Efficient Identity-Based Signature from Lattices

Miaomiao Tian, Liusheng Huang

Efficient identity-based signature from lattices

Miaomiao Tian * and Liusheng Huang

School of Computer Science and Technology, University of Science and Technology of China

Abstract. Identity-based signature is an important technique for light-weight authentication. Recently, many efforts have been made to construct identity-based signatures over lattice assumptions since they would remain secure in future quantum age. In this paper we present a new identity-based signature scheme from lattice problems. This scheme is more efficient than other lattice-based identity-based signature schemes in terms of both computation and communication complexities. We prove its security in the random oracle model under short integer solution assumption that is as hard as approximating several worst-case lattice problems.

Keywords: identity-based signature, lattice, performance.

1 Introduction

As the rapid development of networks, authentication between users is becoming increasingly important. In many scenarios, improving the performance of authentication is crucial. For example, in wireless sensor network and mobile social network, the battery life of devices is so short that complex authentication protocols are intolerable. Since digital signature is a main building block of authentication, reducing its complexity is an apparent approach towards meeting this demand. One way of reducing the complexity of signatures is to use identity-based signatures instead of regular signatures (which rely on certificates).

Identity-based signature (IBS) is a basic component of identity-based cryptography that was first introduced by Shamir [18] in 1984. As an alternative of traditional certificate-based cryptography, identity-based cryptography possesses an arresting advantage, i.e., it eliminates the onerous certificate management procedure in traditional certificate-based cryptography. To achieve the merit, each user in identity-based cryptosystem sets his identity (e.g. his e-mail address) as his public key (while in traditional certificate-based cryptosystem, users' public keys are random strings). The secret key of any user is generated by a trusted Private Key Generator (PKG) from PKG's secret key and the user's identity. Thanks to this advantage, IBSs are more preferable than regular signatures in many real-world applications.

After Shamir's seminal work, several IBSs emerged (e.g. [9]), however fully practical implementations are recently proposed due to the work of [6]. In [6], Boneh and Franklin designed an efficient identity-based encryption scheme by utilizing bilinear pairings. Since then, many excellent proposals for IBS appeared based on pairings [11,8,5,15]. These IBS proposals are very efficient for practical applications, whereas they all substantially rely on the discrete logarithm problem that is facile for quantum computers [19]. In view of the recent progresses of quantum computer, looking for quantum-immune IBSs is no longer alarmist. To achieve this, new mathematical tool on which cryptographic schemes are built should be developed. Lattice seems to be

* Corresponding author. E-mail: miaotian@mail.ustc.edu.cn.

our best option because cryptographic schemes based on lattices are supported by worst-case hardness assumption and conjectured to withstand quantum attacks. Moreover, lattice-based cryptographic schemes are also easy to implement since typical computations involved in them are only integer matrix-vector multiplication and modular addition. (See [16] for an overview on lattice-based cryptography.)

In 2010, Rückert [17] successfully constructed the first two (hierarchical) IBSs over lattice assumptions. One is secure in the random oracle model and the other is secure in the standard model. Later on, some other lattice-based IBSs also appeared, e.g., [20,12]). All of the IBS constructions followed the signature framework of Gentry, Peikert and Vaikuntanathan [10]. According to the framework, the signing key $\mathbf{S}$ of a user is a trapdoor of the function like $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \mod q$, where $\mathbf{A}$ is a user-related matrix. Typically $\mathbf{S}$ is a short basis of the lattice defined by $\mathbf{A}$. Armed with the signing key $\mathbf{S}$, the user can run a preimage sampling algorithm for the function $f_{\mathbf{A}}$ to obtain a signature sig. For those lattice IBS schemes, the generation of users' signing keys requires lattice basis delegation technique [7,2,1]. Since the signing key size and the signature length will increase dramatically after lattice basis delegation, those IBSs would be inefficient in practice. In addition, the short basis (signing key) extraction algorithms involved in them are also very expensive, thus PKG will be overburdened.

Our Contributions. In this paper, we construct a new IBS scheme over lattice assumptions, which does not follow the signature framework of [10]. Actually, our IBS scheme adopts the rejection sampling technique of [13] and can be viewed as an identity-based version of Lyubashevsky's signature scheme [13]. Compared with other lattice-based IBS schemes, our scheme is much more efficient in terms of both communication and computation overhead. We prove the IBS scheme is secure against adaptive chosen message and identity attacks in the random oracle model under conventional short integer solution (SIS) assumption which, in turn, leads our IBS scheme to be secure under the worst-case hardness of approximating several classic lattice problems, by the results of [14].

Paper Organization. The remainder of this paper is organized as follows. Section 2 and Section 3 respectively give some preliminaries and an efficient signing key extraction algorithm to be used in this work. Section 4 provides our lattice-based IBS scheme. Section 5 concludes the whole paper.

2 Preliminaries

2.1 Notation

Throughout this paper, the security parameter is a positive integer n. For a positive integer k, $[k]$ denotes the set $\{1, \cdots, k\}$. Vectors are assumed to be in column form and are written as bold low-case letters, e.g., $\mathbf{v}$. The ith component of $\mathbf{v}$ is represented by v_i, and the ℓ_p norm of $\mathbf{v}$ is denoted by $||\mathbf{v}||_p$ (we will avoid writing p if $p = 2$). Matrices are represented by bold upper-case letters, e.g., $\mathbf{A}$. Let the ith column of $\mathbf{A}$ be $\mathbf{a}_i$ and define $||\mathbf{A}||_p = \max_i(||\mathbf{a}_i||_p)$. For a full rank square matrix $\mathbf{A}$, its Gram-Schmidt orthogonalization is denoted as $\widetilde{\mathbf{A}}$.

We say a function $f(n)$ is negligible if it is smaller than all polynomial fractions for sufficiently large n, and we use $\mathsf{negl}(n)$ to denote a negligible function of n. We say an event occurs with overwhelming probability if its probability is $1 - \mathsf{negl}(n)$.

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

2.2 Lattices

An m-dimensional lattice Λ is a full-rank discrete subgroup of $\mathbb{R}^m$. In this paper, we focus on integer lattices, i.e., those lattices whose points have coordinates in $\mathbb{Z}^m$. Among these lattices are the "q-ary" lattices.

Definition 1. *For prime q, $\boldsymbol{u}\in\mathbb{Z}_q^n$ and $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$, define the "q-ary" lattices as follows:*

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

2.3 Gaussians on Lattices

The Gaussian function is a useful tool in lattice-based cryptography.

Definition 2. *For any $s>0$ and $\boldsymbol{c}\in\mathbb{R}^m$, define the Gaussian function as:*

$$g_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp(-\pi||\boldsymbol{x}-\boldsymbol{c}||^2/s^2).$$

Let $g_{s,\boldsymbol{c}}(\Lambda)$ be a sum of $g_{s,\boldsymbol{c}}$ over the lattice Λ. The discrete Gaussian distribution over Λ with center $\boldsymbol{c}$ and parameter s is defined as

$$G_{\Lambda,s,\boldsymbol{c}}=g_{s,\boldsymbol{c}}(\boldsymbol{x})/g_{s,\boldsymbol{c}}(\Lambda).$$

For notational convenience, in the rest of the paper, $g_{s,0}$ and $G_{\Lambda,s,0}$ will be abbreviated as g_s and $G_{\Lambda,s}$, respectively.

The following facts about discrete Gaussian distribution are very useful in this work. They are from [14] and [10], respectively.

Lemma 1. *Let q prime and integer $m\geq 2n\log q$ and let Gaussian parameter $s\geq\omega(\sqrt{\log m})$. For any $\boldsymbol{u}\in\mathbb{Z}_q^n$, we have:*

1. *For all but a q^{-n} fraction of $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$, $Pr[\ \boldsymbol{x}\leftarrow G_{\Lambda^{\boldsymbol{u}}(\boldsymbol{A}),s}:||\boldsymbol{x}||>s\sqrt{m}\ ]\leq\mathsf{negl}(\mathrm{n})$.*
2. *For all but a $2q^{-n}$ fraction of $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$, if $\boldsymbol{e}\leftarrow G_{\mathbb{Z}^m,s}$, then the distribution of the syndrome $\boldsymbol{t}=\boldsymbol{A}\boldsymbol{e} \pmod q$ is statistically close to uniform over $\mathbb{Z}_q^n$.*

2.4 Hardness Assumption

The security of our signature scheme rests on the hardness of SIS problem [3].

Definition 3. *Given an integer $q>0$, a matrix $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ and a real γ, the SIS problem is finding a vector $\boldsymbol{v}\in\mathbb{Z}^m\backslash\{0\}$ such that $\boldsymbol{A}\boldsymbol{v}=0 \pmod q$ and $||\boldsymbol{v}||\leq\gamma$.*

For the hardness of SIS problem, Micciancio and Regev [14] have showed that, for any polynomial-bounded m, γ and for any prime $q\geq\gamma\cdot\omega(\sqrt{n\log n})$, solving SIS on the average is as hard as approximating some intractable lattice problems such as the shortest lattice vector problem in the worst case.

2.5 Short Bases of Lattices

Short basis of a lattice is an important concept in many lattice-based cryptographic schemes. Here, we recall two useful theorems on short lattice bases. The first theorem is adapted from Lemma 3.5 of [4] that shows a recent result on how to generate a short basis of an approximate uniform lattice. The second theorem comes from [10] that is about how to use a short lattice basis to solve a kind of SIS problems.

Theorem 1. *Let $q \geq 3$ be odd and $m > 5n \log q$. There is a probabilistic polynomial-time (PPT) algorithm $\mathsf{TrapGen}(q, n)$ that outputs a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ and a basis $\boldsymbol{B} \in \mathbb{Z}^{m \times m}$ of $\Lambda^{\perp}(\boldsymbol{A})$ such that $\boldsymbol{A}$ is statistical close to uniform, and $||\boldsymbol{B}|| \leq O(n \log q)$ and $||\widetilde{\boldsymbol{B}}|| \leq O(\sqrt{n \log q})$ with overwhelming probability.*

Theorem 2. *Let $m \geq n$ be an integer and q be prime. Let $\Lambda^{\perp}(\boldsymbol{A})$ be a lattice defined by matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ and $\boldsymbol{B}$ be a basis of $\Lambda^{\perp}(\boldsymbol{A})$. If $s \geq \|\widetilde{\boldsymbol{B}}\| \cdot \omega(\sqrt{\log n})$, then for any $\boldsymbol{u} \in \mathbb{Z}_q^n$, there is a PPT algorithm $\mathsf{SamplePre}(\boldsymbol{A}, \boldsymbol{B}, s, \boldsymbol{u})$ that outputs a vector $\boldsymbol{v} \in \Lambda^{\boldsymbol{u}}(\boldsymbol{A})$ from a distribution that is statistically close to $G_{\Lambda^{\boldsymbol{u}}(\boldsymbol{A}), s}$.*

2.6 Discrete Normal Distribution

This work will also make use of the discrete normal distribution.

Definition 4. *For any $\sigma > 0$ and $\boldsymbol{c} \in \mathbb{Z}^m$, define the continuous normal distribution as:*

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

Let $\rho_{\sigma,\boldsymbol{c}}^m(\mathbb{Z}^m)$ be a sum of $\rho_{\sigma,\boldsymbol{c}}^m$ over $\mathbb{Z}^m$. The discrete normal distribution over $\mathbb{Z}^m$ centered at $\boldsymbol{c} \in \mathbb{Z}$ with parameter σ is defined as

$$D_{\sigma,\boldsymbol{c}}^m(\boldsymbol{x}) = \rho_{\sigma,\boldsymbol{c}}^m(\boldsymbol{x}) / \rho_{\sigma,\boldsymbol{c}}^m(\mathbb{Z}^m).$$

In the rest of the paper, we will abbreviate $\rho_{\sigma,0}^m$ and $D_{\sigma,0}^m$ as ρ_{σ}^m and D_{σ}^m.

The following lemma shows two basic properties of such distributions [13,14].

Lemma 2. *For any $\sigma > 0$ and positive integer m, we have:*

1. $Pr[x \leftarrow D_{\sigma}^1 : |x| > 12\sigma] < 2^{-100}$.
2. $Pr[\boldsymbol{x} \leftarrow D_{\sigma}^m : ||\boldsymbol{x}|| > 2\sigma\sqrt{m}\ ] < 2^{-m}$.

Lyubashevsky [13] also shows the following interesting fact on the distribution.

Lemma 3. *For any $\boldsymbol{v} \in \mathbb{Z}^m$ and positive real α, if $\sigma = \omega(||\boldsymbol{v}||\sqrt{\log m})$, we have*

$$Pr[\boldsymbol{x} \leftarrow D_{\sigma}^m : D_{\sigma}^m(\boldsymbol{x}) / D_{\sigma,\boldsymbol{v}}^m(\boldsymbol{x}) = O(1)] = 1 - 2^{\omega(\log m)},$$

and more specifically, if $\sigma = \alpha||\boldsymbol{v}||$, then

$$Pr[\boldsymbol{x} \leftarrow D_{\sigma}^m : D_{\sigma}^m(\boldsymbol{x}) / D_{\sigma,\boldsymbol{v}}^m(\boldsymbol{x}) < e^{12/\alpha + 1/(2\alpha^2)}] > 1 - 2^{-100}.$$

2.7 Rejection Sampling Technique

The core idea of rejection sampling technique for a signature scheme is to make the distribution of the outputted signatures is independent of signing key. To achieve this goal, rejection sampling technique works as follows. When signing a message, a signer with signing key s first chooses a random y from some distribution and computes the candidate signature sig that is in the form of y adding to (or multiplying by) some function of s. Let the target distribution of the outputted signatures be f which is independent of s, and let the distribution of all candidate signatures be g which may be related to s. If $f(x) \leq Mg(x)$ for all x and some real $M > 0$, then the candidate signature sig can be output with probability $f(\mathsf{sig})/(Mg(\mathsf{sig}))$. By [21], we know if the signer follows the above process, then the distribution of the outputted signatures is f and the expected number of times this process will output a signature is M.

As an example of how to use the rejection sampling technique, consider the signature scheme of Lyubashevsky [13]. Its target distribution is D_σ^m. To sign a message μ, first select a random $\mathbf{y}$ from D_σ^m and compute $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$, where $\mathbf{S}$ is a signing key and $\mathbf{c}$ is a hash value on the inputs of $\mathbf{y}$ and μ. The candidate signature is $(\mathbf{c}, \mathbf{z})$. Notice that the $\mathbf{z}$'s distribution is $D_{\sigma,\mathbf{Sc}}^m$ and, by Lemma 3, $D_\sigma^m(\mathbf{y})/D_{\sigma,\mathbf{Sc}}^m(\mathbf{y}) \approx e$. Therefore, according to the rejection sampling technique, we know there exists a small $M(\approx e)$ such that if we output the candidate signature $(\mathbf{c}, \mathbf{z})$ with possibility $\min(1, \frac{D_\sigma^m(\mathbf{z})}{MD_{\sigma,\mathbf{Sc}}^m(\mathbf{z})})$ then $\mathbf{z}$'s distribution is D_σ^m (in this case, by Lemma 2, we have $||\mathbf{z}|| \leq 2\sigma\sqrt{m}$ with a high probability) and the expected number of running the signing process is no more than M.

3 Matrix Sampling Algorithm

In our construction, we need an efficient algorithm to extract each user's signing key that is a short matrix $\mathbf{S}$ satisfying $\mathbf{AS} = \mathbf{U} \pmod q$ for some user-defined matrix $\mathbf{U}$. We address this problem by introducing the algorithm $\mathsf{SampleMat}$ that is an extension of the preimage sampling algorithm $\mathsf{SamplePre}$ of [10].

The algorithm $\mathsf{SampleMat}(\mathbf{A}, \mathbf{B}, s, \mathbf{U})$ works as follows.

1. Input $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{U} \in \mathbb{Z}_q^{n\times k}$, a basis $\mathbf{B}$ of $\Lambda^\perp(\mathbf{A})$ and parameter $s \geq \|\widetilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$.
2. For each $i \in [k]$, run algorithm $\mathsf{SamplePre}(\mathbf{A}, \mathbf{B}, s, \mathbf{u}_i) \rightarrow \mathbf{s}_i \in \mathbb{Z}^m$.
3. Output $\mathbf{S} = [\mathbf{s}_1, \cdots, \mathbf{s}_k] \in \mathbb{Z}^{m\times k}$.

By Theorem 2, we know, for any $\mathbf{u} \in \mathbb{Z}_q^n$, the algorithm $\mathsf{SamplePre}(\mathbf{A}, \mathbf{B}, s, \mathbf{u})$ will sample a vector $\mathbf{v} \in \Lambda^{\mathbf{u}}(\mathbf{A})$ from a distribution that is statistically close to $G_{\Lambda^{\mathbf{u}}(\mathbf{A}),s}$. Therefore, we can easily check that the output $\mathbf{S}$ of the above algorithm $\mathsf{SampleMat}(\mathbf{A}, \mathbf{B}, s, \mathbf{U})$ satisfies $\mathbf{AS} = \mathbf{U} \pmod q$ and its distribution is statistically close to $G_{\Lambda^{\mathbf{u}_1}(\mathbf{A}),s} \times \cdots \times G_{\Lambda^{\mathbf{u}_k}(\mathbf{A}),s}$ (thus $||\mathbf{S}|| \leq s\sqrt{m}$ with overwhelming probability by Lemma 1). As a result, we have the following lemma.

Lemma 4. *Let $m \geq n$ and $k \geq 2$ be positive integers, and let q be prime. Let $\Lambda^\perp(\boldsymbol{A})$ be a lattice defined by matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ and $\boldsymbol{B}$ be a basis of $\Lambda^\perp(\boldsymbol{A})$. If parameter $s \geq \|\widetilde{\boldsymbol{B}}\| \cdot \omega(\sqrt{\log n})$, then for any $\boldsymbol{U} \in \mathbb{Z}_q^{n\times k}$, there is a PPT algorithm $\mathsf{SampleMat}(\boldsymbol{A}, \boldsymbol{B}, s, \boldsymbol{U})$ that outputs a matrix $\boldsymbol{S} \in \mathbb{Z}^{m\times k}$ from a distribution that is statistically close to $G_{\Lambda^U(\boldsymbol{A}),s}$ such that $\boldsymbol{AS} = \boldsymbol{U} \pmod q$ and $||\boldsymbol{S}|| \leq s\sqrt{m}$ with overwhelming probability, where $G_{\Lambda^U(\boldsymbol{A}),s} = G_{\Lambda^{u_1}(\boldsymbol{A}),s} \times \cdots \times G_{\Lambda^{u_k}(\boldsymbol{A}),s}$.*

4 An efficient IBS scheme from lattices

We here give the description of our efficient IBS scheme based on lattice assumptions.

4.1 Construction

Our IBS construction involves a few parameters defined below:

- prime $q \geq 3$, real M, $m > 5n \log q, k, \lambda$ are all positive integers.
- bound $\widetilde{L} = O(\sqrt{n \log q})$, Gaussian parameter $s = \widetilde{L} \cdot \omega(\sqrt{\log n})$, $\sigma = 12s\lambda m$.

The IBS scheme works as follows.

$\mathsf{Setup}(n)$**.** Given a security parameter n, do the following:

1. Run $\mathsf{TrapGen}(q, n)$ to output an approximate uniform matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ along with a basis $\mathbf{B} \in \mathbb{Z}_q^{m \times m}$ of $\Lambda^{\perp}(\mathbf{A})$ such that $||\widetilde{\mathbf{B}}|| \leq \widetilde{L}$.
2. Select two hash functions $H : \{0,1\}^* \to \{\mathbf{v} : \mathbf{v} \in \{-1, 0, 1\}^k, ||\mathbf{v}||_1 \leq \lambda\}$ and $H_1 : \{0,1\}^* \to \mathbb{Z}_q^{n \times k}$.
3. Output the public parameters $params = \{\mathbf{A}, H, H_1\}$ and PKG's secret key $SK = \mathbf{B}$.

$\mathsf{Extract}(params, SK, ID)$**.** Given the public parameters $params$, PKG's secret key $SK = \mathbf{B}$ and an identity $ID \in \{0,1\}^*$, run algorithm $\mathsf{SampleMat}(\mathbf{A}, \mathbf{B}, s, H_1(ID))$ to obtain a signing key $sk_{ID} = \mathbf{S}_{ID} \in \mathbb{Z}^{m \times k}$ for the user with identity ID. The correctness of $\mathbf{S}_{ID}$ can be verified by checking if $\mathbf{AS}_{ID} = H_1(ID)$ and $||\mathbf{S}_{ID}|| \leq s\sqrt{m}$.

$\mathsf{Sign}(params, \mu, sk_{ID})$**.** Given the public parameters $params$, a message $\mu \in \{0,1\}^*$ and a signing key $sk_{ID} = \mathbf{S}_{ID}$, do the following:

1. Select a random $\mathbf{y} \leftarrow D_{\sigma}^m$.
2. Compute $\mathbf{h} = H(\mathbf{Ay}, \mu)$ and $\mathbf{z} = \mathbf{S}_{ID}\mathbf{h} + \mathbf{y}$.
3. Output $\mathsf{sig} = (\mathbf{h}, \mathbf{z})$ with probability $\min(1, \frac{D_{\sigma}^m(\mathbf{z})}{MD_{\sigma, \mathbf{S}_{ID}\mathbf{h}}^m(\mathbf{z})})$. If nothing is outputted, repeat the algorithm $\mathsf{Sign}(params, \mu, sk_{ID})$.

$\mathsf{Verify}(params, \mathsf{sig}, \mu, ID)$**.** Given the public parameters $params$, a signature $\mathsf{sig} = (\mathbf{h}, \mathbf{z})$, a message μ and an identity ID, output 1 if and only if $\mathbf{h} = H(\mathbf{Az} - H_1(ID)\mathbf{h}, \mu)$ and $||\mathbf{z}|| \leq 2\sigma\sqrt{m}$.

4.2 Correctness

Theorem 3. *The identity-based signature scheme above satisfies correctness.*

Proof. According to the construction of the IBS scheme, we know that

$$\begin{aligned} & \mathbf{Az} - H_1(ID)\mathbf{h} \\ = \ & \mathbf{Az} - \mathbf{AS}_{ID}\mathbf{h} \\ = \ & \mathbf{A}(\mathbf{z} - \mathbf{S}_{ID}\mathbf{h}) \\ = \ & \mathbf{Ay} \end{aligned}$$

Therefore, we have $H(\mathbf{Az} - H_1(ID)\mathbf{h}, \mu) = H(\mathbf{Ay}, \mu) = \mathbf{h}$.

By simply combining the rejection sampling technique described in Section 2.7 with Lemma 3, we know the distribution of $\mathbf{z}$ is very close to D_{σ}^m. Therefore, by Lemma 2, we have $||\mathbf{z}|| \leq 2\sigma\sqrt{m}$ with probability at least $1 - 2^{-m}$.

4.3 Efficiency

The most efficient (presently known) lattice-based IBS schemes are those ones that are secure in the random oracle model, e.g., the IBS schemes[1] proposed respectively by Rückert [17] and Tian et al. [20]. We now compare the performance of our IBS scheme to that of the two schemes.

Table 1 lists the comparison on the communication overhead of the three schemes for the same security parameter n, where the constant c is the bit length of all identities in Rückert's scheme with random oracle, $\bar{s} = s\sqrt{(c+1)m}\omega(\sqrt{\log n})$ and $\hat{s} = s \cdot m\omega(\log^{3/2} n)$ are extended Gaussian parameters, and other parameters are the same as those in Section 4.1. Since $m \gg k$ and $n \gg \lambda(\log k + 1)$ for reasonable security (e.g., 512 bits or more), one can easily check that the signing key size and the signature length of our scheme are both much smaller than those of Rückert's scheme as well as those of Tian et al.'s scheme.

Table 1. Comparison of several lattice-based IBS schemes

Scheme	Signing key size	Signature size
Rückert [17] with RO	$\big(m(c+1)\big)^2 \log(\bar{s}\sqrt{(c+1)m})$	$m(c+1)\log(\bar{s}\sqrt{(c+1)m}) + n$
Tian et al. [20]	$m^2 \log(\hat{s}\sqrt{m})$	$m\log(\hat{s}\sqrt{m}) + n$
This work	$mk\log(s\sqrt{m})$	$m\log(12\sigma) + \lambda(\log k + 1)$

In terms of computation complexity, we can see that the signing and verification algorithms of our scheme are very simple because they only take matrix-vector multiplication, integer addition and hash operations, whereas signing a message in the schemes of Rückert and Tian et al. both need to run the more complicated algorithm SamplePre. Moreover, the signing key extraction algorithm in our scheme is the algorithm SampleMat, which is much faster than the algorithm RandBasis used in the extraction algorithms of Rückert and Tian et al.'s schemes.

Therefore, we can conclude that our IBS scheme is more efficient than other lattice-based ones in terms of both communication and computation overhead.

4.4 Security

Theorem 4. *The proposed identity-based signature scheme is existential unforgeable against adaptive chosen message and identity attacks in the random oracle model, assuming the hardness of SIS problem.*

The proof of Theorem 4 will appear in the full version of this paper.

5 Conclusion

In this paper, we presented the first lattice-based IBS scheme that dose not employ the signature framework of [10]. We proved its security in the random oracle model under the SIS assumption. Our IBS scheme is more efficient than others based on lattices. We believe the ideas and techniques used in this work will also be helpful for designing other lattice-based signatures.

[1] Notice that these IBS schemes are both generalized ones, i.e., they may have more than two hierarchies. For comparability, we here set their hierarchy depth as 2 (including the PKG).

Acknowledgements

This work was partially supported by the National Natural Science Foundation of China (No. 61202407), the Basic Perspective Project of SGCC (No. XXN51201304253), and the Natural Science Foundation of Jiangsu Province of China (No. BK2011357).

References

1. S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (h)ibe in the standard model. In *EUROCRYPT 2010*, pages 553–572. Springer, 2010.
2. S. Agrawal, D. Boneh, and X. Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical ibe. In *CRYPTO 2010*, pages 98–115. Springer, 2010.
3. M. Ajtai. Generating hard instances of lattice problems. In *STOC'96*, pages 99–108. ACM, 1996.
4. J. Alwen and C. Peikert. Generating shorter bases for hard random lattices. *Theory of Computing Systems*, 48(3):535–553, 2011.
5. P.S.L.M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *ASIACRYPT 2005*, pages 515–532. Springer, 2005.
6. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO 2001*, pages 213–229. Springer, 2001.
7. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In *EUROCRYPT 2010*, pages 523–552. Springer, 2010.
8. J.C. Choon and J.H. Cheon. An identity-based signature from gap diffie-hellman groups. In *PKC 2003*, pages 18–30. Springer, 2002.
9. A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. In *CRYPTO'86*, pages 186–194. Springer, 1987.
10. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC 2008*, pages 197–206. ACM, 2008.
11. F. Hess. Efficient identity based signature schemes based on pairings. In *Selected Areas in Cryptography*, pages 310–324. Springer, 2003.
12. Z. Liu, Y. Hu, X. Zhang, and F. Li. Efficient and strongly unforgeable identity-based signature scheme from lattices in the standard model. *Security and Communication Networks*, 6(1):69–77, 2013.
13. V. Lyubashevsky. Lattice signatures without trapdoors. In *EUROCRYPT 2012*, pages 738–755. Springer, 2012.
14. D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Computing*, 37(1):267–302, 2007.
15. K.G. Paterson and J.C.N. Schuldt. Efficient identity-based signatures secure in the standard model. In *ACISP 2006*, pages 207–222. Springer, 2006.
16. O. Regev. Lattice-based cryptography. In *CRYPTO 2006*, pages 131–141. Springer, 2006.
17. M. Rückert. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles. In *Post-Quantum Cryptography*, pages 182–200. Springer, 2010.
18. A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO'84*, pages 47–53. Springer, 1985.
19. P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Computing*, 26(5):1484–1509, 1997.
20. M. Tian, L. Huang, and W. Yang. Efficient hierarchical identity–based signatures from lattices. *Int. J. Electronic Security and Digital Forensics*, 5(1):1–10, 2013.
21. J. Von Neumann. Various techniques used in connection with random digits. *J. Research Nat. Bur. Stand., Appl. Math. Series*, 12(1):36–38, 1951.