (SVP), in which given a basis of a lattice Λ and the goal is to find the shortest vector $v \in \Lambda\backslash\{0\}$. There is a special version of the SVP for the integer lattices, named *small integer solution* problem (SIS).

Definition 2. *The small integer solution problem* SIS *(in the Euclidean* l_2 *norm) is as follows: given an integer* q*, a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$*, and a real* β*, find a nonzero integer vector* $\mathbf{e} \in \mathbb{Z}^m$ *such that* $\mathbf{Ae} = 0 \bmod q$ *and* $\|\mathbf{e}\|_2 \leq \beta$

For functions $q(n)$, $m(n)$, and $\beta(n)$, $\mathsf{SIS}_{q,m,\beta}$ is the ensemble over instances $(q(n), \mathbf{A}, \beta(n))$, where $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is uniformly random.

We write $\mathsf{Adv}^{\mathrm{sis}}_{q,\beta,\mathcal{A}}(k)$ to denote the success probability and distinguishing advantage of an algorithm $\mathcal{A}$ for the SIS problem. Using Gaussian techniques, Micciancio and Regev[20] showed that for any poly-bounded m, $\beta = poly(n)$ and for any prime $q \geq \beta \cdot \omega(\sqrt{n \log n})$, the average-case problem $\mathsf{SIS}_{q,m,\beta}$ is as hard as approximating the SIVP problem (a variant of SVP) in the worst case within a factor $\tilde{O}(\beta \cdot \sqrt{n})$.

2.3 Trapdoors and Basis Delegation Functions

It was shown in [17] that if $\mathsf{SIS}_{q,m,2r\sqrt{m}}$ is hard, $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ defines a one-way function $f_{\mathbf{A}} : D_n \to R_n$ with $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{A}\mathbf{e} \bmod q$, where $D_n = \{\mathbf{e} \in \mathbb{Z}^m : \|\mathbf{e}\| \leq r\sqrt{m}\}$ and $R_n = \mathbb{Z}_q^n$. The input distribution is $D_{\mathbb{Z}^m,r}$. A short basis $\mathbf{B}$ for $\Lambda^{\perp}(\mathbf{A})$ can be used as a trapdoor to sample from $f_A^{-1}(\mathbf{y})$ for any $\mathbf{y} \in \mathbb{Z}_q^n$. Knowledge of such a trapdoor makes it easy to solve some hard problems relative to the lattice, such as LWE and SIS problems. Here we briefly introduce such a set of one-way preimage sampleble functions (defined in [16]), denoted as $\mathsf{TrapGen}$,$\mathsf{SampleD}$, $\mathsf{SampleDom}$, $\mathsf{SamplePre}$, which will be used as building blocks in our cryptographic constructions (we refer the interested reader to [16] for more details). The following functions take the Gaussian smoothing parameter $r \geq \|\tilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log m})$ as a parameter:

- $\mathsf{TrapGen}(1^{\lambda})$: Let n, q, m be integers with $q \geq 2$, $m \geq 5n\log q$. $\mathsf{TrapGen}(1^n)$ outputs a pair $(\mathbf{A}, \mathbf{B})$ such that $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is statistically close to uniform on $\mathbb{Z}_q^{n\times m}$ and $\mathbf{B}$ is a good basis of $\Lambda^{\perp}(\mathbf{A})$ such that $\|\widetilde{\mathbf{B}}\| \leq O(\sqrt{n\log q})$ and $\|\mathbf{B}\| \leq O(n\log q)$ with all but $n^{\omega(1)}$ probability. (Ajtai [5] showed how to sample a pair $(\mathbf{A}, \mathbf{B})$ with low Gram-Schmidt norm. Here we use an improved sampling algorithm from Alwen and Peikert[3]).
- $\mathsf{SampleD}(\mathbf{B}, r, \mathbf{c})$: On input of an m-dimensional basis $\mathbf{B}$ of a lattice Λ, a parameter r, and a center vector $\mathbf{c} \in \mathbb{R}^m$, the algorithm $\mathsf{SampleD}$ samples from a discrete Gaussian distribution over the lattice Λ around the center $\mathbf{c}$ with standard deviation r.
- $\mathsf{SampleDom}(\mathbf{A}, r)$: Samples an $\mathbf{x}$ from distribution $D_{\mathbb{Z}^m,r}$ for which the distribution of $f_{\mathbf{A}}(\mathbf{x})$ is uniform over R_n.
- $\mathsf{SamplePre}(\mathbf{A}, \mathbf{B}, \mathbf{y}, r)$: On input of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a good basis $\mathbf{B}$ for $\Lambda^{\perp}(\mathbf{A})$ as above, a vector $\mathbf{y} \in \mathbb{Z}_q^n$ and r; the conditional distribution of the output $\mathbf{e}$ is within negligible statistical distance of $D_{\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A}),r}$. The algorithm works as follows. First, choose via linear algebra an arbitrary $\mathbf{t} \in \mathbb{Z}^m$ such that $\mathbf{A}\mathbf{t} = \mathbf{y} \bmod q$. Then sample $\mathbf{v}$ from the Gaussian distribution $D_{\Lambda^{\perp}(\mathbf{A}),r,-\mathbf{t}}$ using $\mathsf{SampleD}(\mathbf{B}, r, -\mathbf{t})$, and output $\mathbf{e} = \mathbf{t} + \mathbf{v}$.

We now recall the method proposed in [10,22] which use a good basis of a lattice Λ to generate another good basis for a higher-dimensional lattice Λ' which contains a sublattice isomorphic to Λ . Let n, q, m, k be positive integers with $q \geq 2$ and $m \geq 5n\log q$, the basis delegation algorithms $\mathsf{ExtBasis}$ and $\mathsf{RandBasis}$ are described as follows:

- $\mathsf{ExtBasis}(\mathbf{S}, \mathbf{A} = \mathbf{A}_0|\mathbf{A}_1)$: On input of $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times m_0}$,an arbitrary $\mathbf{A}_1 \in \mathbb{Z}_q^{n\times m_1}$, a basis $\mathbf{S}_0 \in \mathbb{Z}^{m_0\times m_0}$ of $\Lambda^{\perp}(\mathbf{A}_0)$. The algorithm outputs a basis $\mathbf{S} \in \mathbb{Z}^{(m_0+m_1)\times(m_0+m_1)}$ of $\Lambda^{\perp}(\mathbf{A})$ such that $\|\tilde{\mathbf{S}}\| = \|\tilde{\mathbf{S}}_0\|$.
- $\mathsf{RandBasis}(\mathbf{A}, \mathbf{S}, r)$: On input of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a basis $\mathbf{S} \in \mathbb{Z}^{m\times m}$ of $\Lambda^{\perp}(\mathbf{A})$ and a parameter $r \geq \|\mathbf{S}\| \cdot \omega(\sqrt{\log n})$. The algorithm outputs a basis $\mathbf{S}'$ of $\Lambda^{\perp}(\mathbf{A})$ such that $\|\mathbf{S}'\| \leq r \cdot \sqrt{m}$ and no information particular to $\mathbf{S}$ is leaked by the output $\mathbf{S}'$.

2.4 Ring Signature and Identity-Based Ring Signature

Ring Signature. A ring signature scheme is a tuple of algorithms RS = (KeyGen, Ring-Sign, Ring-Verify) described as follows:

- KeyGen(λ): A probabilistic algorithm takes as input the security parameter λ and outputs a public key pk and secret signing key sk.
- Ring-Sign(pk, sk, R, m): A probabilistic algorithm takes as input a user's key pair (pk, sk); a set of public keys R of the ring and a message M to be signed (We require that $pk \in R$). It returns a ring signature σ of m under sk.
- Ring-Verify(m,σ): A deterministic algorithm takes as input a set of public keys R that constitutes the ring and a ring signature σ on a message m. It outputs "accept" if the ring signature is valid, or "reject" otherwise.

For consistency purposes, we require that for $l \in \mathbb{N}$, all $\{(pk_i, sk_i)_1^l\} \in [\mathsf{KeyGen}(\lambda)]$, all $i \in [l]$ and all $M \in \{0,1\}^*$. $\mathsf{Verify}(M, \mathsf{Sign}(sk_i, M, R)) = 1$ where $R = (pk_1, ..., pk_l)$.

The security of a ring signature scheme consists of two requirements, namely *Anonymity* and *Unforgeability*. Here we follow the formal security definitions for ring signature presented by Bender, Katz, and Morselli[8].

Anonymity: Anonymity against full key exposure for a ring signature scheme RS is defined using the following game between a challenger $\mathcal{B}_1$ and an adversary $\mathcal{A}_1$: $\mathcal{B}_1$ firstly runs algorithm KeyGen to obtain public/private key pairs $(pk_1, sk_1), ..., (pk_l, sk_l)$. Here l is a game parameter. The adversary $\mathcal{A}_1$ is given the public keys $\{pk_i\}_1^l$. The adversary $\mathcal{A}_1$ is allowed to make ring signing queries and corruption queries. A ring signing query is of the form (s, R, m). where m is the message to be signed, R is a set of public keys, and s is an user index with $pk_s \in R$. The challenger responds with $\sigma = \mathsf{Sign}(pk_s, sk_s, R, M)$. A corruption query is an index s. The challenger provides sk_s to $\mathcal{A}_2$. Once the adversary $\mathcal{A}_1$ decides that the query phase is over, $\mathcal{A}_1$ requests a challenge by sending to the challenger the values (i_0, i_1, R, M) such that M is a message to be signed with the ring R, and i_0 and i_1 are indices with $pk_{i_0}, pk_{i_1} \in R$. The challenger chooses a bit $b_R \leftarrow \{0,1\}$, computes the challenge signature $\sigma \leftarrow \mathsf{Sig}(pk_{i_b}, sk_{i_b}, R, M)$, and provides $\mathcal{A}_1$ with σ. The adversary $\mathcal{A}_1$ outputs a guess $b' \in \{0,1\}$ and wins the game if $b' = b$.

Denote $\mathrm{Adv}_{RS,\mathcal{A}_1}^{rsig-anon-ke}$ to be the advantage over 1/2 of $\mathcal{A}_1$ in the above game. A ring signature scheme RS is anonymous, if for every probabilistic polynomial-time adversary $\mathcal{A}_1$ the advantage $\mathrm{Adv}_{RS,\mathcal{A}_1}^{rsig-anon-ke}$ is negligible.

Unforgeability: For a ring signature scheme with l public keys, the existential unforgeability(with insider corruption)is defined as the following game between a challenger and an adversary $\mathcal{A}_2$. The challenger firstly runs algorithm KeyGen to obtain public/private key pairs $(pk_1, sk_1), ..., (pk_l, sk_l)$. $\mathcal{A}_2$ is given the public keys PK=$\{pk_i\}$.The challenger also initializes the set C of corrupted users as $C \leftarrow \emptyset$. $\mathcal{A}_2$ is allowed to make ring signing queries and corruption queries as in the anonymity game. Finally $\mathcal{A}_2$ outputs a tuple (L^*, m^*, σ^*). $\mathcal{A}_2$ wins the game if: [1] $L^* \subseteq L$; [2] (L^*, m^*) has not been submitted to the signing oracle;

[3] $\mathsf{Verify}(L^*, m^*, \sigma^*) = \mathsf{Accept}$.

We denote $\mathcal{A}_2$'s advantage in above game to be $Adv\mathcal{A}_2 = \Pr[\mathcal{A}_2 \text{ wins}]$. A ring signature scheme RS is traceable, if for every probabilistic polynomial-time adversary $\mathcal{A}_2$ the advantage $Adv\mathcal{A}_2$ is negligible.

Identity-Based Ring Signature. An identity-based ring signature scheme is a tuple of algorithms IBRS = (Setup, KeyGen, Ring-Sign, Verify) described as follows: $\mathsf{Setup}(\lambda)$: Takes as input the security parameter λ and outputs a list of system parameters PK and the master key MSK for the KGC.$\mathsf{Extract}(MSK, ID_i)$: Takes as input a user's identity string $ID_i \in \{0,1\}^*$ $(1 \leq i \leq l)$ and the master key of the KGC. It outputs a user private key sk_{ID_i}. $\mathsf{Sign}(sk_{ID_i}, M, R)$: Takes as input a user ID_i's secret key sk_{ID_i}; the identities $ID_1, ..., ID_k$ of the members in the ring R and a message M to return a ring signature σ of M under sk_{ID_i}. $\mathsf{Verify}(M,\sigma)$: Takes as input a message m and a ring signature σ, that includes the identities of the members in the corresponding ring, and outputs "accept" if the ring signature is valid, or "reject" otherwise.

For consistency purposes, we require that for $l \in \mathbb{N}$, $MSK \in \mathsf{Setup}(\lambda)$, all $i \in [l]$, $sk_{ID_i} \in [\mathsf{Extract}(MSK, ID_i)]$, and all $M \in \{0,1\}^*$; $\mathsf{Verify}(m, \mathsf{Sign}(sk_{ID_i}, M, R)) = 1$ where $R = (ID_1, ..., ID_l)$.

A secure identity-based ring signature scheme should be unforgeable and anonymous which is defined in a similar way to that of a ring signature scheme.

3 Lattice Based Ring Signature

In this section, we describe our ring signature system using the lattice basis delegation technique. We start with a slight variant of the generalized sampling algorithm GenSamplePre which was first proposed in [10], with different choice of parameters and the structure of the extended lattice. The original algorithm enables the growth of extended matrices in a tree form. In our approach, we will handle with another extension policy better suited for our ring signature scheme given later.

3.1 Sampling Preimage for Extended Lattice

Let k, k_1, k_2, k_3, k_4 be positive integers and $k = k_1 + k_2 + k_3 + k_4$. Assume without loss of generality that $S = [k]$. We write $\mathbf{A}_S = [\mathbf{A}_{S_1} \| \mathbf{A}_{S_2} \| \mathbf{A}_{S_3} \| \mathbf{A}_{S_4}] \in \mathbb{Z}_q^{n \times km}$, where $\mathbf{A}_{S_1} \in \mathbb{Z}_q^{n \times k_1 m}$, $\mathbf{A}_{S_2} \in \mathbb{Z}_q^{n \times k_2 m}$, $\mathbf{A}_{S_3} \in \mathbb{Z}_q^{n \times k_3 m}$, $\mathbf{A}_{S_4} \in \mathbb{Z}_q^{n \times k_4 m}$. Let $\mathbf{A}_R = [\mathbf{A}_{S_1} \| \mathbf{A}_{S_3}] \in \mathbb{Z}_q^{n \times (k_1 + k_3)m}$. Given a short basis $\mathbf{B}_R$ for $\Lambda^{\perp}(\mathbf{A}_R)$ and an integer $r \geq \|\tilde{\mathbf{B}}_R\| \cdot \omega(\sqrt{\log n})$, the algorithm GenSamplePre allows to sample a preimage of the function $f_{\mathbf{A}_S}(\mathbf{e}) = \mathbf{A}_S \mathbf{e} \bmod q$. $\mathsf{GenSamplePre}(\mathbf{A}_S, \mathbf{A}_R, \mathbf{B}_R, \mathbf{y}, r)$ proceeds as follows:

1 Sample $\mathbf{e}_{S_2} \in \mathbb{Z}^{k_2 m}$ from the distribution $D_{\mathbb{Z}^{k_2 m}, r}$ and sample $\mathbf{e}_{S_4} \in \mathbb{Z}^{k_4 m}$ from the distribution $D_{\mathbb{Z}^{k_4 m}, r}$. Parse $\mathbf{e}_{S_2} = [\mathbf{e}_{k_1+1}, ..., \mathbf{e}_{k_1+k_2}] \in (\mathbb{Z}^m)^{k_2}$ and $\mathbf{e}_{S_4} = [\mathbf{e}_{k-k_4+1}, ..., \mathbf{e}_k] \in (\mathbb{Z}^m)^{k_4}$.

2 Let $\mathbf{z} = \mathbf{y} - \mathbf{A}_{S_2}\mathbf{e}_{S_2} - \mathbf{A}_{S_4}\mathbf{e}_{S_4} \bmod q$. Run $\mathsf{SamplePre}(\mathbf{A}_R, \mathbf{B}_R, \mathbf{z}, r)$ to sample a vector $\mathbf{e}_R \in \mathbb{Z}^{(k_1+k_3)m}$ from the distribution $D_{\Lambda^{\perp}_{\mathbf{y}}(\mathbf{A}_S),r}$. Parse $\mathbf{e}_R = [\mathbf{e}_1, ..., \mathbf{e}_{k_1}, \mathbf{e}_{k_1+k_2+1}, ..., \mathbf{e}_{k-k_4}] \in (\mathbb{Z}^m)^{k_1+k_3}$ and let $\mathbf{e}_{S_1} = [\mathbf{e}_1, ..., \mathbf{e}_{k_1}] \in (\mathbb{Z}^m)^{k_1}$, $\mathbf{e}_{S_3} = [\mathbf{e}_{k_1+k_2+1}, ..., \mathbf{e}_{k-k_4}] \in (\mathbb{Z}^m)^{k_3}$.
3 Output $\mathbf{e} \in \mathbb{Z}^{km}$, as $\mathbf{e} = [\mathbf{e}_1, ..., \mathbf{e}_k]$.

Note that by construction, we have $\mathbf{A}_{S_1}\mathbf{e}_{S_1} + \mathbf{A}_{S_3}\mathbf{e}_{S_3} = \mathbf{A}_R\mathbf{e}_R = \mathbf{z} \bmod q$. Thus $\mathbf{A}_S\mathbf{e} = \sum_{i=1}^{4} \mathbf{A}_{S_i}\mathbf{e}_{S_i} = \mathbf{y} \bmod q$, and the output vector $\mathbf{e}$ of $\mathsf{GenSamplePre}$ is contained in $\Lambda^{\perp}_y(\mathbf{A}_S)$. For the analysis of the output distribution, Theorem 3.4 in [10] showed that $\mathbf{e}$ is within negligible statical distance of $D_{\Lambda^{\perp}_y(\mathbf{A}_S),r}$

3.2 Basic Construction

Let l, m, n, q, t be positive integers with $q \geq 2$ and $m \geq 5n\log q$. The ring signature scheme shares parameter functions L, r defined in [10] as follows:

- $\widetilde{L} \geq O(\sqrt{n \log q})$: an upper bound of the Gram-Schmidt size of a user's secret basis;
- $r \geq \widetilde{L} \cdot \omega(\sqrt{\log n})$: a Gaussian parameter used to generate the secret basis and short vectors.

The scheme employs a hash functions $H_1 : \{0,1\}^* \to \mathbb{Z}_q^n$. The security analysis will view H_1 as a random oracle.

KeyGen(l):A user with index i runs the trapdoor generation algorithm $\mathsf{TrapGen}(1^\lambda)$ (described in section 2.4) to generate $\mathbf{A}_i \in \mathbb{Z}_q^{n\times m}$ with a basis $\mathbf{B}_i \in \mathbb{Z}^{m\times m}$ for $\Lambda^{\perp}(\mathbf{A}_i)$. Note that by Theorem 1 we have $\|\widetilde{\mathbf{B}}_i\| \leq \widetilde{L}$. The public/private key pair for the user i is $\langle pk_i = \mathbf{A}_i, sk_i = \mathbf{B}_i\rangle$.

Ring-Sign(R, sk_i, M): Given a ring of l individuals with public keys R, assume for notational simplicity that $R = \{\mathbf{A}_1, ..., \mathbf{A}_l\} \in \mathbb{Z}_q^{n\times m}$, a user i's ($i \in [l]$) private key $sk_i = \mathbf{B}_i$, and a message $M \in \{0,1\}^*$, the user i does the following:

- Set $\mathbf{A}_R$=$[\mathbf{A}_1\|...\|\mathbf{A}_l] \in \mathbb{Z}_q^{n\times lm}$ and $\mathbf{y} = H_1(M) \in \mathbb{Z}_q^n$. Define a label lab_R that contains information about how $\mathbf{A}_R$ is associated with the sequence of the ring numbers $\{1, ..., l\}$.
- Generate $\mathbf{e} \leftarrow \mathsf{GenSamplePre}(\mathbf{A}_R, \mathbf{A}_i, \mathbf{B}_i, \mathbf{y}, r) \in \mathbb{Z}^{lm}$. Note that $\mathbf{e}$ is distributed according to $D_{\Lambda^{\perp}_{\mathbf{y}}\mathbf{A}_R,r}$.
- Output the ring signature $\sigma =< \mathbf{e}, lab_R >$.

Ring-Verify(σ, M): Given a ring of public keys $R = \{\mathbf{A}_1, ..., \mathbf{A}_l\} \in \mathbb{Z}_q^{n\times m}$, a message M, and a ring signature $\sigma =< \mathbf{e}, lab_R >$, the verifier accepts the signature only if both the following conditions satisfied:

- $0 \leq \|\mathbf{e}\| \leq r\sqrt{lm}$
- $\mathbf{A}_R\mathbf{e} \bmod q$=$H_2(M)$.

Otherwise, the verifier rejects.

3.3 Correctness

The scheme's correctness is inherited by the properties of the trapdoor functions [15]. In the signing process, the ring members in R construct a one-way function $f_{A_R} : D_R \rightarrow \mathbb{Z}_q^n$ as $f_{\mathbf{A}_R}(\mathbf{e}) = \mathbf{A}_R\mathbf{e} \bmod q$, where $D_R = \{\mathbf{e} \in \mathbb{Z}^{lm} : \|\mathbf{e}\| \leq r\sqrt{lm}\}$ with the following properties:

Correct Distributions: By Lemma 5.1 in [17], the distribution of the syndrome $\mathrm{y} = \mathbf{A}_R\mathbf{e} \bmod q$ is within statistical distance 2ϵ of uniform over $\mathbb{Z}_q^n$. By the Theorem 2, algorithm $\mathsf{GenSamplePre}(\mathbf{A}_R, \mathbf{A}_i, \mathbf{B}_i, \mathrm{y}, r)$ samples an element $\mathbf{e}$ from distribution within negligible statistical distance of $D_{\Lambda^{\perp}_{\mathbf{y}(\mathbf{A}_R),r}}$.

One-Wayness Without Trapdoors: By Theorem 5.9 in [17], inverting a random function $f_{\mathbf{A}_R}$ on a uniform output $\mathbf{u} \in \mathbb{Z}_q^n$ is equivalent to solving the *inhomogeneous small integer solution* problem ISIS(a variant of SIS) as $\mathsf{ISIS}_{q,lm,r}$.

3.4 Security Analysis

We now prove that our ring signature scheme is anonymous against full key exposure and unforgeable with regard to insider corruption.

Full Anonymity: Before proving the full anonymity, we prepare the following lemma on our ring signature scheme.

Lemma 1. *Let (i_0, i_1, R, M) be a tuple such that $M \in \{0,1\}^*$ is a message to be signed with the ring $R = \{\mathbf{A}_1, ..., \mathbf{A}_l\} \in \mathbb{Z}_q^{n\times m}$, and i_0 and i_1 are indices with $\mathbf{A}_{i_0}, \mathbf{A}_{i_1} \in R$. If $\mathsf{ISIS}_{q,lm,r}$ is hard, $\sigma_{i_0} \leftarrow \mathsf{Sig}(sk_{i_0}, R, M)$ and $\sigma_{i_1} \leftarrow \mathsf{Sig}(sk_{i_1}, R, M)$ are computationally indistinguishable.*

Proof: The proof is straightforward from the algorithm Sign. Recall that in the signing process, σ_{i_0} and σ_{i_1} have the same distribution of the domain in $f_{\mathbf{A}_R}$ within negligible statistical distance of $D_{\Lambda^{\perp}_{H_1(M)}(\mathbf{A}_R),r}$ and it implies that σ_{i_0} and σ_{i_1} are computationally indistinguishable.

Theorem 1. *Let $q \geq 2$ and $m \geq 5n \log q$. If H_1 is modeled as a random oracle, the ring signature scheme above is fully-anonymous assuming that $\mathsf{SIS}_{q,lm,r}$ is hard.*

Proof. Assume that there exists an adaptive adversary $\mathcal{A}_1$ attacking our ring signature scheme following the definition of anonymity against full key exposure. We construct a PPT algorithm $\mathcal{B}_1$ to simulate the attacking environment for $\mathcal{A}_1$. Both $\mathcal{A}_1$ and $\mathcal{B}_1$ are given as input q_E, the total number of extraction queries that can be issued by $\mathcal{A}_1$. To respond to $\mathcal{A}_1$'s queries in the random oracle, $\mathcal{B}_1$ will maintain two lists H_1 and $\mathcal{G}$, which are initialized to be empty and will store tuples of values.

In the Setup phase, $\mathcal{B}_1$ runs the algorithm $\mathsf{TrapGen}$ q_E times to generate $\mathbf{A}_i \in \mathbb{Z}_q^{n\times m}$ with the corresponding short basis $\mathbf{B}_i \in \mathbb{Z}^{m\times m}$ $(1 \leq i \leq q_E)$. $\mathcal{B}$ stores the tuple $\langle i, \mathbf{A}_i, \mathbf{B}_i\rangle (1 \leq i \leq q_E)$ in list $\mathcal{G}$ and the system parameters $< \mathbf{A}_1 \| ... \| \mathbf{A}_{q_E}] >$ are given to $\mathcal{A}_1$. In the query phase, $\mathcal{B}_1$ answers the hash queries, corruption queries and signing queries of $\mathcal{A}_1$ as follows:

- *Hash Query to* $H_1(m_j)$: $\mathcal{B}_1$ returns a random $\mathbf{y}_j \in \mathbb{Z}_q^n$ to $\mathcal{A}_1$ and stores $\langle m_j, \mathbf{y}_j \rangle$ in list-H_1.
- $\mathsf{Corrupt}(i) : \mathcal{B}_1$ looks for the tuple $\langle i, \mathbf{A}_i, \mathbf{B}_i \rangle$ in list G and returns $\mathbf{B}_i$ to $\mathcal{A}_1$.
- $\mathsf{Sign}\ (R_j, i, M_j) : \mathcal{B}_1$ computes the signature $\mathbf{e}_j \leftarrow \mathsf{GenSamplePre}(\mathbf{A}_{R_j}, \mathbf{B}_i, \mathbf{y}_j, r)$ and returns $\mathbf{e}_j$ to $\mathcal{A}_1$.

At some point, $\mathcal{A}_1$ provides $< i_0, i_1, R^*, M^* >$ such that M^* is a message to be signed with the ring R^*, and i_0 and i_1 are indices with $pk_{i_0}, pk_{i_1} \in R^*$. $\mathcal{B}_1$ chooses a bit $b^* \leftarrow \{0,1\}$, and retrieves the tuple $\langle M^*, \mathbf{y}^* \rangle$ in list-H_1. Then $\mathcal{B}_1$ computes the challenge signature $\mathbf{e}^* \leftarrow \mathsf{GenSamplePre}(\mathbf{A}_{R^*}, \mathbf{A}_{i_{b^*}}, \mathbf{B}_{i_{b^*}}, \mathbf{y}^*, r)$ (here l is the size of the ring R^*), and provides $\mathcal{A}_1$ with $\mathbf{e}^*$. Finally, the adversary $\mathcal{A}_1$ outputs a guess $b' \in \{0,1\}$. In the view of $\mathcal{A}_1$, the behavior of $\mathcal{B}_1$ is statistically close to the one provided by the real adaptive security experiment. Observe that the ring members in R^* construct a one-way function $f_{\mathbf{A}_{R^*}}(\mathbf{e}) = \mathbf{A}_{R^*}\mathbf{e} \bmod q$: with the domain $D_{R^*} = \{\mathbf{e} \in \mathbb{Z}^{lm} : \|\mathbf{e}\| \leq r\sqrt{lm}\}$ and $\mathbb{Z}_q^n$. If $\mathcal{A}_1$ exhibits a different success probability in distinguishing between i_0 and i_1 with non-negligible probability, it will contradict with the lemma 1. Hence, we claim that the adversary $\mathcal{A}_1$ in the anonymity game under the simulated environment has negligible advantage to guess the correct identity.

Unforgeability: The unforgeability proof closely follows the proof for the original lattice signature scheme given by Gentry, Peikert, and Vaikuntanathan [17].

Theorem 2. *Our ring signature scheme is unforgeable with regard to the insider corruption assuming that* H_1 *is collision resistant and* $\mathsf{SIS}_{q,lm,r}$ *is hard (l is a guess for the size of the challenge ring).*

Proof: Let $\mathcal{A}_2$ be an adversary that breaks the unforgeability of the ring signature scheme with probability $\epsilon = \epsilon(n)$. We construct a poly-time adversary $\mathcal{B}_2$ that solves $\mathrm{SIS}_{q,lm,r}$ with probability

$$\mathsf{Adv}_{q,r}^{\mathrm{SIS}}(\mathcal{B}_2) \geq \frac{\mathsf{Adv}_l^{RS}(\mathcal{A}_2)}{q_E \mathrm{C}_{q_E}^{q_E/2}} - \mathrm{negl}$$

Both the adversary $\mathcal{A}_2$ and the challenger $\mathcal{B}_2$ are given as input q_E, the total number of extraction queries that can be issued by $\mathcal{A}_2$. $\mathcal{B}_2$ interacts with $\mathcal{A}_2$ as follows:

Setup : $\mathcal{B}_2$ chooses $l \in [q_E]$, a guess for the size of the challenge ring. Next $\mathcal{B}$ obtains an instance $\mathbf{A}_R \in \mathbb{Z}_q^{n \times lm}$ from the SIS oracle and parses it as $\mathbf{A}_{i^*} \in \mathbb{Z}_q^{n \times m}$ $(1 \leq i^* \leq l)$. $\mathcal{B}_2$ then picks a vector $\mathbf{t} = (t_1, ..., t_l) \in [q_E]$. To respond to $\mathcal{A}_2$'s hash queries and signing queries in the random oracle, $\mathcal{B}_2$ will maintain two lists H_1 and $\mathcal{G}$, which are initialized to be empty and will store tuples of values. For $1 \leq i \leq q_E$ and $i \notin \mathbf{t}$, $\mathcal{B}_2$ runs the algorithm $\mathsf{TrapGen}$ to generate $\mathbf{A}_i \in \mathbb{Z}_q^{n \times m}$ with the corresponding short basis $\mathbf{B}_i \in \mathbb{Z}^{m \times m}$ and stores the tuple $\langle i, \mathbf{A}_i, \mathbf{B}_i \rangle$ in list $\mathcal{G}$. For $1 \leq i \leq q_E$ and $i = t_j \in \mathbf{t}$, $\mathcal{B}_2$ sets $\mathbf{A}_i = \mathbf{A}_{j^*} \in \mathbb{Z}_q^{n \times m}$. The system parameters $< \mathbf{A}_1 \| ... \| \mathbf{A}_{q_E}] >$ are given to $\mathcal{A}_2$.

Query Phase: $\mathcal{B}_2$ answers the hash queries, corruption queries and signing queries of $\mathcal{A}_2$ as follows:

- *Hash Query to* $H_1(m_j)$. $\mathcal{B}_2$ chooses a random $\mathbf{e}_j \leftarrow D_{lm,r}$ by running the algorithm $\mathsf{SampleDom}(1^n)$, returns $\mathbf{y}_j \leftarrow \mathbf{A}_R\mathbf{e}_j \bmod q \in \mathbb{Z}_q^n$ to $\mathcal{A}_2$ and stores $\langle m_j, \mathbf{e}_j, \mathbf{y}_j\rangle$ in list-H_1.
- *Corruption Query* (i). If $i \notin \mathbf{t}$, $\mathcal{B}_2$ looks for the tuple $\langle i, \mathbf{A}_i, \mathbf{B}_i\rangle$ in list G and returns $\mathbf{B}_i$ to $\mathcal{A}_2$. Otherwise, $\mathcal{B}_2$ aborts.
- *Signing query*(i, m_j, R_j). It can be assumed, without loss of generality, that $\mathcal{A}_2$ has made a H_1 query on m_j. If $R_j = R$, $\mathcal{B}_2$ searches the tuple $\langle m_j, \mathbf{e}_j\rangle$ in list-H_1 and returns $\mathbf{e}_j$ to $\mathcal{A}_1$. Otherwise if the tuple $\langle i, \mathbf{A}_i, \mathbf{B}_i\rangle$ contains in list $\mathcal{G}$, $\mathcal{B}_2$ retrieves the tuple $\langle m_j, \mathbf{e}_j, \mathbf{y}_j\rangle$ in list-H_1 and then returns $\sigma_j \leftarrow \mathsf{GenSamplePre}(\mathbf{A}_{R_j}, \mathbf{A}_i, \mathbf{B}_i, \mathbf{y}_j, r)$ to $\mathcal{A}_2$. Otherwise, $\mathcal{B}_2$ looks for a $j \in R_j$ such that $\langle j, \mathbf{A}_j, \mathbf{B}_j\rangle$ contains in list $\mathcal{G}$. $\mathcal{B}_2$ then computes $\sigma_j \leftarrow \mathsf{GenSamplePre}(\mathbf{A}_{R_j}, \mathbf{A}_j, \mathbf{B}_j, \mathbf{y}_j, r)$ and returns σ_j to $\mathcal{A}_2$.

Challenge : Finally, $\mathcal{A}_2$ outputs a forgery $\langle i^*, m^*, \sigma^*, R^*\rangle$. If $R^* \neq R$, $\mathcal{B}_2$ aborts. Otherwise, $\mathcal{B}_2$ looks up the tuple $\langle m^*, e^*, y^*\rangle$ in list-H_1 and output $\langle \sigma^*, e^*\rangle$ as a collision of m^* in $f_{\mathcal{A}_R}$

Analysis. It is easy to see that the probability of an abort is $1-\frac{1}{q_E C_{q_E}^{q_E/2}}$. We claim that the view of $\mathcal{A}_2$ in the adaptively chosen message attack is identical to its view as provided by $\mathcal{B}_2$. For each distinct query m_j to H_1, the value returned by $\mathcal{B}_2$ is $f_{\mathcal{A}_R}(e_j) \in \mathbb{Z}_q^n$ where $e_j \leftarrow \mathsf{SampleDom}(1^n)$; by the uniform output property of the constructed hash function, this is identical to the uniformly random value of $H_1(m_j) \in \mathbb{Z}_q^n$ in the real environment. Therefore $\mathcal{A}_2$ outputs a valid forgery $\langle m^*, \sigma^*\rangle$ with probability (negligibly close to) ϵ.Because σ^* is a valid signature of the ring on m^*, we have $\sigma^* < r\sqrt{lm}$ and $f_{\mathcal{A}_R}(\sigma^*) = H_1(m^*) = f_{\mathcal{A}_R}(e^*)$, and they form a collision in $f_{\mathcal{A}_R}$.

3.5 Ring Signature in the Standard Model

Recently, Boyen [28] proposed a framework for fully secure lattice-based signatures in the standard model. Using the method in [28] , we can extend our work to a ring signature in the standard model as follows.

Setup(l, d): For some integers l, d and t, the following construction assumes that messages M are arbitrary $d+1$-bit strings in $\{0\} \times \{0,1\}^d$. Choose $d+1$ independent matrix $\mathbf{C}_0, ..., \mathbf{C}_d \in \mathbb{Z}_q^{n\times tm}$.

KeyGen(l): As in the basic construction in section 3.2.

Ring-Sign(R, sk_i, M): Given a ring with public keys $R = \{\mathbf{A}_1, ..., \mathbf{A}_l\} \in \mathbb{Z}_q^{n\times m}$, a user i's$(i \in [l])$ private key $sk_i = \mathbf{B}_i$, and a message $M \in \{0\} \times \{0,1\}^d$, the user i does the following:

- Set $\mathbf{C}_m = \sum_{i=0}^{d}(-1)^{M[i]}\mathbf{C}_i$.

- Set $\mathbf{A}_R$=$[\mathbf{A}_1\|...\|\mathbf{A}_l\|\mathbf{C}_m] \in \mathbb{Z}_q^{n\times(l+t)m}$. Define a label lab_R that contains information about how $\mathbf{A}_R$ is associated with the sequence of the ring numbers $\{1, ..., l\}$.
- Run the generalized preimage sampling algorithm $\mathsf{GenSamplePre}$ and generate $\mathbf{e} \leftarrow \mathsf{GenSamplePre}(\mathbf{A}_R, \mathbf{A}_i, \mathbf{B}_i, 0, r) \in \mathbb{Z}^{(l+t)m}$. Note that $\mathbf{e}$ is distributed according to $D_{\Lambda^\perp \mathbf{A}_R, r}$.
- Output the ring signature $\sigma =< \mathbf{e}, lab_R >$.

Ring-Verify(σ, M): Given a ring of public keys $R = \{\mathbf{A}_1, ..., \mathbf{A}_l\} \in \mathbb{Z}_q^{n\times m}$, a message $M \in \{0\} \times \{0,1\}^d$, and a ring signature $\sigma =< \mathbf{e}, lab_R >$, the verifier accepts the signature only if both the following conditions satisfied:
- $0 \le \|\mathbf{e}\| \le r\sqrt{(l+t)m}$
- $[\mathbf{A}_1\|...\|\mathbf{A}_l\|\sum_{i=0}^{d}(-1)^{M[i]}\mathbf{C}_i]\mathbf{e} = 0 \bmod q$.

Otherwise, the verifier rejects.

Security Analysis The scheme holds full anonymity and unforgeability in the standard model. The security proof involves the following two lemmas in [28].

Lemma 2. *Let $\mathbf{A}_0, \mathbf{A}_1 \in \mathbb{Z}_q^{n\times m}$ where $\mathbf{A}_1$ is rank n with a basis $\mathbf{B}_1$ of $\Lambda^\perp(\mathbf{A}_1)$ ($\|\tilde{\mathbf{B}}_1\| \le L$). Let $\mathbf{R}_0 \in \{0,1\}^{m\times m}$ and $\mathbf{F}_2 = [\mathbf{A}_0|\mathbf{A}_0\mathbf{R}_0 + \mathbf{A}_1]$. There is a PPT algorithm $\mathsf{SampleRight}(\mathbf{A}_0, \mathbf{A}_1, \mathbf{R}_0, \mathbf{B}_1, \mathbf{y}, r(2))$ that outputs a vector $\mathbf{e} \in \mathbb{Z}^{2m}$ sampled from a distribution statically close to $D_{\Lambda_{\mathbf{y}}^\perp(\mathbf{F}_2), r(2)}$.*

Lemma 3. *Let $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{H} \in \mathbb{Z}_q^{n\times n}$. Suppose that $\mathbf{H}$ is invertible modulo q. Then, the preimage-samplable functions $\mathbf{A}_0$ mod q and $\mathbf{H}\mathbf{A}_0$ mod q admit exactly the same trapdoors $\mathbf{B}_0 \in \mathbb{Z}^{m\times m}$ for $\Lambda^\perp(\mathbf{A}_0)$.*

Unforgeability: The unforgeability proof closely follows the combination of the methods in the proof of Theorem 4 and the proof of Theorem 23 in [28]. We will give the details in the full version of the paper.

Theorem 3. *Our ring signature scheme is unforgeable with regard to the insider corruption assuming that $\mathsf{SIS}_{q,m,r}$ is hard.*

Proof: Let $\mathcal{A}_2$ be an adversary that breaks the unforgeability of the ring signature scheme with probability $\epsilon = \epsilon(n)$. We construct a poly-time adversary $\mathcal{B}_2$ that solves $\mathrm{SIS}_{q,m,r}$ with probability

$$\mathsf{Adv}_{q,r}^{\mathrm{SIS}}(\mathcal{B}) \ge \frac{\mathsf{Adv}_l^{RS}(\mathcal{A}_1)}{q_E \mathrm{C}_{q_E}^{q_E/2}} - \mathrm{negl}$$

4 Identity Based Ring Signature

4.1 Basic Construction

Let k, l, m, n, q, t be positive integers with $q \ge 2$ and $m \ge 5n\log q$. Let $k \le l$, where l is the size of the ring set. The identity-based ring signature scheme involves the following parameters L, L_1,r_1 as in [10]:

- $\widetilde{L} \geq O(\sqrt{n \log q})$: an upper bound of the Gram-Schmidt size of the KGC's secret basis;
- $\widetilde{L_1} \geq \widetilde{L} \cdot O(\sqrt{n \log q}) \cdot \omega(\sqrt{\log n})$: an upper bound of the Gram-Schmidt size of a user's secret basis;
- $r_1 \geq \widetilde{L_1} \cdot \omega(\sqrt{\log n})$: a Gaussian parameter used to generate the secret basis and short vectors.

The scheme employs two hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^n$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^{n \times m}$. The security analysis will view H_1, H_2 as random oracles.

Setup(λ, l): The KGC runs the trapdoor generation algorithm $\mathsf{TrapGen}$ (described in section 2.4) to generate $\mathbf{A}_0 \in \mathbb{Z}_q^{n \times m}$ with a basis $\mathbf{B}_0 \in \mathbb{Z}^{m \times m}$ for $\Lambda^{\perp}(\mathbf{A}_0)$ such that $(\|\widetilde{\mathbf{B}_0}\| \leq \widetilde{L})$. Output the system public parameters $\mathtt{PK} =< \mathbf{A}_0, H_1, H_2 >$ and the KGC's master key $\mathtt{MSK} = \mathbf{B}_0$.

Extract$(\mathtt{MSK}, ID_i)$: For an arbitrary identity $ID_i \in \{0,1\}^*$, define the associated matrix $\mathbf{Q}_{ID_i}$ as

$$\mathbf{Q}_{ID_i} = [\mathbf{A}_0 \| \mathbf{A}_{ID_i}] \in \mathbb{Z}_q^{n \times 2m}$$

where $\mathbf{A}_{ID_i} = H_2(ID_i) \in \mathbb{Z}_q^{n \times m}$. Generate $\mathbf{B}_{ID_i} \leftarrow \mathsf{RandBasis}(\mathsf{ExtBasis}(\mathbf{Q}_{ID_i}, \mathbf{B}_0), r_1)$, which is a short basis for $\Lambda^{\perp}(\mathbf{Q}_{ID_i})$. Note that by Theorem 1 we have $\|\widetilde{\mathbf{B}}_{ID_i}\| \leq \widetilde{L_1}$. The secret key for ID_i is $\mathbf{B}_{ID_i}$.

Ring-Sign(R, sk_i, M): Given a ring R of identities, assume for notational simplicity that $R = \{ID_1, ..., ID_l\} \in \{0,1\}^*$, a user ID_i's secret key $\mathbf{B}_i$ $(i \in [l])$, and a message $M \in \{0,1\}^*$, the user i does the following:

- Set $\mathbf{A}_R$=$[\mathbf{A}_0 \| \mathbf{A}_1 \| ... \| \mathbf{A}_l] \in \mathbb{Z}_q^{n \times (l+1)m}$, where $\mathbf{A}_i = H_2(ID_i) \in \mathbb{Z}_q^{n \times m} (1 \leq i \leq l)$ and $\mathbf{y} = H_1(M) \in \mathbb{Z}_q^n$. Define a label lab_R that contains information about how $\mathbf{A}_R$ is associated with the sequence of the ring numbers $\{ID_1, ..., ID_i\}$.
- Generate $\mathbf{e} \leftarrow \mathsf{GenSamplePre}(\mathbf{A}_R, \mathbf{Q}_{ID_i}, \mathbf{B}_i, \mathbf{y}, r) \in \mathbb{Z}^{lm}$. Note that $\mathbf{e}$ is distributed according to $D_{\Lambda_{\mathbf{y}}^{\perp} \mathbf{A}_R, r}$.
- Output the ring signature $\sigma =< \mathbf{e}, lab_R >$.

Ring-Verify(σ, M): Given a ring of public keys $R = \{\mathbf{A}_1, ..., \mathbf{A}_l\} \in \mathbb{Z}_q^{n \times m}$, a message M, and a ring signature $\sigma =< \mathbf{e}, lab_R >$, the verifier accepts the signature only if both the following conditions satisfied:

- $\mathbf{e} \in D_{lm,r}$ such that $0 \leq \|\mathbf{e}\| \leq r_1 \sqrt{(l+1)m}$
- $\mathbf{A}_R \mathbf{e} \bmod q = H_2(M)$.

Otherwise, the verifier rejects.

Our identity-based ring scheme holds full anonymity and unforgeability in the random orale model. The security analysis of our identity-based ring signature scheme is similar to the analysis of our ring signature presented in Section 3. We will give the details in the full version of the paper.

4.2 Identity-Based Ring Signature in the Standard Model

Agrawal et al. [29] recently showed how to construct efficient IBE in the standard model based on LWE assumption. The construction involved two distinct trap doors in the security proof. Using the similar technique in [28,29] , we can modify our basic IBRS construction to obtain an identity-based ring signature scheme in the standard model as follows:

- The construction assumes that messages M are arbitrary string in $\{0\} \times \{0,1\}^d$. Choose $d+1$ independent matrix $\mathbf{C}_0, ..., \mathbf{C}_d \in \mathbb{Z}_q^{n \times m}$.
- Each identity ID_i is presented as elements in $\mathbb{Z}_q^n$ and then mapped to matrices in $\mathbb{Z}_q^{n \times n}$ using an encoding function $H_2 : \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q^{n \times n}$ (defined in [29]).
- In the algorithm Setup, the KGC selects two uniformly random matrices $E_0, E_1 \in \mathbb{Z}_q^{n \times m}$. For an arbitrary identity $ID_i \in \mathbb{Z}_q^n$, define $\mathbf{Q}_{ID_i} = [\mathbf{A}_0 \| \mathbf{E}_0 + H_2(ID_i)\mathbf{E}_1] \in \mathbb{Z}_q^{n \times 2m}$. As in the basic IBBE in section 3, a trapdoor for $\mathbf{A}_0$ is used as the master secret and enables one to generate private keys for $\mathbf{Q}_{ID_i}$.
- In order to sign a message $M \in \{0\} \times \{0,1\}^d$ for a ring $R = \{ID_1, ..., ID_l\}$, the user $ID_i (i \in [l])$ does the following:
  - Set $\mathbf{C}_m = \sum_{i=0}^{d} (-1)^{M[i]} \mathbf{C}_i$.
  - Let $\mathbf{A}_R = [\mathbf{A}_0 \| \mathbf{E}_0 + H_2(ID_1)\mathbf{E}_1 \| ... \| \mathbf{E}_0 + H_2(ID_l)\mathbf{E}_1 \| \mathbf{C}_m]$
  - Generate $\mathbf{e} \leftarrow \mathsf{GenSamplePre}(\mathbf{A}_R, \mathbf{Q}_{ID_i}, \mathbf{B}_i, 0, r) \in \mathbb{Z}^{(l+2)m}$. Note that $\mathbf{e}$ is distributed according to $D_{\Lambda^{\perp}_{\mathbf{A}_R}, r}$.
- The verifier accepts the signature only if both the following conditions satisfied:
  - $0 \leq \|\mathbf{e}\| \leq r\sqrt{(l+t)m}$
  - $\mathbf{A}_R \mathbf{e} = 0 \bmod q$.

  Otherwise, the verifier rejects.

Security. The above IBRS scheme holds full anonymity and unforgeability in the standard model. The security analysis is similar to the analysis of our ring signature presented in Section 3. We will give the details in the full version of the paper.

References

1. Abe, M., Ohkubo, M., Suzuki, K.: 1-out-of-n Signatures from a Variety of Keys. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 415-432. Springer, Heidelberg (2002)
2. Au, M.H., Liu, J.K., Yuen, T.H., Wong, D.S.: Id-based Ring Signature Scheme Secure in the Standard Model. In: Yoshiura, H., Sakurai, K., Rannenberg, K., Murayama, Y., Kawamura, S.-i. (eds.) IWSEC 2006. LNCS, vol. 4266, pp. 1-16. Springer, Heidelberg (2006)
3. Alwen, J., Peikert, C.: Generating shorter bases for hard random lattices. In: Proc. of STACS 2009, pp. 75-86 (2009)
4. Ajtai, M., Dwork, C.: A public-key cryptosystem with worst-case/average-case equivalence. In: STOC, pp. 284-293 (1997)

5. Ajtai, M.: Generating hard instances of the short basis problem. In: Wiedermann, J., Van Emde Boas, P., Nielsen, M. (eds.) ICALP 1999. LNCS, vol. 1644, pp. 1-9. Springer, Heidelberg (1999)
6. Agrawal, S.,Boyen, S. Identity-based encryption from lattices in the standard model. In manuscript, 2009.
7. Bresson, E., Stern, J., Szydlo, M.: Threshold Ring Signatures and Applications to Ad-hoc Groups. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 465-480. Springer, Heidelberg (2002)
8. Bender, A., Katz, J., Morselli, R.: Ring signatures: Stronger definitions, and constructions without random oracles. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 60-79. Springer, Heidelberg (2006)
9. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213-229. Springer, Heidelberg (2001)
10. Cash, D.,Hofheinz,D.,Kiltz,E.: How to delegate a lattice basis.In: Halevi, S. (ed.) CRYPTO rumption (2009). Cryptology ePrint Archive, Report 2009/351 (2009), http://eprint.iacr.org/2009/351
11. Cha, J.C., Cheon, J.H.: An identity-based signature from gap Diffie-Hellman groups. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 18-30. Springer, Heidelberg (2002)
12. Chow, S.S.M., Yiu, S.M., Hui, L.C.K.: Efficient Identity Based Ring Signature. In: Ioannidis, J., Keromytis, A., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 499-512. Springer, Heidelberg (2005)
13. Chow, S.S.M.,Wei, V.K., Liu, J.K., Yuen, T.H.: Ring Signatures without Random Oracles. In: ASIACCS'06: Proceedings of the 2006 ACM Symposium on Information, Taipei, Taiwan. Computer and Communications Security, pp. 297-302. ACM Press, New York (2006)
14. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: IMA Int. Conf., pp. 360-363 (2001)
15. Delerabl'ee, C.: Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 200-215. Springer, Heidelberg (2007)
16. Gentry, C.: Practical Identity-Based Encryption Without Random Oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445-464. Springer, Heidelberg (2006)
17. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC, pp. 197-206 (2008)
18. Herranz, J., Saez, G.: Forking lemmas for ring signature schemes. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 266-279. Springer, Heidelberg (2003)
19. Herranz, J., Saez, G.: New Identity-based Ring Signature Schemes. In: Lopez, J., Qing, S., Okamoto, E. (eds.) ICICS 2004. LNCS, vol. 3269, pp. 27-39. Springer, Heidelberg (2004)
20. Liu, D.Y.W., Liu, J.K., Mu, Y., Susilo, W., Wong, D.S.: Revocable ring signature. J. Comput. Sci. Technol. 22(6),785-794, 2007.
21. Micciancio, D., Regev, O.:Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput. 37(1), 267-302 (2007); Preliminary version in FOCS 2004
22. Peikert, C.: Bonsai Trees:Arboriculture in Lattice-Based Cryptography. In manuscript, 2009.

23. Rivest, R.L., Shamir, A., Tauman, Y.: How to Leak a Secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552-565, Springer, Heidelberg (2001).
24. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC, pp. 84-93 (2005)
25. Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47-53. Springer, Heidelberg (1985)
26. Shacham, H., Waters, B.: Efficient ring signatures without random oracles. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 166-180, Springer-Verlag, 2007.
27. Zhang, F., Kim, K.: ID-Based Blind Signature and Ring Signature from Pairings. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 533-547. Springer, Heidelberg (2002)
28. Boyen, X.: Lattice Mixing and Vanishing Trapdoors: A Framework for Fully Secure Short Signatures and More. In: P.Q.Nguyen(eds.) PKC 2010. LNCS, vol 6056,pp. 499-517,Springer, Heidelberg (2010)
29. Agrawal, S., Boneh, D., and Boyen, X.: Ecient lattice (H)IBE in the standard model. In: Gilbert H.(ed.): EUROCRYPT 2010, LNCS, vol.6110, pp. 553-572. Springer, Heidelberg (2010)
30. M. Au, J. K. Liu, P. P. Tsang, and D. S. Wong. A suite of id-based threshold ring signature schemes with different levels of anonymity. Cryptology ePrint Archive, Report 2005/326, 2005. http://eprint.iacr.org/.
31. Brakerski, Z., Kalai, Y.T.: A framework for efficient signatures, ring signatures and identity based encryption in the standard model. Cryptology ePrint Archive, Report 2010/086 (2010)