Scalable Hierarchical Identity-based Signature Scheme from Lattices

Geontae Noh and Ik Rae Jeong
CIST (Center for Information Security Technologies), Korea University
Anam-dong, Seongbuk-gu, Seoul 136-713, Korea
[e-mail: oldos@korea.ac.kr, irjeong@korea.ac.kr]
*Corresponding author: Ik Rae Jeong

Received August 17, 2013; revised October 25, 2013; accepted November 20, 2013;
published December 27, 2013

Abstract

In the paper, we propose a novel adaptively secure hierarchical identity-based signature scheme from lattices. The size of signatures in our scheme is shortest among the existing hierarchical identity-based signature schemes from lattices. Our scheme is motivated by Gentry et al.'s signature scheme and Agrawal et al.'s hierarchical identity-based encryption scheme.

Keywords: Hierarchical identity-based signatures, adaptive identity security, strong unforgeability, lattice-based cryptography, provable security

This research was partly supported by Basic Science Research Programs through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(NRF-2012R1A1A3005550, 2013R1A2A2A01068200) and the IT R&D program of MOTIE/KEIT [KI002113, Development of Security Technology for Car-Healthcare].

http://dx.doi.org/10.3837/tiis.2013.12.017

1. Introduction

In 1984, Shamir introduced the concept of identity-based cryptography and proposed an identity-based signature scheme [1]. In an identity-based signature scheme, a trusted third party, called KGC (key generation center), only issues a signer's secret key, because the signer's public key is the signer's identity such as an email address and a phone number related to the signer. That is, the public key distribution problem (or the certification management problem) is eliminated. When a verifier wants to verify a signature, therefore, the verifier does not need to ask the KGC for the signer's public key, because the verifier can easily deduce the signer's public key from the signer's identity. Actually, many identity-based signature schemes have been studied [2][3][4].

The concept of hierarchical identity-based signatures is the hierarchical extension of identity-based signatures. Like an identity-based signature scheme, the KGC issues a signer's secret key. In addition, the signer can delegate the secret keys of the signer's child identities in an identity hierarchy using its own secret key.

In 2002, Gentry and Silverberg proposed the first hierarchical identity-based signature scheme from bilinear pairings, but the security is not formally proved [5]. Since then, Chow et al. proposed the first provably secure hierarchical identity-based signature scheme from bilinear pairings [6]. However, these schemes are not resistant to quantum analysis [7].

So far, lattice-based cryptography is believed to be resistant to quantum analysis. Lattice-based cryptography is also asymptotically efficient because it requires only linear operations.

In 2010, Ruckert proposed two binary tree signature[1] schemes from lattices, but both of them increase the size of the signatures by the level of hierarchy [8]. In 2012 & 2013, Tian et al. and Liu et al. proposed hierarchical identity-based signature schemes from lattices, but their schemes are insecure against adaptive identity attacks [9][10]. In 2013, Tian et al. proposed another hierarchical identity-based signature scheme from lattices [11]. In Tian et al.'s hierarchical identity-based signature scheme, however, the size of signatures depends on both the security parameter and the dimension of the lattices. We compare our scheme and existing hierarchical identity-based signature schemes from lattices in **Table 1**. The size of signatures in our scheme is shortest among the existing hierarchical identity-based signature schemes from lattices.

Table 1. Comparison of security and efficiency

	ROM / STM	**DoS**	**SI / AI**	**BTS / HIBS**
[8] #1	ROM	$(1+l)\cdot m+n$	AI	BTS
[8] #2	STM	$(1+l+h)\cdot m+n$	SI	BTS
[9]	STM	$m+n$	SI	HIBS
[10]	STM	$(2+l)\cdot m+n$	SI	HIBS
[11]	ROM	$m+n$	AI	HIBS
Our Scheme	ROM	m	AI	HIBS

[1] Binary tree signature is the special case of hierarchical identity-based signature with identity space $\{0,1\}$.

ROM means the scheme is probably secure in the random oracle model and STM means the scheme is probably secure in the standard model. DoS is the dimension of the signatures, n is the security parameter, m is the dimension of the lattices, l is the depth of the identities, and h is the bit length of the hash values for messages. SI means the scheme is secure against selective identity attacks and AI means the scheme is secure against adaptive identity attacks. BTS means the scheme is a binary tree signature scheme and HIBS means the scheme is a hierarchical identity-based signature scheme.

1.1 Our Contribution

In this paper, we propose a hierarchical identity-based signature scheme from lattices. Our scheme is adaptively secure and the size of signatures in our scheme is shortest among the existing hierarchical identity-based signature schemes from lattices. Our scheme is motivated by Gentry et al.'s signature scheme and Agrawal et al.'s hierarchical identity-based encryption scheme [12][13]. The security of our scheme is based on the SIS problem on lattices in the random oracle model.

1.2 Organization

The remainder of this paper is organized as follows: Some preliminaries such as the properties of the lattices and the definitions for hierarchical identity-based signatures are presented in Section 2. Our hierarchical identity-based signature scheme is given in Section 3. We analyze our hierarchical identity-based signature scheme in Section 4. Finally, Section 5 draws the conclusion.

2. Preliminaries

2.1 Notations

We let $\mathbb{Z}$ and $\mathbb{R}$ denote the integers and the real numbers, respectively. For any positive integer $q \geq 2$, we let $\mathbb{Z}_q$ denote the ring of integers modulo q. For any positive integer k, we let $[k] = \{1, \cdots, k\}$. We use upper-case letters (e.g., A) to denote matrices and lower-case letters (e.g., v) to denote vectors. We let 0 denote a zero vector.

We let $\| v \|$ denote the Euclidean norm of v. We let $\tilde{S}$ denote the Gram-Schmidt orthogonalization of S. The statistical distance between two distributions X and Y over a countable domain $\mathbb{D}$ is $\frac{1}{2} \cdot \sum_{i \in \mathbb{D}} | X(i) - Y(i) |$. If v is chosen uniformly at random from $\mathbb{D}$, we denote $v \leftarrow \mathbb{D}$.

We use standard big-O notation. For sufficiently large n, if $f(n)$ is smaller than all polynomial fractions, then we say that a function $f : \mathbb{R}^+ \to \mathbb{R}^+$ is negligible. $\Pr[\text{an event}]$ is the probability that the event occurs.

2.2 Lattices

First, we define m-dimensional full-rank integer lattices. An m-dimensional full-rank integer lattice Λ for m linearly independent basis vectors $B = \{b_1, \cdots, b_m\} \subset \mathbb{Z}^m$ is defined as follows:

$$\Lambda = \left\{ B \cdot c : c \in Z^m \right\}. \tag{1}$$

We define the dual lattice Λ^* of Λ as follows:

$$\Lambda^* = \left\{ x \in Z^m : \forall y \in \Lambda, \langle x, y \rangle \in Z^m \right\}. \tag{2}$$

In this paper, we use an m -dimensional q -ary integer lattice which is one of m -dimensional full-rank integer lattices. Let $n \geq 1$ and $q \geq 2$ be positive integers. An m -dimensional q -ary integer lattice $\Lambda^{\perp}(A)$ for a uniformly random matrix $A \in Z_q^{n \times m}$ is defined as follows:

$$\Lambda^{\perp}(A) = \left\{ x \in Z^m : A \cdot x = 0 \in Z_q^n \right\}. \tag{3}$$

We define the coset $\Lambda_u^{\perp}(A)$ of $\Lambda^{\perp}(A)$ for a syndrome $u \in Z_q^n$ as follows:

$$\Lambda_u^{\perp}(A) = \left\{ x \in Z^m : A \cdot x = u \in Z^m \right\}. \tag{4}$$

2.2.1 Hard Problems

We define the SIS (short integer solution) problem which is used to analyze the security of our construction.

Definition 2.1. An instance of the $\text{SIS}_{q,\beta}$ problem is a uniformly random matrix $A \in Z_q^{n \times m}$. Then, the $\text{SIS}_{q,\beta}$ problem is to find a non-zero vector $z \in Z^m$ such that $A \cdot z = 0 \in Z_q^n$ and $\| z \| \leq \beta$.

In case of $q \geq \beta \cdot \sqrt{n} \cdot \omega\left(\sqrt{\log n}\right)$, the classic average-case $\text{SIS}_{q,\beta}$ problem is reduced to the worst-case SIVP (shortest independent vectors problem) [12][14][15].

2.2.2 Gaussian Distributions

We recall Gaussian distributions [12][15].

Definition 2.2. For any positive integer $s \in \mathbb{R}$, a Gaussian function ρ_s with center 0 is defined as follows:

$$\rho_s = \exp\left(-\pi \cdot \| x \|^2 / s^2\right). \tag{5}$$

Definition 2.3. Let $\Lambda \subset Z^m$ be an m-dimensional full-rank integer lattice. For any positive integer $s \in \mathrm{R}$, the discrete integral of ρ_s over Λ is defined as follows:

$$\rho_s(\Lambda) = \sum\nolimits_{x \in \Lambda} \rho_s(x). \tag{6}$$

Definition 2.4. Let $\Lambda \subset Z^m$ be an m-dimensional full-rank integer lattice. For any positive integer $s \in \mathrm{R}$ and all $x \in \Lambda$, the discrete Gaussian distribution over Λ with center 0 is defined as follows:

$$D_{\Lambda,s}(x) = \rho_s(x) / \rho_s(\Lambda). \tag{7}$$

Definition 2.5. Let $\Lambda \subset Z^m$ be an m-dimensional full-rank integer lattice and Λ^* a dual lattice of Λ. For any positive real number $\varepsilon \in \mathrm{R}$, a Gaussian parameter $\eta_\varepsilon(\Lambda)$ is the smallest s such that $\rho_{1/s}\left(\Lambda^* \setminus \{0\}\right) \le \varepsilon$.

Next, we recall the following useful facts.

Fact 2.1 [12][15][16]. Let $S \in Z^{m \times m}$ be a basis for $\Lambda^\perp(A)$ and $A \in Z_q^{n \times m}$ a uniformly random matrix. For any $s \ge \|\tilde{S}\| \cdot \omega(\sqrt{n})$ and any syndrome $u \in Z_q^n$, the probability that $\|x\| > s \cdot \sqrt{m}$ is negligible for n, where $x \leftarrow \mathrm{D}_{\Lambda_u^\perp(A),s}$.

Fact 2.2 [12][15][16]. Let $S \in Z^{m \times m}$ be a basis for $\Lambda^\perp(A)$ and $A \in Z_q^{n \times m}$ a uniformly random matrix. For any $s \ge \|\tilde{S}\| \cdot \omega(\sqrt{n})$, the probability that x is a zero vector is negligible for n, where $x \leftarrow \mathrm{D}_{\Lambda^\perp(A),s}$.

Fact 2.3 [13][17]. Let $A \in Z_q^{n \times m}$ be a uniformly random matrix, q a prime, and $R \leftarrow \mathrm{D}_{Z^{m \times m},s}$ a Z_q-invertible matrix. For any $s \ge \omega(\sqrt{\log n})$, two matrices $A \cdot R \in Z_q^{n \times m}$ and $A \cdot R^{-1} \in Z_q^{n \times m}$ are also uniformly random.

2.2.3 Basic Algorithms

We review basic algorithms which are used to construct our construction and to analyze the security of our construction.

Lemma 2.1 [18]. For positive integers $n \ge 1$, $q \ge 2$, and $m = O(n \log q)$, a probabilistic polynomial time algorithm BasisGen$(1^n, 1^m, q)$ outputs a pair $(A \leftarrow Z_q^{n \times m}, S \in Z^{m \times m})$ of a uniformly random matrix and a short basis for $\Lambda^\perp(A)$ such that $\|\tilde{S}\| \le O(\sqrt{n \log q})$.

Lemma 2.2 [13]. Let $A \in Z_q^{n\times m}$ be a uniformly random matrix, $S \in Z^{m\times m}$ a basis for $\Lambda^{\perp}(A)$, and $R \leftarrow D_{Z^{m\times m},s}$ a Z_q -invertible matrix. For any $s > \|\tilde{S}\| \cdot \sqrt{m} \cdot \sqrt{n\log q} \cdot \omega(\log m)^2$, a probabilistic polynomial time algorithm $\text{BasisDel}(A,R,S,s)$ outputs a basis $S' \in Z^{m\times m}$ for $\Lambda^{\perp}(B)$ such that $\|\tilde{S}'\| = \|\tilde{S}\|$, where $B = A \cdot R^{-1} \in Z_q^{n\times m}$.

Lemma 2.3 [12]. Let m be a positive integer. For any Gaussian parameter s , a probabilistic polynomial time algorithm $\text{SampleDom}(1^m, s)$ outputs a vector $v \leftarrow D_{Z^m,s}$.

Lemma 2.4 [12]. Let $A \in Z_q^{n\times m}$ be a uniformly random matrix, $S \in Z^{m\times m}$ a basis for $\Lambda^{\perp}(A)$, and $u \in Z_q^n$ a syndrome. For any $s \geq \|\tilde{S}\| \cdot \omega(\sqrt{\log n})$, a probabilistic polynomial time algorithm $\text{SampleD}(A,S,u,s)$ outputs a vector $v \leftarrow D_{\Lambda_u^{\perp}(A),s}$.

Lemma 2.5 [13]. Let m be a positive integer. For any $s = \sqrt{n\log q} \cdot \omega(\sqrt{\log m})$, a probabilistic polynomial time algorithm $\text{SampleR}(1^m, s)$ outputs a Z_q -invertible matrix $R \leftarrow D_{Z^{m\times m},s}$.

Lemma 2.6 [13]. Let $A \in Z_q^{n\times m}$ be a uniformly random matrix. For any $s \geq O(\sqrt{n\log q}) \cdot \omega(\sqrt{m})$, a probabilistic polynomial time algorithm $\text{SampleRwithBasis}(A,s)$ outputs a Z_q -invertible matrix $R \leftarrow D_{Z^{m\times m},s}$ and a short basis $S_B \in Z^{m\times m}$ for $\Lambda^{\perp}(B)$ such that $\|\tilde{S}_B\| \leq O(\sqrt{n\log q})$, where $B = A \cdot R^{-1} \in Z_q^{n\times m}$.

2.3 Definitions for Hierarchical Identity-based Signatures

We define hierarchical identity-based signatures. A hierarchical identity-based signature scheme $\text{HIBS} = \{\text{HIBS.Setup}, \text{HIBS.Extract}, \text{HIBS.Sign}, \text{HIBS.Vrfy}\}$ is defined as follows:

- $\text{HIBS.Setup}(1^n, 1^d)$: On input of a security parameter n and the maximum hierarchy depth d , this algorithm outputs a set params of public parameters and a master secret key msk .
- $\text{HIBS.Extract}(\text{params}, sk_{\text{id}_{|l}}, \text{id})$: On input of a set params of public parameters, a secret key $sk_{\text{id}_{|l}}$ of a parent identity $\text{id}_{|l} = (\text{id}_1, \cdots, \text{id}_l)$, and a child identity $\text{id} = (\text{id}_1, \cdots, \text{id}_l, \cdots, \text{id}_c)$, this algorithm outputs a secret key sk_{id} of id . In case of $l = 0$, $sk_{\text{id}_{|l}} = \text{msk}$.
- $\text{HIBS.Sign}(\text{params}, \text{id}, sk_{\text{id}}, \text{m})$: On input of a set params of public parameters, an identity id with its secret key sk_{id} , and a message m , this algorithm outputs a signature σ .

- $\mathrm{HIBS.Vrfy}(\mathrm{params},\mathrm{id},\mathrm{m},\sigma)$: On input of a set params of public parameters, an identity id, a message m, and a signature σ, this algorithm outputs 1 if σ is valid and 0 otherwise.

Correctness. A hierarchical identity-based signature scheme HIBS is correct if, for any valid signature σ on any message m corresponding to any identity id, the $\mathrm{HIBS.Vrfy}(\mathrm{params},\mathrm{id},\mathrm{m},\sigma)$ algorithm outputs 1 with an overwhelming probability.

Unforgeability. A hierarchical identity-based signature scheme HIBS is strongly unforgeable under chosen message and adaptive identity attacks if, in the following game $\mathrm{Game}^{\mathrm{SU}}_{\mathrm{HIBS,F}}(n)$ for a forger F, the advantage $\mathrm{Adv}^{\mathrm{SU}}_{\mathrm{HIBS,F}}(n)$ of F is negligible.

- **Setup**: F is given params, where $(\mathrm{params},\mathrm{msk}) \leftarrow \mathrm{HIBS.Setup}(1^n,1^d)$. Note that params is a set of public parameters and msk is a master secret key.
- **Extract queries**: F queries an identity id_i, adaptively. Then, F receives a secret key sk_{id_i} of id_i.
- **Sign queries**: F queries an identity id_i and a message m_i, adaptively. Then, F receives a signature $\sigma_i \leftarrow \mathrm{HIBS.Sign}(\mathrm{params},\mathrm{id}_i,sk_{\mathrm{id}_i},\mathrm{m}_i)$.
- **Output**: F outputs $(\mathrm{id}^*,\mathrm{m}^*,\sigma^*)$ such that
  - for all i, id_i is not a prefix of id^* in the **Extract queries** and
  - σ^* is not made for $(\mathrm{id}^*,\mathrm{m}^*)$ through the **Sign queries**.

If the $\mathrm{HIBS.Vrfy}(\mathrm{params},\mathrm{id}^*,\mathrm{m}^*,\sigma^*)$ algorithm outputs 1, F wins the game $\mathrm{Game}^{\mathrm{SU}}_{\mathrm{HIBS,F}}(n)$.

The advantage $\mathrm{Adv}^{\mathrm{SU}}_{\mathrm{HIBS,F}}(n)$ of F is defined as follows:

$$\mathrm{Adv}^{\mathrm{SU}}_{\mathrm{HIBS,F}}(n) = \Pr[\mathrm{F}\text{ wins the game }\mathrm{Game}^{\mathrm{SU}}_{\mathrm{HIBS,F}}(n)]. \tag{8}$$

3. Our Construction

We propose an adaptively secure hierarchical identity-based signature scheme SHIBS without increasing the dimension of the signatures. Our construction SHIBS uses the following parameters:

- $n \geq 1$ is a security parameter.
- $m = O(n\log q)$ is the dimension of the lattices.
- $q \geq O(\sqrt{n})\cdot O(\sqrt{m})^{3d-1}\cdot\omega(\sqrt{\log n})\cdot\omega(\sqrt{\log m})^d$ is a positive integer.
- $d \geq 1$ is the maximum hierarchy depth.[2]
- The followings are Gaussian parameters:
  - $s = O(\sqrt{n\log q})\cdot\omega(\sqrt{\log m})$.

[2] In case of $d = 1$, we call it an identity-based signature scheme IBS instead of HIBS.

- $s_0 = O(\sqrt{n \log q})$.
- For $1 \le i \le d$, $s_i > O(\sqrt{n \log q})^{3i+1} \cdot \omega(\log n)^{2i}$ such that $s_i > s_{i-1} \cdot O(\sqrt{n \log q})^{3} \cdot \omega(\log m)^2$.
- For $1 \le i \le d$, $s_i' = O(\sqrt{n \log q})^{3i-2} \cdot \omega(\sqrt{\log m})^{i}$.

In our construction SHIBS, a message space is $\{0,1\}^k$. Then, our construction $\mathrm{SHIBS} = \{\mathrm{SHIBS.Setup}, \mathrm{SHIBS.Extract}, \mathrm{SHIBS.Sign}, \mathrm{SHIBS.Vrfy}\}$ consists of the following algorithms:

- $\mathrm{SHIBS.Setup}(1^n, 1^d)$: On input of a security parameter n and the maximum hierarchy depth d:
  - Run the $\mathrm{BasisGen}(1^n, 1^m, q)$ algorithm to obtain a pair $(A \leftarrow Z_q^{n\times m}, S \in Z^{m\times m})$ of a uniformly random matrix and a short basis for $\Lambda^{\perp}(A)$.
  - Choose two hash functions $\mathrm{H}_1 : \{0,1\}^* \to \mathrm{D}_{Z^{m\times m}, s}$ and $\mathrm{H}_2 : \{0,1\}^k \to Z_q^n$, where the hash values of H_1 are Z_q-invertible [13][19].
  - Output a set $\mathrm{params} = (A, \mathrm{H}_1, \mathrm{H}_2)$ of public parameters and a master secret key $\mathrm{msk} = S$.
- $\mathrm{SHIBS.Extract}(\mathrm{params}, sk_{\mathrm{id}_{|l}}, \mathrm{id})$: On input of a set params of public parameters, a secret key $sk_{\mathrm{id}_{|l}}$ of a parent identity $\mathrm{id}_{|l} = (\mathrm{id}_1, \cdots, \mathrm{id}_l)$, and a child identity $\mathrm{id} = (\mathrm{id}_1, \cdots, \mathrm{id}_l, \cdots, \mathrm{id}_c)$:
  - Compute $R_{\mathrm{id}_{|l}} = \mathrm{H}_1(\mathrm{id}_{|l}) \cdots \mathrm{H}_1(\mathrm{id}_{|1}) \in Z^{m\times m}$ and $F_{\mathrm{id}_{|l}} = A \cdot R_{\mathrm{id}_{|l}}^{-1} \in Z_q^{n\times m}$. In case of $l = 0$, $sk_{\mathrm{id}_{|l}} = \mathrm{msk}$ and $F_{\mathrm{id}_{|l}} = A \in Z_q^{n\times m}$.
  - Compute $R = \mathrm{H}_1(\mathrm{id}_{|c}) \cdots \mathrm{H}_1(\mathrm{id}_{|l+1}) \in Z^{m\times m}$ and $F_{\mathrm{id}} = F_{\mathrm{id}_{|l}} \cdot R^{-1} \in Z_q^{n\times m}$.
  - Run the $\mathrm{BasisDel}(F_{\mathrm{id}_{|l}}, R, sk_{\mathrm{id}_{|l}}, s_c)$ algorithm to obtain a short basis $S' \in Z^{m\times m}$ for $\Lambda^{\perp}(F_{\mathrm{id}})$, where $sk_{\mathrm{id}_{|l}}$ is a short basis for $\Lambda^{\perp}(F_{\mathrm{id}_{|l}})$.
  - Output a secret key $sk_{\mathrm{id}} = S'$ of id.
- $\mathrm{SHIBS.Sign}(\mathrm{params}, \mathrm{id}, sk_{\mathrm{id}}, \mathrm{m})$: On input of a set params of public parameters, an identity id at depth $|\mathrm{id}| = l$ with its secret key sk_{id}, and a message $\mathrm{m} \in \{0,1\}^k$:
  - Compute $h = \mathrm{H}_2(\mathrm{m}) \in Z_q^n$.
  - Compute $R_{\mathrm{id}} = \mathrm{H}_1(\mathrm{id}_{|l}) \cdots \mathrm{H}_1(\mathrm{id}_{|1}) \in Z^{m\times m}$ and $F_{\mathrm{id}} = A \cdot R_{\mathrm{id}}^{-1} \in Z_q^{n\times m}$.
  - Run the $\mathrm{SampleD}(F_{\mathrm{id}}, sk_{\mathrm{id}}, h, s_l')$ algorithm to obtain a vector $\sigma \leftarrow \mathrm{D}_{\Lambda_h^{\perp}(F_{\mathrm{id}}), s_l'}$, where sk_{id} is a short basis for $\Lambda^{\perp}(F_{\mathrm{id}})$.
  - Output a signature σ.
- $\mathrm{SHIBS.Vrfy}(\mathrm{params}, \mathrm{id}, \mathrm{m}, \sigma)$: On input of a set params of public parameters, an

identity id at depth $|\mathrm{id}|=l$, a message $\mathrm{m}\in\{0,1\}^k$, and a signature σ:

- Compute $R_{\mathrm{id}}=\mathrm{H}_1(\mathrm{id}_{|l})\cdots\mathrm{H}_1(\mathrm{id}_{|1})\in Z^{m\times m}$ and $F_{\mathrm{id}}=A\cdot R_{\mathrm{id}}^{-1}\in Z_q^{n\times m}$.
- Output 1, if $F_{\mathrm{id}}\cdot\sigma=\mathrm{H}_2(\mathrm{m})\in Z_q^n$ and $\|\sigma\|\le s'_l\cdot\sqrt{m}$. Otherwise, output 0.

4. Analysis

4.1 Correctness

We show that our construction SHIBS is correct.

Theorem 4.1. Our hierarchical identity-based signature scheme SHIBS is correct.

Proof of Theorem 4.1. Suppose $|\mathrm{id}|=i$. The $\mathrm{SHIBS.Extract}(\mathrm{params},sk_{\mathrm{id}},\mathrm{id})$ algorithm can generate a short basis sk_{id} for $\Lambda^{\perp}(F_{\mathrm{id}})$. Then, the $\mathrm{SHIBS.Sign}(\mathrm{params},\mathrm{id},sk_{\mathrm{id}},\mathrm{m})$ algorithm can sample $\sigma\leftarrow\mathrm{D}_{\Lambda^{\perp}(F_{\mathrm{id}}),s'_i}$ such that $F_{\mathrm{id}}\cdot\sigma=h=\mathrm{H}_2(\mathrm{m})\in Z_q^n$ and $\|\sigma\|\le s'_i\cdot\sqrt{m}$ with an overwhelming probability using the $\mathrm{SampleD}(F_{\mathrm{id}},sk_{\mathrm{id}},h,s'_i)$ algorithm. Therefore, our hierarchical identity-based signature scheme SHIBS is correct. W

4.2 Unforgeability

We show that our construction SHIBS is strongly unforgeable under chosen message and adaptive identity attacks.

Theorem 4.2. In the random oracle model [20], our hierarchical identity-based signature scheme SHIBS is strongly unforgeable under chosen message and adaptive identity attacks if the $\mathrm{SIS}_{q,\beta}$ problem for $\beta=O(\sqrt{n\log q})^{3d-1}\cdot\omega(\sqrt{\log m})^d$ is hard.

Proof of Theorem 4.2. Suppose the hash functions H_1 and H_2 are random oracles controlled by an algorithm A. Then, our construction SHIBS is strongly unforgeable under chosen message and adaptive identity attacks assuming the $\mathrm{SIS}_{q,\beta}$ problem for $\beta=O(\sqrt{n\log q})^{3d-1}\cdot\omega(\sqrt{\log m})^d$ is hard. That is, if there exists a forger F mounting strong forgery attacks on SHIBS, then we can construct A solving the $\mathrm{SIS}_{q,\beta}$ problem for $\beta=O(\sqrt{n\log q})^{3d-1}\cdot\omega(\sqrt{\log m})^d$. A simulates the strong unforgeability game for F as follows:

- **Setup**: A takes an instance $A^*\in Z_q^{n\times m}$ of the $\mathrm{SIS}_{q,\beta}$ problem as an input. A proceeds as follows:
  - A chooses d positive integers $q_1^*,\cdots,q_d^*\leftarrow[q_{\mathrm{H}_1}]$. Suppose F sends at most q_{H_1} identities to A in the H_1 **queries** at each depth of the hierarchy.
  - A runs the $\mathrm{SampleR}(1^m,s)$ algorithm d times to obtain d matrices $R_1^*,\cdots,R_d^*\leftarrow\mathrm{D}_{Z^{m\times m},s}$.

- $\mathcal{A}$ chooses a positive integer $w \leftarrow [d]$.
- $\mathcal{A}$ computes $A = A^* \cdot R_w^* \cdots R_1^* \in Z_q^{n\times m}$. Note that $A \in Z_q^{n\times m}$ is uniformly random by **Fact 2.3**.
- $\mathcal{A}$ sends $\text{params} = A$ to $\mathcal{F}$.

- H_1 **queries**: After receiving the q-th identity $\text{id} = (\text{id}_1, \cdots, \text{id}_i)$ from $\mathcal{F}$, $\mathcal{A}$ proceeds as follows:
  - If $q = q_i^*$, $\mathcal{A}$ sets $\text{H}_1(\text{id}) = R_i^*$ and sends $\text{H}_1(\text{id})$ to $\mathcal{F}$.
  - Otherwise, $\mathcal{A}$ computes $A_i = A \cdot (R_{i-1}^* \cdots R_1^*)^{-1} \in Z_q^{n\times m}$. In case of $i = 1$, $\mathcal{A}$ sets $A_i = A$. $\mathcal{A}$ runs the SampleRwithBasis(A_i, s) algorithm to obtain a matrix $R \leftarrow \text{D}_{Z^{m\times m}, s}$ and a short basis $S_B \in Z^{m\times m}$ for $\Lambda^{\perp}(B)$, where $B = A_i \cdot R^{-1} \in Z_q^{n\times m}$. $\mathcal{A}$ sets $\text{H}_1(\text{id}) = R$, sends $\text{H}_1(\text{id})$ to $\mathcal{F}$, and adds a tuple $(i, \text{id}, R, B, S_B)$ to the H_1 list.

- H_2 **queries**: After receiving the i-th message m_i of to $\mathcal{A}$ from $\mathcal{F}$, $\mathcal{A}$ proceeds as follows:
  - $\mathcal{A}$ runs the SampleDom$(1^m, s)$ algorithm to obtain a vector $v_i \leftarrow \text{D}_{Z^m, s}$, computes $h_i = A \cdot v_i \in Z_q^n$, sends h_i to $\mathcal{F}$, and adds a tuple (m_i, v_i, h_i) to the H_2 list.

- **Extract queries**: After receiving an identity $\text{id} = (\text{id}_1, \cdots, \text{id}_c)$ at depth $|\text{id}| = c$ from $\mathcal{F}$, $\mathcal{A}$ proceeds as follows:
  - We assume that all prefixes of id already appears on the H_1 list. Otherwise, $\mathcal{A}$ sends the others to the H_1 **queries**.
  - $\mathcal{A}$ finds $j \in [c]$ which is the shallowest level such that $\text{H}_1(\text{id}_{|j}) \neq R_j^*$. In case of $j \notin [c]$, $\mathcal{A}$ aborts.
  - $\mathcal{A}$ looks up $(j, \text{id}_{|j}, R, B, S_B)$ in the H_1 list, where $B = A \cdot (R_1^*)^{-1} \cdots (R_{j-1}^*)^{-1} \cdot R^{-1} \in Z_q^{n\times m}$ and S_B is a short basis for $\Lambda^{\perp}(B)$.
  - If $j = c$, $\mathcal{A}$ sets $sk_{\text{id}} = S_B$. Otherwise, $\mathcal{A}$ runs the SHIBS.Extract$(\text{params}, S_B, \text{id})$ algorithm to obtain a secret key sk_{id} of id.
  - $\mathcal{A}$ sends sk_{id} to $\mathcal{F}$.

- **Sign queries**: After receiving an identity $\text{id} = (\text{id}_1, \cdots, \text{id}_c)$ at depth $|\text{id}| = c$ and a message m_i from $\mathcal{F}$, $\mathcal{A}$ proceeds as follows:
  - If for all $j \in [c]$, $\text{H}_1(\text{id}_{|j}) = R_j^*$, $\mathcal{A}$ looks up (m_i, v_i, h_i) in the H_2 list. If m_i does not appear on the H_2 list, $\mathcal{A}$ sends m_i to the H_2 **queries**. $\mathcal{A}$ computes $\sigma_i = R_c^* \cdots R_1^* \cdot v_i$ and sends σ_i.
  - Otherwise, $\mathcal{A}$ sends id to the **Extract queries** to obtain sk_{id}, runs the SHIBS.Sign$(\text{params}, \text{id}, sk_{\text{id}}, \text{m}_i)$ algorithm to obtain σ_i, and sends σ_i.

- **Output**: Assume that $\mathcal{F}$ outputs $(\text{id}^*, \text{m}^*, \sigma^*)$.

- In case of $w \neq |\mathrm{id}^*|$, $\mathcal{A}$ aborts. Note that the probability of $w \neq |\mathrm{id}^*|$ is $1-\frac{1}{d}$, since w is randomly selected from $[d]$.
- $\mathcal{A}$ finds $j \in [w]$ which is the shallowest level such that $\mathrm{H}_1(\mathrm{id}^*_{|i}) \neq R_i^*$. In case of $j \in [w]$, $\mathcal{A}$ aborts. Note that the probability of $j \in [w]$ is $1-(1/q_{\mathrm{H}_1})^w$.
- $\mathcal{A}$ outputs $z = \sigma^* - R_w^* \cdots R_1^* \cdot v_i \in \mathbb{Z}^m$ as a solution to the $\mathrm{SIS}_{q,\beta}$ problem.

We can assume that $(\mathrm{m}_i = \mathrm{m}^*, v_i, h_i = \mathrm{H}_2(\mathrm{m}^*))$ is in the H_2 list. Then, z is a solution to the $\mathrm{SIS}_{q,\beta}$ problem, because

$$\begin{aligned} A^* \cdot z &= A^* \cdot (\sigma^* - R_w^* \cdots R_1^* \cdot v_i) \\ &= A^* \cdot \sigma^* - A^* \cdot R_w^* \cdots R_1^* \cdot v_i \\ &= F_{\mathrm{id}^*} \cdot \sigma^* - A^* \cdot R_w^* \cdots R_1^* \cdot v_i \\ &= F_{\mathrm{id}^*} \cdot \sigma^* - A \cdot v_i \\ &= \mathrm{H}_2(\mathrm{m}^*) - h_i = 0 \in \mathbb{Z}_q^n, \end{aligned} \tag{9}$$

where

$$\begin{aligned} F_{\mathrm{id}^*} &= A \cdot (R_1^*)^{-1} \cdots (R_w^*)^{-1} \\ &= A^* \cdot R_w^* \cdots R_1^* \cdot (R_1^*)^{-1} \cdots (R_w^*)^{-1} \\ &= A^* \in \mathbb{Z}_q^{n \times m} \end{aligned} \tag{10}$$

and

$$\begin{aligned} \| z \| &\leq O(\sqrt{n \log q})^{3w-2} \cdot \omega(\sqrt{\log m})^w \cdot \sqrt{m} \\ &= O(\sqrt{n \log q})^{3w-1} \cdot \omega(\sqrt{\log m})^w \\ &\leq O(\sqrt{n \log q})^{3d-1} \cdot \omega(\sqrt{\log m})^d \\ &= \beta. \end{aligned} \tag{11}$$

To reduce the SIS problem to the SIVP, we set q as follows:

$$\begin{aligned} q &\geq \beta \cdot \sqrt{n} \cdot \omega(\sqrt{\log n}) \\ &= O(\sqrt{n \log q})^{3d-1} \cdot \omega(\sqrt{\log m})^d \cdot \sqrt{n} \cdot \omega(\sqrt{\log n}) \\ &= O(\sqrt{n}) \cdot O(\sqrt{m})^{3d-1} \cdot \omega(\sqrt{\log n}) \cdot \omega(\sqrt{\log m})^d. \end{aligned} \tag{12}$$

The advantage $\mathrm{Adv}^{\mathrm{SU}}_{\mathrm{SHIBS},\mathcal{F}}(n)$ of $\mathcal{F}$ is computed as follows:

$$\begin{aligned} \mathrm{Adv}_{\mathrm{A}}^{\mathrm{SIS}} &\geq \frac{1}{d\cdot q_{\mathrm{H}_1}^{w}}\cdot \mathrm{Adv}_{\mathrm{SHIBS,F}}^{\mathrm{SU}} \\ &\geq \frac{1}{d\cdot q_{\mathrm{H}_1}^{d}}\cdot \mathrm{Adv}_{\mathrm{SHIBS,F}}^{\mathrm{SU}}\,. \end{aligned} \tag{13}$$

W

5. Conclusion

In this paper, we have proposed a hierarchical identity-based signature scheme from lattices. Our scheme is adaptively secure and the size of signatures in our scheme is shortest among the existing hierarchical identity-based signature schemes from lattices. We proved the security of our scheme based on the SIS problem on lattices in the random oracle model. The question of constructing an adaptively secure hierarchical identity-based signature scheme from lattices without increasing the dimension of the signatures in the standard model still remains open.

References

[1] Adi Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. of Advances in Cryptology - Crypto 1984*, LNCS 0196, pp. 47-53, August 19-22, 1985. Article (CrossRef Link)

[2] Florian Hess, "Efficient identity based signature schemes based on pairings," in *Proc. of 9th Annual International Workshop on Selected Areas in Cryptology - SAC 2002*, LNCS 2595, pp. 310-324, August 15-16, 2002. Article (CrossRef Link)

[3] Jae Choon Cha and Jung Hee Cheon, "An identity-based signature from gap Diffie-Hellman groups," in *Proc. of 6th International Workshop on Theory and Practice in Public Key Cryptography - PKC 2003*, LNCS 2567, pp. 18-30, January 6-8, 2002. Article (CrossRef Link)

[4] Paulo S. L. M. Barreto, Benoit Libert, Noel McCullagh, and Jean-Jacques Quisquat, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. of Advances in Cryptology - Asiacrypt 2005*, LNCS 3788, pp. 515-532, December 4-8, 2005. Article (CrossRef Link)

[5] Craig Gentry and Alice Silverberg, "Hierarchical ID-based cryptography," in *Proc. of Advances in Cryptology - Asiacrypt 2002*, LNCS 2501, pp. 548-566, December 1-5, 2002. Article (CrossRef Link)

[6] Sherman S.M. Chow, Lucas C.K. Hui, Siu Ming Yiu, and K.P. Chow, "Secure hierarchical identity based signature and its application," in *Proc. of 6th International Conference on Information and Communications Security - ICICS 2004*, LNCS 3269, pp. 480-494, October 27-29, 2004. Article (CrossRef Link)

[7] Peter W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484-1509, October, 1997. Article (CrossRef Link)

[8] Markus Ruckert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in *Proc. of Third International Workshop on Post-quantum Cryptography - PQCrypto 2010*, LNCS 6061, pp. 182-200, May 25-28, 2010. Article (CrossRef Link)

[9] Miaomiao Tian, Liusheng Huang, and Wei Yang, "A new hierarchical identity-based signature scheme from lattices in the standard model," *International Journal of Network Security*, vol. 14, no. 6, pp. 310-315, November, 2012. Article (CrossRef Link)

[10] Zhenhua Liu, Yupu Hu, Xiangsong Zhang, and Fagen Li, "Efficient and strongly unforgeable identity-based signature scheme from lattices in the standard model," *Security and Communication Networks*, vol. 6, no. 1, pp. 69-77, January, 2013. Article (CrossRef Link)

[11] Miaomiao Tian, Liusheng Huang, and Wei Yang, "Efficient hierarchical identity-based signatures from lattices," *International Journal of Electronic Security and Digital Forensics*, vol. 5, no. 1, pp. 1-10, June, 2013. Article (CrossRef Link)

[12] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. of 40th Annual ACM Symposium on Theory of Computing - STOC 2008*, pp. 197-206, May 17-20, 2008. Article (CrossRef Link)

[13] Shweta Agrawal, Dan Boneh, and Xavier Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Proc. of Advances in Cryptology - Crypto 2010*, LNCS 6223, pp. 98-115, August 15-19, 2010. Article (CrossRef Link)

[14] Miklos Ajtai, "Generating hard instances of lattice problems," in *Proc. of 28th ACM Symposium on the Theory of Computing - STOC 1996*, pp. 99-108, May 22-24, 1996. Article (CrossRef Link)

[15] Daniele Micciancio and Oded Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267-302, April 2007. Article (CrossRef Link)

[16] Chris Peikert and Alon Rosen, "Efficient collision-resistant hashing from worst-case assumptions on cyclic lattcies," in *Proc. of 3rd Theory of Cryptography Conference - TCC 2006*, LNCS 3876, pp. 145-166, March 4-7, 2006. Article (CrossRef Link)

[17] Xavier Boyen, "Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more," in *Proc. of 13th International Conference on Practice and Theory in Public Key Cryptography - PKC 2010*, LNCS 6056, pp. 499-517, May 26-28, 2010. Article (CrossRef Link)

[18] Joel Alwen J and Chris Peikert, "Generating shorter bases for hard random lattices," *Theory of Computing Systems*, vol. 48, no. 3, pp. 535-553, April 2011. Article (CrossRef Link)

[19] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Proc. of Advances in Cryptology - Eurocrypt 2010*, LNCS 6110, pp. 523-552, May 30-June 3, 2010. Article (CrossRef Link)

[20] Mihir Bellare and Phillip Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. of 1st ACM Conference on Computer and Communications Security - CCS 1993*, pp. 62-73, November 3-5, 1993. Article (CrossRef Link)

Geontae Noh received the B.S. degree in Industrial Systems and Information Engineering from Korea University, Seoul, Korea, in 2008. He received the M.S. degree in Information Management and Security from Korea University, Seoul, Korea, in 2010. Currently, he is Ph.D. course in the Graduate School of Information Security, Korea University, Seoul, Korea. His research interests include cryptographic protocols, lattice-based cryptosystem, and privacy-preserving technologies.

Ik Rae Jeong received the B.S. and M.S. degrees in Computer Science from Korea University, Korea, in 1998 and 2000, respectively. He received the Ph.D. degree in Information Security from Korea University in 2004. From June 2006 to Feb. 2008, he was a senior engineer at ETRI (Electronics and Telecommunications Research Institute) in Korea. Currently, he is a member of the faculty in the Graduate School of Information Security, Korea University, Seoul, Korea. His current research areas include cryptography and theoretical computer science and Cryptology (ICISC 2005). His research interests are on cryptology and information security.