A New Hierarchical Identity-based Signature Scheme From Lattices In The Standard Model

Miaomiao Tian, Liusheng Huang, and Wei Yang
(Corresponding author: Miaomiao Tian)

School of Computer Science and Technology, University of Science and Technology of China
Hefei 230026, P.R. China (Email: miaotian@mail.ustc.edu.cn)

(Received Sep. 13, 2011; revised and accepted Nov. 20, 2011)

Abstract

Hierarchical identity-based signature (HIBS), which plays an important role in large communities, is a generalization of identity-based signature (IBS). In this paper, we present a new HIBS scheme from lattices without random oracles. The new scheme is proven to be strongly unforgeable against selective identity attacks under the standard hardness assumption of the short integer solution (SIS) problem. Furthermore, the secret key size and the signature length of our scheme are both invariant and much shorter than those of the previous lattice-based HIBS schemes. To the best of our knowledge, our construction is the first short lattice-based HIBS scheme in the standard model.

Keywords: Identity-based cryptography, lattice, short signature, standard model

1 Introduction

In 1984, Shamir [18] introduced the concept of identity-based (ID-based) cryptography and also presented an ID-based signature (IBS) scheme. In a IBS scheme, a public key can be derived from user's identity, e.g., his email address, and a corresponding secret key can be evaluated by a Private Key Generator (PKG). Since then, many IBS schemes have been proposed, e.g., [4, 11, 12, 14, 21]. However, IBS schemes are impractical for large organizations because there is only a single PKG in each scheme. Hierarchical ID-based signature (HIBS) [8] generalizes IBS. In a HIBS scheme, there are multiple PKGs that are arranged in a tree structure. Each PKG in the higher level is able to generate private keys for its children PKGs, which in turn generate private keys for the next level of PKGs. Hence, HIBS scheme reduces the burden of the root PKG and is very useful for large communities. Most of previous HIBS schemes are dependent on the hardness of computing discrete logarithms (e.g., [2, 7, 8, 22, 23]). Unfortunately, Shor [19] pointed out that the discrete logarithm problem is no longer hard in the post-quantum era.

Lattice-based cryptography is enjoying great interest these days, due to implementation simplicity and provable security reductions. Moreover, lattice-based cryptography is believed to be hard even for quantum computers (see [17] for a brief overview on lattices). Several lattice-based signature schemes [5, 6, 9, 10, 15, 16, 20] have been proposed so far. Among them, Rückert [16] constructed the first lattice-based HIBS schemes with and without random oracles in 2010 using Cash *et al.*'s signature scheme [6]. The HIBS schemes achieve a higher security level, i.e., strong unforgeability. Strong unforgeability requires that in addition to existential unforgeability, an adversary cannot produce a new signature on some message M even if he has seen a signature on M. Nevertheless, both the private keys and the signatures in Rčkert's schemes become dramatically longer when the identity depth increases. Therefore, they may not be practical for large communities.

In 2010, Boyen [5] proposed the first short lattice-based signature scheme without random oracles. However, his scheme is not strongly unforgeable. Recently, Agrawal *et al.* [3] presented a basis delegation algorithm which keeps the dimension of the lattices involved constant. Based on the algorithm, the first lattice-based hierarchical ID-based encryption scheme with short ciphertexts in the standard model was proposed in [3]. Still, there is no short lattice-based HIBS scheme in the standard model.

In this paper, we propose a short lattice-based HIBS scheme without random oracles, which is obtained from Agrawal *et al.*'s basis delegation algorithm [3] and the modification of Boyen's signature scheme [5]. The new scheme is provably secure against strong forgery for selective identity attacks under the standard short integer solution (SIS) assumption. The secret key size and the signature length of our scheme are much shorter than those of Rückert's HIBS scheme without random oracles [16]. Notice that the secret keys of some existing HIBS schemes in the standard modal (e.g., [2, 16, 22, 23]) are all dependent

on the depth of the signer in the hierarchy. Therefore, our scheme may be of interest since the secret key size and the signature length of our scheme are both constant and independent of the level of the signer.

The rest of this paper is organized as follows. Some definitions and facts are given in Section 2. In Section 3, we define HIBS and its security model. In section 4, we present a short HIBS scheme based on lattices. Analysis will be provided in Section 5. Finally, Section 6 concludes this paper.

2 Preliminaries

2.1 Notations

The security parameter in this work is n. For a positive integer k, $[k]$ denotes the set $\{1, \cdots, k\}$. Let s be a string, we refer to $|s|$ as its length. For a matrix $A = [a_1, \cdots, a_m] \in \mathbb{Z}^{n \times m}$, let $\widetilde{A}$ denote the Gram-Schmidt orthogonalization of A and let $||A|| = \max_{i \in [m]} ||a_i||$ where $||\cdot||$ denotes the Euclidean norm. The function $\mathrm{negl}(n)$ is negligible in n if it is smaller than all polynomial fractions for larger n.

The *statistical distance* between two distributions X and Y over some finite set F is defined as $\max_{G \subseteq F} |X(G) - Y(G)|$. We say that two distributions are statistically close if their statistical distance is negligible in n.

2.2 Lattices

In this work, we focus on integer lattices, which are contained in $\mathbb{Z}^m$.

Definition 2.1. *Let a basis $B = [b_1, \ldots, b_m] \in \mathbb{Z}^{m \times m}$ consist of m-linearly independent vectors. The lattice generated by B is defined as*

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

Definition 2.2. *For a positive integer q, a vector $y \in \mathbb{Z}_q^n$ and a matrix $A \in \mathbb{Z}^{n \times m}$, define two m-dimensional spaces*

$$\Lambda^{\perp}(A) = \{e \in \mathbb{Z}^m : Ae = 0 \pmod q\},$$

$$\Lambda^{y}(A) = \{e \in \mathbb{Z}^m : Ae = y \pmod q\}.$$

Gaussians on lattices. Here we briefly review the Gaussian function which is a useful tool in lattice-based cryptography. For any $\sigma > 0$, the Gaussian function on $\mathbb{R}^m$ centered at c with parameter σ is defined as

$$\rho_{\sigma,c}(x) = \exp(-\pi ||x - c||^2 / \sigma^2).$$

The discrete Gaussian distribution over Λ with center c and parameter σ is

$$\forall x \in \Lambda, \quad D_{\Lambda,\sigma,c} = \rho_{\sigma,c}(x) / \rho_{\sigma,c}(\Lambda).$$

Micciancio and Regev [13] showed the following property about these distributions.

Lemma 2.1. *Let $m \geq n$ and $A \in \mathbb{Z}^{n \times m}$. Let B be a basis of $\Lambda^{\perp}(A)$ and $\sigma \geq \|\widetilde{B}\| \cdot \omega(\sqrt{\log n})$, then for any $y \in \mathbb{Z}_q^n$, $Pr_{x \sim D_{\Lambda^y(A),\sigma,0}}[\|x\| > \sigma \cdot \sqrt{m}] \leq negl(n)$.*

2.3 Hardness Assumption

Security of our HIBS scheme rests on the hardness assumption of the short integer solution (SIS) problem [1].

Definition 2.3. *Given a positive integer q, a matrix $A \in \mathbb{Z}_q^{n \times m}$ and a real β, the goal of the short integer solution problem (q, m, β)-SIS is to find a nonzero vector $e \in \Lambda^{\perp}(A)$ such that $||e|| \leq \beta$.*

For appropriate m, β and for any prime $q \geq \beta \cdot \omega(\sqrt{n \log n})$, solving SIS on the average is as hard as approximating certain lattice problems in the worst case [13].

2.4 Basis Delegation

Let $A \in \mathbb{Z}_q^{n \times m}$ be a random matrix, the one-way function f_A, introduced by Gentry *et al.* [9], is defined as $f_A(x) = Ax \pmod q$, with domain $D_n = \{e \in \mathbb{Z}^m : ||e|| \leq \sigma\sqrt{m}\}$ and range $R_n = \mathbb{Z}_q^n$. Namely, sampling from $f_A^{-1}(y)$ for any $y \in R_n$ is hard without a trapdoor. A trapdoor of f_A is a short basis T_A of $\Lambda^{\perp}(A)$. Some relevant facts about these functions are listed below.

Proposition 2.1. *Let $q \geq 2$ and $m > 5n \log q$. There is a probabilistic polynomial-time (PPT) algorithm **TrapGen**(1^n) that outputs a matrix $A \in \mathbb{Z}_q^{n \times m}$ statistically close to uniform and a basis T_A for $\Lambda^{\perp}(A)$ such that $||\widetilde{T_A}|| \leq O(\sqrt{n \log q})$ with overwhelming probability.*

Lemma 2.2. *Let $q \geq 2$, $m > 5n \log q$ and $A \in \mathbb{Z}_q^{n \times m}$. Let T_A be a basis for $\Lambda^{\perp}(A)$ and $\sigma \geq \|\widetilde{T_A}\| \cdot \omega(\sqrt{\log m})$.*

1) *For any $e \sim D_{\mathbb{Z}^m,\sigma,0}$, the distribution of the syndrome $u = Ae \pmod q$ is statistically close to uniform over $\mathbb{Z}_q^n$.*
2) *For any $y \in \mathbb{Z}_q^n$, there is a PPT algorithm **SamplePre**(A, T_A, σ, y) that outputs a vector $e \in \Lambda^y(A)$ satisfying $||e|| \leq \sigma\sqrt{m}$ with all but negl(n) probability. In addition, the set $\{x \in \mathbb{Z}^m : ||x|| \leq \sigma\sqrt{m} \wedge Ax = y\}$ contains at least $2^{\omega(\log n)}$ elements.*

At CRYPTO 2010, Agrawal *et al.* [3] presented a new short lattice basis delegation algorithm that keeps the lattice dimension unchange. Now, we briefly recall the main results in [3].

Definition 2.4. *Let q be a prime, $m \geq 6n \log q$ and $\sigma \geq \sqrt{m} \cdot \omega(\sqrt{\log m})$, define $D_{m \times m}$ is the distribution on full rank matrices $\{A_i = [a_{i1}, \cdots, a_{im}] \in \mathbb{Z}_q^{m \times m}\}$, where $a_{ij} \sim D_{\mathbb{Z}^m,\sigma,0}$ for all $j \in [m]$.*

Proposition 2.2. *Let $q > 2$, $A \in \mathbb{Z}_q^{n \times m}$ and $R \in \mathbb{Z}^{m \times m}$ be a product of d matrices sampled from $D_{m \times m}$.*

Let T_A be a basis of $\Lambda^{\perp}(A)$, there exists a PPT algorithm ***BasisDel***(A, R, T_A, σ) *that outputs a random basis B for $\Lambda^{\perp}(AR^{-1})$ such that $||\widetilde{B}|| \leq \sigma\sqrt{m}$, where $\sigma \geq \|\widetilde{T_A}\| \cdot m^d \cdot \omega(\log^{d+1} m)$.*

Proposition 2.3. *For $q > 2$, $m > 5n\log q$ and $A \in \mathbb{Z}_q^{n\times m}$, there is a PPT algorithm* ***SampleRwithBasis***(A) *that outputs a random matrix $R \sim D_{m\times m}$ and a basis B for $\Lambda^{\perp}(AR^{-1})$ such that $\|\widetilde{B}\| \leq \sqrt{m}$.*

3 HIBS Scheme and Its Security Model

3.1 HIBS Scheme

A HIBS scheme consists of four algorithms: **Setup**, **Extract**, **Sign** and **Verify**. They are specified as follows:

Setup. On input the security parameter n, the root PKG generates system parameters PP and a master secret key MSK.

Extract. On input an identity ID and the master secret key MSK or parent's private key, this algorithm outputs a secret key SK_{ID} for ID.

Sign. Given a private key SK_{ID} and a message M, the algorithm signs the massage M for ID and outputs the signature $v = Sign(M, SK_{ID})$.

Verify. Given a signature v, a massage M and an identity ID, it outputs 1 if the signature is valid. Otherwise, it outputs 0.

These algorithms must satisfy the standard consistency constraint, namely, for any massage-identity pair (M, ID) if $v = Sign(M, SK_{ID})$, then $Verify(v, M, ID)$ outputs 1 with overwhelming probability.

3.2 Security Model

There are two security models for HIBS, i.e., the adaptive identity security model and the selective identity security model. The adaptive identify security model allows an adversary to adaptively issue queries on arbitrary identity. The selective identity security model demands that an adversary must announce its target identity before seeing the public key. Our HIBS scheme is strongly unforgeable under selective identity attack (SU-sIDA) which is formally defined in the following SU-sIDA game played between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.

Init. On input the maximum depth of the hierarchy $l+1$, the adversary $\mathcal{A}$ outputs a target identity $ID^* = (ID_0, ID_1^*, \cdots, ID_k^*)$, where $k \leq l$.

Setup. The challenger $\mathcal{C}$ runs **Setup** and sends the system parameters PP to the adversary $\mathcal{A}$.

Extract queries. The adversary $\mathcal{A}$ adaptively delivers queries on any identity ID where each ID is not a prefix of ID^*. The challenger $\mathcal{C}$ runs **Extract** to obtain a private key SK_{ID} and sends the result to $\mathcal{A}$.

Sign queries. The adversary $\mathcal{A}$ adaptively chooses an identity ID and a message M. The challenger $\mathcal{C}$ computes $v = Sign(M, SK_{ID})$ and sends the signature (v, M, ID) to $\mathcal{A}$.

Forgery. The adversary $\mathcal{A}$ outputs a signature (v^*, M^*, ID^*) such that the **Verify** algorithm outputs 1.

The adversary $\mathcal{A}$ wins the game if (v^*, M^*, ID^*) does not appear in the *Sign queries* phase.

Definition 3.1. *A HIBS scheme is $(t, q_E, q_S, \varepsilon)$-SU-sIDA secure in the standard model if there is no t-time adversary that succeeds in the above game with probability at least ϵ, and makes at most q_E extract queries and q_S sign queries.*

4 Proposed Lattice-based HIBS Scheme

Assume that the maximum depth of the hierarchy, including the root PKG, is $l+1$, where $l \geq 1$. Let $q \geq 2$ be a prime and $m \geq 6n\log q$. Choose two cryptographic hash functions $H : ID \to H(ID) \in \{0,1\}^{\lambda_1}$ and $h : \{0,1\}^* \to \{0,1\}^{\lambda_2}$. For $0 \leq d \leq l$, the Gaussian parameter in level d is σ_d. Define ID_0 is the root PKG's identity and $ID|k = (ID_0, \cdots, ID_k)$ for $k \in [l]$. Our HIBS scheme works as follows:

Setup: Given the security parameter n and the maximum depth $l+1$, run **TrapGen**(1^n) to generate a matrix $A \in \mathbb{Z}_q^{n\times m}$ and a corresponding short basis $T_A \in \mathbb{Z}_q^{m\times m}$. Select a random nonzero vector $y \in \mathbb{Z}_q^n$, $2l\lambda_1$ random matrices $R_{i,j}^0, R_{i,j}^1 \in D_{m\times m}$ (for $1 \leq i \leq l, 1 \leq j \leq \lambda_1$) and λ_2 random matrices $C_i \in \mathbb{Z}_q^{n\times m}$. Publish the system parameter $PP = \{A, \langle R_{i,j}^0, R_{i,j}^1\rangle, \langle C_i\rangle, y\}$ and keep the master secret key T_A secret.

Extract: On input a private key $SK_{ID|d}$ for the identity $ID|d$ and an identity $ID = (ID_0, \cdots, ID_d, \cdots, ID_k)$, do the following steps:

1) Set $\mu_i = H(ID|i)$ for all $i \in [k]$.
2) Compute $R_{\mu_i} = R_{i,\lambda_1}^{\mu_i[\lambda_1]} \cdots R_{i,1}^{\mu_i[1]} \in \mathbb{Z}_q^{m\times m}$ and $F_{ID|d} = A(R_{\mu_d} \cdots R_{\mu_1})^{-1}$. Define $SK_{ID|0} = T_A$ and $F_{ID|0} = A$. The secrete key $SK_{ID|d}$ in $\mathbb{Z}_q^{m\times m}$ is a short basis of $\Lambda^{\perp}(F_{ID|d})$.
3) Let $R = R_{\mu_k} \cdots R_{\mu_{d+1}}$ and $F_{ID|k} = F_{ID|d}R^{-1} \in \mathbb{Z}_q^{n\times m}$.
4) Run **BasisDel**$(F_{ID|d}, R, SK_{ID|d}, \sigma_d)$ to generate a private key $SK_{ID|k}$ for ID, where $SK_{ID|k}$ is a random basis for $\Lambda^{\perp}(F_{ID|k})$.

Sign: On input the secret key $SK_{ID|k}$ of the user $ID|k$ and a message $M \in \{0,1\}^*$, do as follows:

1) Select a random string $r \in \{0,1\}^n$ and compute $\nu = h(M, r, ID|k)$.
2) Set $C = (-1)^{\nu[1]}C_1 + \cdots + (-1)^{\nu[\lambda_2]}C_{\lambda_2} \in \mathbb{Z}_q^{n\times m}$.
3) Pick $v_1 \in D_{\mathbb{Z}^m,\sigma_k,0}$ uniformly at random. By Lemma 1, $||v_1|| \le \sigma_k\sqrt{m}$ with $1-\text{negl}(n)$ probability.
4) Run $v_2 \leftarrow \textbf{SamplePre}(F_{ID|k}, SK_{ID|k}, \sigma_k, y - Cv_1)$.
5) Output the signature (v, r), where $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ in $\mathbb{Z}_q^{2m}$.

Verify: Given a identity $ID|k$, a signature (v, r) and a massage M, do:

1) For all $i \in [k]$, set $\mu_i = H(ID|i)$.
2) Compute $F_{ID|k} = A(R_{\mu_k} \cdots R_{\mu_1})^{-1}$, where $R_{\mu_i} = R_{i,\lambda_1}^{\mu_i[\lambda_1]} \cdots R_{i,1}^{\mu_i[1]}$.
3) Set $\nu = h(M, r, ID|k)$ and $C = (-1)^{\nu[1]}C_1 + \cdots + (-1)^{\nu[\lambda_2]}C_{\lambda_2}$.
4) The verifier accepts the signature if and only if $(C|F_{ID|k})v = y$ and $||v|| \le \sigma_k\sqrt{2m}$.

5 Analysis

5.1 Correctness

According to the above definitions, we have

$$F_{ID|k} = F_{ID|d}R^{-1} = A(R_{\mu_k} \cdots R_{\mu_1})^{-1} \pmod q.$$

By Lemma 2.2, we know that $F_{ID|k}v_2 = y - Cv_1 \pmod q$ and the vector v_2 satisfies $||v_2|| \le \sigma_k\sqrt{m}$ with all but negligible probability in n. Therefore, $(C|F_{ID|k})v = Cv_1 + F_{ID|k}v_2 = y \pmod q$ and $||v|| = \sqrt{v_1^2 + v_2^2} \le \sqrt{2(\sigma_k)^2 m} = \sigma_k\sqrt{2m}$ with overwhelming probability.

Now we evaluate the Gaussian parameter σ_k for each $k \in [l]$. Let $\sigma_0 = O(\sqrt{m})$, by Proposition 2.2 we can obtain that the Gaussian parameter $\sigma_k \ge \sigma_0 m^{k\lambda_1+k/2} \cdot \omega(\log^{k\lambda_1+k} m)$ since $||\widetilde{SK}_{ID|d-1}|| \le \sigma_{d-1}\sqrt{m}$ and $\sigma_d \ge ||\widetilde{SK}_{ID|d-1}|| \cdot m^{\lambda_1} \cdot \omega(\log^{\lambda_1+1} m)$ for all $d \in [l]$.

5.2 Comparison

The lattice-based HIBS scheme without random oracles constructed by Rückert is also provably secure in the above security model. However, the private keys and the signatures in his scheme are dependent on the identity length of the signer. In contrast, both the private key size and the signature size in our scheme are unchanged and much shorter. Therefore, our scheme is more practical, though the public key size in this scheme is larger than that of Rückert's scheme. For the signer $ID|k = (ID_0, \cdots, ID_d, \cdots, ID_k)$ of depth $k \in [l]$, Table 1 shows the comparison of the schemes, where $m_1 = \tilde{O}(ln)$ and $m_2 = \tilde{O}(\lambda_1 ln)$.

5.3 Strong Unforgeability

Theorem 5.1. *The proposed HIBS scheme is $(t, q_E, q_S, \varepsilon)$-SU-sIDA secure if there is no PPT algorithm that solves $(q, m, 2\sigma_l\sqrt{2m}(\lambda_2\eta\sqrt{m}+1))$-SIS with probability $\epsilon' \ge 5\epsilon/6 - negl(n)$, where $\eta \ge \sqrt{m}\cdot\omega(\sqrt{\log m})$.*

Proof. Suppose that there is a t-time adversary $\mathcal{A}$ that succeeds in the SU-sIDA game with probability at least ϵ, then we can construct a PPT algorithm $\mathcal{C}$ that solves the SIS problem instance with non-negligible probability.

Init: The adversary $\mathcal{A}$ first outputs a target identity $ID^* = (ID_0, ID_1^*, \cdots, ID_u^*)$, where $u \le l$. To simplify the notation, let $u = l$ (the proofs of other cases are similar and therefore omitted).

Setup: The algorithm $\mathcal{C}$ picks a random matrix $A_0 \in \mathbb{Z}_q^{n\times m}$ and λ_2 random matrices $E_1, \cdots, E_{\lambda_2} \in \mathbb{Z}_q^{m\times m}$, where each column of E_i is selected independently from $D_{\mathbb{Z}^m,\eta,0}$. Let $C_i = A_0E_i \ (mod\ q)$ for all $i \in [\lambda_2]$. According to Lemma 2.2, we know that C_i is statistically close to uniform over $\mathbb{Z}_q^{n\times m}$. $\mathcal{C}$ selects $l\lambda_1$ random matrices $R_{i,j} \sim D_{m\times m}$, where $i \in [l], j \in [\lambda_1]$. For $\forall j \in [\lambda_1]$, the rest of the public parameters are chosen as follows:

1) For each $i \in [l]$, compute $\mu_i^* = H(ID^*|i)$ and set $R_{i,j}^{\mu_i^*[j]} \leftarrow R_{i,j}$.
2) Define $R_{\mu_i^*} = R_{i,\lambda_1}^{\mu_i^*[\lambda_1]} \cdots R_{i,1}^{\mu_i^*[1]}$ and compute $A = A_0(R_{\mu_l^*} \cdots R_{\mu_1^*})$.
3) Select $x_0 \in \mathbb{Z}_q^m$ uniformly at random from $D_{\mathbb{Z}^m,\eta,0}$ and let $y = A_0x_0 \pmod q$. If $y = 0 \pmod q$, repeat this step until y is a non-zero vector.
4) For each $i \in [l]$, compute $A_{i,j} = A \cdot (R_{\mu_{i-1}^*} \cdots R_{\mu_1^*})^{-1}(R_{i,j-1}^{\mu_i^*[j-1]} \cdots R_{i,1}^{\mu_i^*[1]})^{-1}$, where $A_{1,1} = A$.
5) Invoke $\textbf{SampleRwithBasis}(A_{i,j})$ to generate a matrix $R \sim D_{m\times m}$ and a short basis T_B for $\Lambda^{\perp}(B = A_{i,j}R^{-1})$. Return $R_{i,j}^{1-\mu_i^*[j]} \leftarrow R$.
6) Preserve the tuple (i, j, R, B, T_B).

Finally, $\mathcal{C}$ sends the system parameters $PP = \{A, \langle R_{i,j}^0, R_{i,j}^1\rangle, \langle C_i\rangle, y\}$ to $\mathcal{A}$.

Extract queries: $\mathcal{A}$ queries the secret key of the identity $ID = (ID_0, \cdots, ID_w)$. If $w > l$ or $ID = ID^*|w$, $\mathcal{C}$ answers $\perp$. Otherwise, do these steps:

1) For $i \in [w]$, define $\mu_i = H(ID|i)$ and $R_{\mu_i} = R_{i,\lambda_1}^{\mu_i[\lambda_1]} \cdots R_{i,1}^{\mu_i[1]}$.
2) Let (k, j) be the first position such that $\mu_k[j] \ne \mu_k^*[j]$, where $k \in [w], j \in [\lambda_1]$.
3) Retrieve the tuple (k, j, R, B, T_B). By construction $B = A_{k,j} \cdot (R_{k,j}^{\mu_k[j]})^{-1}$.
4) On input T_B, run $\textbf{BasisDel}(B, (R_{\mu_w} \cdots R_{\mu_{k+1}}) \cdot (R_{k,\lambda_1}^{\mu_k[\lambda_1]} \cdots R_{k,j+1}^{\mu_k[j+1]}), T_B, \sigma_k)$ to generate a private key for ID and sends the result to $\mathcal{A}$.

Table 1: Comparison between Rückert's HIBS scheme and our scheme

Scheme	Public key size	Secret key size	Signature size
[16] no RO	$(1+2l\lambda_1+2\lambda_2)nm_1+n$	$(m_1+k\lambda_1 m_1)^2$	$(1+k\lambda_1+\lambda_2)m_1+n$
This work	$(n+2l\lambda_1 m_2+\lambda_2 n)m_2+n$	$(m_2)^2$	$2m_2+n$

Sign queries: On input a message M and an identity ID:

- If $ID = ID^*$, then $F_{ID^*} = A(R_{\mu_l^*}\cdots R_{\mu_1^*})^{-1} = A_0$. $\mathcal{C}$ does the following steps:
  1) Choose a random string $r \in \{0,1\}^n$ and evaluate $\nu = h(M, r, ID)$.
  2) Let $E_\nu = \sum_{i\in[\lambda_2]}(-1)^{\nu[i]}E_i$. We then have $C = \sum_{i\in[\lambda_2]}(-1)^{\nu[i]}C_i = A_0E_\nu$.
  3) Select a random vector $v_1 \in D_{\mathbb{Z}^m,\eta,0}$ and compute $v_2 = x_0 - E_\nu v_1 \pmod q$. If $E_\nu v_1 = 0$, repeat this step.
  4) It outputs $v = \binom{v_1}{v_2}$ and r.

  Now we show that (v, r) is a valid signature. By the above process, we have $(C|F_{ID^*})v = A_0E_\nu v_1 + A_0v_2 = A_0x_0 = y \pmod q$. On the other hand, we know, for any ν, $||E_\nu|| \le \lambda_2 \max||E_i|| \le \lambda_2\eta\sqrt{m}$ with $1-\mathrm{negl}(n)$ probability. Thus, for all $k \in [l]$, $||v|| \le ||v_1||+||v_2|| \le 2\eta\sqrt{m} + ||E_\nu|| \cdot ||v_1|| \le \eta\sqrt{m}(2+\lambda_2\eta\sqrt{m}) \le \sigma_k\sqrt{2m}$ with overwhelming probability.
- Otherwise, do:
  1) Invoke the *Extract queries* process to obtain a secret key SK_{ID} for ID.
  2) Run the algorithm **Sign**.
  3) It returns the signature (v, r).

Forgery: The adversary $\mathcal{A}$ outputs a signature (v^*, r^*, M^*, ID^*) such that the algorithm **Verify** returns 1.

Let $\nu^* = h(M^*, r^*, ID^*)$ and $E_{\nu^*} = \sum_{i\in[\lambda_2]}(-1)^{\nu[i]}E_i$. Then $F_{ID^*} = A_0$ and $C = A_0E_{\nu^*}$. There are two different cases that need to be considered.

– *Case 1.* The message (M^*, r^*) has been queried in the *Sign queries* phase, namely, this is a strong forgery. We have $(C|F_{ID^*})v^* = A_0(E_{\nu^*}v_1^* + v_2^*) = y = A_0(E_{\nu^*}v_1 + v_2) \pmod q$ and $v \neq v^*$ (by the definition of strong unforgeability). Obviously, $e = E_{\nu^*}(v_1^* - v_1) + v_2^* - v_2$ satisfies $A_0e = 0 \pmod q$. According to the Lemma 26 in [5], $\Pr[e \neq 0] \ge 2/3$. Hence, $\mathcal{C}$ obtains a solution of the SIS problem.

– *Case 2.* The message (M^*, r^*) has not been queried in the *Sign queries* phase. In this case, we know that $\nu^* = h(M^*, r^*, ID^*)$ is a new vector and $(C|F_{ID^*})v^* = A_0(E_{\nu^*}v_1^* + v_2^*) = A_0x_0 \pmod q$. Let $e = E_{\nu^*}v_1^* + v_2^* - x_0$. Notice that $\Pr[e = 0] \le \mathrm{negl}(n)$ (by Lemma 2.2), thus $\mathcal{C}$ also solves the SIS problem.

In the first case, we have

$$\begin{aligned} ||e|| &\le ||E_{\nu^*}|| \cdot ||v_1^* - v_1|| + ||v_2^* - v_2|| \\ &\le 2\sigma_k\sqrt{2m}(\lambda_2\eta\sqrt{m}+1) \\ &\le 2\sigma_l\sqrt{2m}(\lambda_2\eta\sqrt{m}+1), \end{aligned}$$

since $||E_{\nu^*}|| \le \lambda_2\eta\sqrt{m}$ and $\sigma_k \le \sigma_l$.

Similarly, for case 2, we have

$$\begin{aligned} ||e|| &\le ||E_{\nu^*}v_1^*|| + ||v_2^*|| + ||x_0|| \\ &\le \sqrt{2}\lambda_2\eta\sigma_k m + \sigma_k\sqrt{2m} + \eta\sqrt{m} \\ &\le 2\sigma_k\sqrt{2m}(\lambda_2\eta\sqrt{m}+1) \\ &\le 2\sigma_l\sqrt{2m}(\lambda_2\eta\sqrt{m}+1). \end{aligned}$$

Thus, we can set $\beta = 2\sigma_l\sqrt{2m}(\lambda_2\eta\sqrt{m}+1)$.

Here we calculate the advantage of the algorithm $\mathcal{C}$. Suppose that each case will happen with the same probability, therefore, the PPT algorithm $\mathcal{C}$ has advantage $\epsilon' \ge \epsilon/2 \cdot 2/3 + \epsilon/2 - \mathrm{negl}(n) = 5\epsilon/6 - \mathrm{negl}(n)$ in solving the SIS problem instance. □

6 Conclusion

In this paper, we have constructed a new lattice-based HIBS scheme with short secret keys and signatures. We have also proven that this scheme is strongly unforgeable in the standard model. It is more practical than Rückert's HIBS scheme without random oracles.

Acknowledgements

This work is supported by the Major Research Plan of the National Natural Science Foundation of China (No. 90818005) and the National Natural Science Foundation of China (No. 60903217).

References

[1] M. Ajtai, "Generating hard instances of lattice problems," *STOC 1996*, pp. 99–108, 1996.

[2] M. Au, J. Liu, T. Yuen, and D. Wong, "Practical hierarchical identity based encryption and signature schemes without random oracles," *Cryptology ePrint Archive*, Report 2006/368. (http://eprint.iacr.org/2006/368).

[3] S. Agrawal, D. Boneh, and X. Boyen, "Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE," *Crypto 2010*, LNCS 6223, Springer-Verlag, pp.98–115, 2010.

[4] P. Barreto, B. Libert, N. McCullagh, and J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," *Asiacrypt 2005*, LNCS 3788, Springer-Verlag, pp.515–532, 2005.

[5] X. Boyen, "Lattice Mixing and Vanishing Trapdoors: A Framework for Fully Secure Short Signatures and more," *PKC 2010*, LNCS 6056, Springer-Verlag, pp.499–517, 2010.

[6] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai Trees, or How to Delegate a Lattice Basis," *Eurocrypt 2010*, LNCS 6110, Springer-Verlag, pp.523–552, 2010.

[7] S. Chow, L. Hui, S. Yiu, and K. Chow, "Secure Hierarchical Identity Based Signature and Its Application," *The 6th International Conference on Information and Communication Security (ICICS 2004)*, LNCS 3269, Springer-Verlag, pp.480–494, 2004.

[8] C. Gentry, and A. Silverberg, "Hierarchical ID-based cryptography," *Asiacrypt 2002*, LNCS 2501, Springer-Verlag, pp.548–566, 2002.

[9] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for Hard Lattices and New Cryptographic Constructions," *STOC 2008*, pp.197–206, 2008.

[10] D. Gordon, J. Katz, and V. Vaikuntanathan, "A group singnature scheme from lattice assumptions," *Asiacrypt 2010*, LNCS 6477, Springer-Verlag, pp.395–412, 2010.

[11] F. Hess, "Efficient identity based signature schemes based on pairings," *Selected Areas in Cryptography (SAC 2002)*, LNCS 2595, Springer-Verlag, pp.310–324, 2003.

[12] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Short designated verifier signature scheme and its identity-based variant," *International Journal of Network Security*, vol. 6, no. 1, pp.82–93, 2008.

[13] D. Micciancio, and O. Regev, "Worst-case to average-case reductions based on gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp.267–302, 2007.

[14] K. Paterson, and J. Schuldt, "Efficient Identity-based Signatures Secure in the Standard Model," *The 11th Australasian Conference on Information Security and Privacy (ACISP 2006)*, LNCS 4058, Springer-Verlag, pp. 207–222, 2006.

[15] M. Rückert, "Lattice-based Blind Signatures," *Asiacrypt 2010*, LNCS 6477, Springer-Verlag, pp.413–430, 2010.

[16] M. Rückert, "Strongly unforgeable signatures and hierarchical identitybased signatures from lattices without random oracles," *PQCrypto 2010*, LNCS 6061, Springer-Verlag, pp.182–200, 2010.

[17] O. Regev, "Lattice-based cryptography," *Crypto 2006*, LNCS 4117, Springer-Verlag, pp.131–141, 2006.

[18] A. Shamir, "Identity-based cryptosystems and signature schemes," *Crypto'84*, LNCS 196, Springer-Verlag, pp.47–53, 1985.

[19] P. 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, 1997.

[20] J. Wang, "Ring Signature and Identity-Based Ring Signature from Lattice Basis Delegation," *Cryptology ePrint Archive*, Report 2010/378. (http://eprint.iacr.org/2010/378.)

[21] H. Xiong, Z. Qin, and F. Li, "Identity-based Threshold Signature Secure in the Standard Model," *International Journal of Network Security*, vol. 10, no. 1, pp.75–80, 2010.

[22] T. Yuen, and V. Wei, "Constant-size hierarchical identity-based signature/signcryption without random oracles," *Cryptology ePrint Archive*, Report 2005/412. (http://eprint.iacr.org/2005/412.)

[23] L. Zhang, Y. Hu, and Q. Wu, "New Construction of Short Hierarchical ID-Based Signature in the Standard Model," *Fundamenta Informaticae*, vol. 90, no. 1, pp.191–201, 2009.

Miaomiao Tian is a Ph.D. student in School of Computer Science and Technology at University of Science and Technology of China. His research interests include cryptography and information security.

Liusheng Huang is a professor in School of Computer Science and Technology at University of Science and Technology of China. His research interests include information security, wireless sensor network and distributed computing. He is author or coauthor of more than 100 research papers and 6 books.

Wei Yang is a postdoctoral research fellow in School of Computer Science and Technology at University of Science and Technology of China. In 2007, he received his Ph.D. degree in computer science from University of Science and Technology of China and was awarded the Dean's Prize of Chinese Academy of Sciences. His research interests include information theory, quantum information and cryptography.