Frontiers of Information Technology & Electronic Engineering
www.zju.edu.cn/jzus; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Efficient identity-based signature over NTRU lattice*

Jia XIE†[1,2], Yu-pu HU[1,2], Jun-tao GAO[1,2], Wen GAO[1,2]

([1]*School of Telecommunications Engineering, Xidian University, Xi'an 710071, China*)

([2]*The State Key Laboratory of Integrated Services Network, Xi'an 710071, China*)

†E-mail: xiejia199325@163.com

Received June 21, 2015; Revision accepted Oct. 12, 2015; Crosschecked Dec. 30, 2015

Abstract: Identity-based signature has become an important technique for lightweight authentication as soon as it was proposed in 1984. Thereafter, identity-based signature schemes based on the integer factorization problem and discrete logarithm problem were proposed one after another. Nevertheless, the rapid development of quantum computers makes them insecure. Recently, many efforts have been made to construct identity-based signatures over lattice assumptions against attacks in the quantum era. However, their efficiency is not very satisfactory. In this study, an efficient identity-based signature scheme is presented over the number theory research unit (NTRU) lattice assumption. The new scheme is more efficient than other lattice- and identity-based signature schemes. The new scheme proves to be unforgeable against the adaptively chosen message attack in the random oracle model under the hardness of the γ-shortest vector problem on the NTRU lattice.

Key words: Identity, Signature, Lattice, Number theory research unit (NTRU)
http://dx.doi.org/10.1631/FITEE.1500197 **CLC number:** TP309.7

1 Introduction

Digital signatures are the cornerstones of e-business, e-government, software security, and other applications. Their importance is increasing as increasing numbers of tasks and processes are computerized every day. In the most basic form, each user in the digital signature system generates his/her own key pair consisting of a public key and a corresponding private key, and the user is assumed to be uniquely identified by his/her public key. However, the cost associated with public key infrastructures and certificates is huge.

To simplify the key management procedures of certificated-based public key infrastructures, an identity-based signature (IBS) scheme was proposed by Shamir (1984). Since then, several IBS schemes have been proposed based on the integer factorization problem, such as the first IBS scheme (Desmedt and Quisquater, 1987), a new realization scheme (Tanaka, 1987), the IBS scheme in Tsuji and Itoh (1989), and an identity-based noninteractive public-key distribution system (Maurer and Yacobi, 1991). However, the first fully practical IBS was proposed by Boneh and Franklin (2001) based on bilinear pairings. Thereafter, many excellent proposals for IBS based on pairings appeared, such as the IBS proposed by Hess (2003), the efficient IBS scheme proposed by Paterson and Schuldt (2006), and the signature scheme proposed by Barreto *et al.* (2005). These IBS proposals were very efficient for practical applications, and they all substantially relied on the discrete logarithm problem. However, Shor (1997) indicated that the discrete logarithm problem and the integer factorization problem would no longer be hard when quantum computers come into reality. In view of the recent progress in quantum computers, looking for a quantum-immune IBS scheme is very crucial (Krenn *et al.*, 2014).

Lattice seems to be the best candidate because

* Project supported by the National Natural Science Foundation of China (Nos. 61173151, 61472309, and 61303217), the Fundamental Research Funds for the Central Universities, China (No. JB140115), and the Natural Science Foundation of Shaanxi Province, China (Nos. 2013JQ8002 and 2014JQ8313)

ORCID: Jia XIE, http://orcid.org/0000-0002-0894-0369

cryptographic schemes based on lattices are supported by the worst-case hardness assumption, and Bernstein (2009) has conjectured that lattice can withstand quantum attacks. What is more, lattice-based cryptographic schemes are easy to implement because typical computations involved in them are only integer matrix-vector multiplication and modular addition (refer to Micciancio and Regev (2006) for an overview on lattice-based cryptography). Rückert (2010) successfully constructed the first two (hierarchical) IBS schemes over lattice assumptions. One is secure in the random oracle model, and the other in the standard model. Some other lattice-based IBS schemes appeared later on, such as the identity-based signcryption (Li *et al.*, 2012), the efficient IBS proposed by Tian *et al.* (2013), the efficient and strongly unforgeable IBS (Liu *et al.*, 2013), and the efficient lattice-based IBS (Tian and Huang, 2014). Nevertheless, the efficiency of these lattice-based IBS schemes is not very satisfactory. As is well known, the number theory research unit (NTRU) lattice is the most efficient lattice. So, the IBS scheme on an NTRU lattice may be a good attempt.

Inspired by the identity-based encryption (IBE) scheme (Ducas *et al.*, 2014), we propose the first efficient IBS scheme based on the small integer solution (SIS) problem over the NTRU lattice. Since the NTRU lattice features reasonable simplicity, easily created keys, high speed, and low memory requirements, it is believed that the cryptosystems over the NTRU lattice are always more efficient than those over the general lattice. Actually, compared with other lattice-based IBS schemes, our scheme is more efficient. And it is proved that the IBS scheme is secure against adaptively chosen message and adaptively chosen identity attacks in the random oracle model under the SIS assumption over the NTRU lattice, which in turn leads our IBS scheme to be secure under the hardness of the γ-shortest vector problem (γ-SVP).

2 Preliminaries

2.1 Notation

2.1.1 The ring $\mathbb{Z}_q[x]/(x^N+1)$

Throughout this study, the security parameter $N=2^t$ is an integer larger than 8. $\mathbb{R}$ and $\mathbb{Z}$ are the real and integer spaces, respectively. We will work in the ring $R=\mathbb{Z}[x]/(x^N+1)$ and ring $R_q=\mathbb{Z}_q[x]/(x^N+1)$, where the prime q is larger than 5. It is also satisfied that x^N+1 can be split into k_q irreducible factors modulo prime q. $R^\times$ denotes the set of invertible elements in R. Vectors will be denoted by bold lower-case letters in italics (e.g., $\boldsymbol{x}$), and matrices will be denoted by bold capital letters in italics (e.g., $\boldsymbol{X}$). The inner product of two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ will be denoted by $<\boldsymbol{x}, \boldsymbol{y}>$. For $\boldsymbol{x}\in\mathbb{R}^N$, $\|\boldsymbol{x}\|$ denotes the Euclidean norm of $\boldsymbol{x}$.

Let $f=\sum_{i=0}^{N-1} f_i x^i$ and $g=\sum_{i=0}^{N-1} g_i x^i$ be polynomials in R. fg denotes the polynomial multiplication in R, $f*g=fg \bmod (x^N+1)$, and $(f, g)\in \mathbb{R}^{2N}=R^{1\times 2}$ is the concatenation of f and g.

2.1.2 Anticirculant matrices

Definition 1 (Anticirculant matrices) An N-dimensional anticirculant matrix of f is the following Toeplitz matrix:

$$\boldsymbol{C}_N(f)=\begin{pmatrix} f_0 & f_1 & \cdots & f_{N-1} \\ -f_{N-1} & f_0 & \cdots & f_{N-2} \\ \vdots & \vdots & & \vdots \\ -f_1 & -f_2 & \cdots & f_0 \end{pmatrix}=\begin{pmatrix} f \\ x*f \\ \vdots \\ x^{N-1}*f \end{pmatrix}.$$

When it is clear from the context, we will drop the subscript N, and just write $\boldsymbol{C}(f)$.

2.2 Lattices

An N-dimensional lattice is a full-rank discrete subgroup of $\mathbb{R}^N$. Here, we focus on the NTRU lattice.

Definition 2 (NTRU lattice) Let q be a prime larger than 5 and N an integer which is a power of 2, and f, $g\in R$ (f is invertible modulo q). Let $h=(g\times f^{-1} \bmod q)$. The NTRU lattice associated with h and q is $\Lambda_{h,q}=\{(u, v)\in R^2: u+v\times h=0 \,(\mathrm{mod}\, q)\}$. Here, $\Lambda_{h,q}$ is a full-rank lattice of $\mathbb{R}^{2N}$ generated by the row of

$$\boldsymbol{A}_{h,q}=\begin{pmatrix} -\boldsymbol{C}_N(h) & \boldsymbol{I}_N \\ q\boldsymbol{I}_N & \boldsymbol{O}_N \end{pmatrix},$$

where $\boldsymbol{I}_N$ and $\boldsymbol{O}_N$ are the $N\times N$ unit matrix and $N\times N$ null matrix, respectively.

2.3 Gaussians on lattices

Gaussian sampling was introduced by Gentry *et al.* (2008) as a technique to use a short basis as a trapdoor without leaking any information about the short basis. The discrete Gaussian distribution on lattice is defined as follows:

Definition 3 (Discrete Gaussian distribution) For any $s>0$, $\boldsymbol{c}\in\mathbb{R}^N$, define the N-dimensional Gaussian function $\rho_{s,\boldsymbol{c}}$: $\mathbb{R}^N\to(0, 1]$ as

$$\rho_{s,\boldsymbol{c}}(\boldsymbol{x})\triangleq\exp\left(-\pi\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}\right).$$

For any lattice $\Lambda\subset\mathbb{R}^N$, $\rho_{s,\boldsymbol{c}}(\Lambda)\triangleq\sum_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})$. The probability mass function of the discrete Gaussian distribution is $D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\rho_{s,\boldsymbol{c}}(\boldsymbol{x})/\rho_{s,\boldsymbol{c}}(\Lambda)$. For convenience, in the rest of this paper, $\rho_{s,\boldsymbol{0}}(\boldsymbol{x})$ and $D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})$ will be abbreviated as $\rho_s(\boldsymbol{x})$ and $D_{\Lambda,s}(\boldsymbol{x})$, respectively.

In the following lemmas, we review several well-known facts about discrete Gaussian distribution.

Lemma 1 (Nguyen and Regev, 2006) Given any N-dimensional lattice Λ, center $\boldsymbol{c}\in\mathbb{R}^N$, $\varepsilon>0$, and $s>2\eta_\varepsilon(\Lambda)$, for any $\boldsymbol{x}\in\Lambda$, we have

$$D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})\le\frac{1+\varepsilon}{1-\varepsilon}2^{-N},$$

where $2\eta_\varepsilon(\Lambda)$ is the smoothing parameter of the lattice Λ. For $\varepsilon<1/3$, the minimum entropy of $D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})$ is at least $N-1$.

Lemma 2 For any $\sigma>0$ and positive integer m, the probability that the following event occurs satisfies

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

Lemma 3 (Lyubashevsky, 2012) For any $\boldsymbol{v}\in\mathbb{Z}^m$ and positive real α, if $\sigma=\omega(\|\boldsymbol{v}\|\sqrt{\log m})$ where $\omega(\cdot)$ is the non-asymptotic tight lower bound, 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 $\sigma=\alpha\|\boldsymbol{v}\|$, it is derived that

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

To obtain the vectors following a discrete Gaussian distribution, we introduce the Gaussian sampler algorithm in Algorithm 1.

Algorithm 1 Gaussian_Sampler($\boldsymbol{B}$, σ, $\boldsymbol{c}$)

Input: A basis $\boldsymbol{B}$ of an N-dimensional lattice Λ, standard deviation $\sigma>0$, and center $\boldsymbol{c}\in\mathbb{Z}^N$

Output: $\boldsymbol{v}$ sampled in $D_{\Lambda,\sigma,\boldsymbol{c}}$

$\boldsymbol{v}_N\leftarrow\boldsymbol{0}$
$\boldsymbol{c}_N\leftarrow\boldsymbol{c}$
for $i\leftarrow N, \ldots, 2, 1$ **do**
  $c_i'\leftarrow<\boldsymbol{c}_i,\boldsymbol{b}_i>/\|\tilde{\boldsymbol{b}}_i\|^2$
  $\sigma_i'\leftarrow\sigma/\|\tilde{\boldsymbol{b}}_i\|^2$
  $z_i\leftarrow$Sample_$Z(\sigma_i',c_i')$
  $\boldsymbol{c}_{i-1}\leftarrow\boldsymbol{c}_i-z_i\boldsymbol{b}_i$ and $\boldsymbol{v}_{i-1}\leftarrow\boldsymbol{v}_i-z_i\boldsymbol{b}_i$
end for
return $\boldsymbol{v}_0$

In Algorithm 1, $\tilde{\boldsymbol{B}}=(\tilde{\boldsymbol{b}}_i)_{i\in N}$ is the Gram-Schmidt orthogonalization of $\boldsymbol{B}$, and the procedure Sample_$Z(\sigma_i',c_i')$ samples a one-dimensional vector from Gaussian distribution $D_{\mathbb{Z},\sigma',\boldsymbol{c}'}$.

2.4 Rejection sampling technique

Rejection sampling was first proposed by Lyubashevsky (2012). The core idea of the rejection sampling technique for a signature scheme is to make the distribution of the output signatures independent of the signing key (Algorithm 2).

Algorithm 2 Signature scheme with rejection sampling (Lyubashevsky, 2012)

Input: H: $\{0,1\}^*\to\{\boldsymbol{v}:\boldsymbol{v}\in\{-1,0,1\}^k,\|\boldsymbol{v}\|_1\le c\}$ (c is constant, k is a positive integer and $k\ll m$), message μ, a matrix $\boldsymbol{A}$ randomly sampled from $\mathbb{Z}_q^{n\times m}$, and a signature key $\boldsymbol{S}$ sampled from $\{-d,\ldots,0,\ldots,d\}^{m\times k}$

Output: vectors $\boldsymbol{z}$ and $\boldsymbol{c}$

Sample D_σ^m randomly to obtain $\boldsymbol{y}$
$\boldsymbol{c}\leftarrow H(\boldsymbol{A}\boldsymbol{y},\mu)$
$\boldsymbol{z}\leftarrow\boldsymbol{S}\boldsymbol{c}+\boldsymbol{y}$
return $(\boldsymbol{z},\boldsymbol{c})$ with probability $\min(1, D_\sigma^m(\boldsymbol{z})/(MD_{\boldsymbol{S}\boldsymbol{c},\sigma}^m(\boldsymbol{z})))$

2.5 Hardness assumption

Our signature scheme is based on the SIS problem on the NTRU lattice.

Definition 4 (SIS over ring $R-\mathrm{SIS}^{\phi}_{q,m,\beta}$) The small integer solution problem on ring with parameters q, m, β, and ϕ is defined as follows: given m polynomials a_1, a_2, …, a_m chosen uniformly and independently in $R_q=\mathbb{Z}_q[x]/(\phi)$, finding the solution $t\in\boldsymbol{a}^{\perp}\backslash 0$ which satisfies the condition $\|\boldsymbol{t}\|\leq\beta$, where $\boldsymbol{a}^{\perp}:=\{(t_1,t_2,...,t_m)\in R^m:\sum_i t_i a_i=0 \pmod q\}$.

When f and g are chosen according to Algorithm 3, Theorem 4.1 in Stehlé and Steinfeld (2013) shows that the statistical distance between the distribution of $h=g/f$ and the uniform distribution of $R^{\times}$ is $2^{10N}q^{-\lfloor \varepsilon N\rfloor}$, which is negligible. So, the SIS on the NTRU lattice can be defined in the following manner:

Definition 5 (SIS on the NTRU lattice, namely $R-\mathrm{SIS}^{\kappa}_{q,1,2,\beta}$) A way to state the SIS problem on the NTRU lattice is to set $R=\mathbb{Z}[x]/(x^N+1)$ and let κ be the distribution that picks small f and g according to Algorithm 3, $\boldsymbol{A}_{h,q}=(h,1)\in R_q^{1\times 2}$, and $h=g/f$. So, the SIS on the NTRU lattice is to find (z_1,z_2) that satisfies the conditions $\boldsymbol{A}_{h,q}(z_1,z_2)^{\mathrm{T}}=\boldsymbol{0} \pmod q$ and $\|(z_1,z_2)\|\leq\beta$.

Algorithm 3 Sample(f, g)

Input: N, q, σ
Output: f, g, h
1 Sample f from $D_{\mathbb{Z}^N,\sigma}$
2 **if** $(f \bmod q)\notin R_q^{\times}$ **then**
3 Resample
4 **end if**
5 Sample g from $D_{\mathbb{Z}^N,\sigma}$
6 **if** $(g \bmod q)\notin R_q^{\times}$ **then**
7 Resample
8 **end if**
9 **return** f, g, and $h=g/f$

Definition 6 (SVP on the NTRU lattice) For the NTRU lattice $\Lambda_{h,q}$ generated by the basis $\boldsymbol{A}_{h,q}$, the SVP on this lattice is to find the vector $(u,v)\in\Lambda_{h,q}$ such that $\|(u,v)\|\leq\|(s,t)\|$, $\forall(s,t)\in\Lambda_{h,q}$. So, γ-SVP is to find the vector $(u,v)\in\Lambda_{h,q}$ such that $\|(u,v)\|\leq\gamma\lambda_1(\Lambda_{h,q})$, where $\lambda_1(\Lambda_{h,q})$ is the successive minimum of $\Lambda_{h,q}$.

According to Definitions 5 and 6, we know that the SIS problem on the NTRU lattice is equal to the approximate SVP on the NTRU lattice when $\gamma=\beta/\lambda_1(\Lambda_{h,q})$. So, the new IBS signature scheme is based on the hardness of γ-SVP on the NTRU lattice against polynomial time algorithms.

3 Syntax and the proposed IBS scheme

3.1 Syntax

Definition 7 (IBS scheme) An IBS scheme has five probabilistic polynomial time algorithms (Setup, Extract, Master_Keygen, Signature, and Verification), where

1. Setup(λ): a randomized algorithm that takes a security parameter λ as input and outputs the system-wide public parameter pp;

2. Master_Keygen(pp): on input of the public parameter pp, the algorithm outputs the master public/private keys (msk, mpk);

3. Extract(id, msk, mpk): taking the identity id and the master public/private key pair (msk, mpk) as input, this algorithm produces the private key $\mathrm{sk}_{\mathrm{id}}$ of the identity id and sends it to id;

4. Signature(id, μ, mpk, $\mathrm{sk}_{\mathrm{id}}$): given the identity id, the master public key mpk, the message μ, and the private key $\mathrm{sk}_{\mathrm{id}}$ of the identity id as input, this algorithm subsequently outputs the signature sig of message μ;

5. Verification(id, μ, sig): on input of the identity id, the message μ, and the signature sig, the deterministic algorithm outputs 1 when the verification is correct, and outputs 0 otherwise.

3.2 The proposed IBS scheme

We construct a new IBS scheme over the NTRU lattice:

1. Setup(N): on input of the security parameter N, this algorithm outputs the public parameters as follows:

$$q=\mathrm{Poly}(N),\ \varepsilon\in\left(0,\frac{\ln N}{\ln q}\right),\ s=\tilde{\Omega}(N^{3/2}\sigma),$$

where Poly(N) is the polynomial function of security parameter N and $\tilde{\Omega}(\cdot)$ the asymptotic lower bound.

If k_q=N>2, we have $\sigma=N\sqrt{\ln(8Nq)}\cdot q^{1/2+\varepsilon}$ and $q^{1/2-\varepsilon}=\tilde{\Omega}(N^{7/2})$; if k_q=2, we have $\sigma=\sqrt{N\ln(8Nq)}\cdot q^{1/2+\varepsilon}$ and $q^{1/2-\varepsilon}=\tilde{\Omega}(N^3)$.

2. Master_Keygen(N, q), as shown in Algorithm 4.

3. Extract($\boldsymbol{B}$, id), as shown in Algorithm 5.

4. Signature(id, μ), as shown in Algorithm 6.

5. Verification(id, μ, (z_1, z_2, u)), as shown in Algorithm 7.

Algorithm 4 Master_Keygen(N, q)

Input: $N, q \in \mathbb{Z}, \sigma > 0$

Output: $(\text{msk}, \text{mpk}) \in \mathbb{R}^{2N\times 2N} \times R_q^{\times}$

1 Sample f and g from $D_{\mathbb{Z}^N,\sigma}$ that satisfy $(f \bmod q) \notin R_q^{\times}$ and $(g \bmod q) \notin R_q^{\times}$

2 **if** $\|f\| > \sigma\sqrt{N}$ or $\|g\| > \sigma\sqrt{N}$ **then**

3 Restart

4 **end if**

5 **if** $\langle f, g\rangle \neq R$ **then**

6 Restart

7 **end if**

8 Compute F_1, $G_1 \in R$ such that $fG_1 - gF_1 = 1$

9 Set $F_q = qF_1$ and $G_q = qG_1$

10 Use the nearest plane algorithm (Babai, 1986) to approximate pair (F_q, G_q) by an integer linear combination of (f, g), (xf, xg), …, ($x^{n-1}f$, $x^{n-1}g$). Let (F, G) be the output, such that there exists $k \in R$ with $(F, G)=(F_q, G_q)-k(f, g)$

11 **if** $\|(F, G)\| > N\sigma$ **then**

12 Restart

13 **end if**

14 **return** $\text{msk}=\boldsymbol{B}=\begin{pmatrix}\boldsymbol{C}(f) & \boldsymbol{C}(g)\\ \boldsymbol{C}(F) & \boldsymbol{C}(G)\end{pmatrix}$ and the master public key $\text{mpk}=h=g/f \in R_q^{\times}$

Algorithm 5 Extract($\boldsymbol{B}$, id)

Input: hash function $H: \{0,1\}^* \to \mathbb{Z}_q^N$, user identity id, and

$$\text{msk}=\begin{pmatrix}\boldsymbol{C}(f) & \boldsymbol{C}(g)\\ \boldsymbol{C}(F) & \boldsymbol{C}(G)\end{pmatrix}$$

Output: $\text{sk}_{\text{id}}=(s_1, s_2)$

1 **if** sk_{id} in local storage **then**

2 **return** sk_{id} to user id

3 **else**

4 $t \leftarrow H(\text{id}) \in \mathbb{Z}_q^N$

5 $(s_1, s_2) \leftarrow [(t, 0) - \text{Gaussian\_Sampler}(\boldsymbol{B}, \sigma, (t, 0))]$, where s_1 and s_2 satisfy $\{s_1+s_2*h=t\}$

6 $\text{sk}_{\text{id}} \leftarrow (s_1, s_2)$

7 **return** sk_{id} to user id and keep it in local storage

8 **end if**

Algorithm 6 Signature(id, μ)

Input: private key sk_{id}, user's identity id, message μ, and the hash function $H': \{0,1\}^* \to \{v \in \{-1, 0, 1\}^N, \|v\|_1 \le \lambda\}$

Output: sig=(z_1, z_2, u)

1 Choose $y_1, y_2 \in D_{\mathbb{Z}^N,s}$

2 Compute $u=H'(y_1+h*y_2, \mu)$

3 **for** i=1, 2 **do**

4 Compute $z_i=y_i+s_i*u$

5 **end for**

6 **return** (z_1, z_2, u) with probability $\min\left(\frac{D_{\mathbb{Z}^N,s}}{MD_{\mathbb{Z}^N,s,\text{sk}_{\text{id}}u}}, 1\right)$, where $M=O(1)$

Algorithm 7 Verification(id, μ, (z_1, z_2, u))

Input: H, H', id, μ, and (z_1, z_2, u)

Output: 1 or 0

1 **if** $\|(z_1, z_2)\| \le 2s\sqrt{2N}$, $H'(h*z_2+z_1-H(\text{id})*u, \mu)=u$ **then**

2 **return** 1

3 **else**

4 **return** 0

5 **end if**

4 Analysis of the proposed IBS scheme

4.1 Correctness

To retain the correctness of the proposed IBS scheme, we have taken the same parameters as the ones in the presample function (Stehlé and Steinfeld, 2013) and set $H': \{0,1\}^* \to v \in \mathbb{Z}_q^N$, where the coefficients of the polynomial v are the integers in [−1, 1]. So, the signature (Lyubashevsky, 2012) can run correctly.

Theorem 1 The IBS scheme proposed in Section 3.2 satisfies correctness.

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

$$z_1 + hz_2 - H(\text{id})u = s_1u + y_1 + h(s_2u + y_2) - H(\text{id})u.$$

Since $s_1+s_2*h=H(\text{id})$, we have

$$\begin{aligned} &z_1 + h*z_2 - H(\text{id})u\\ &= s_1u + y_1 + h*(s_2u + y_2) - H(\text{id})u = y_1 + h*y_2. \end{aligned}$$

Hence, $H'(z_1 + h * z_2 - H(\mathrm{id})u, \mu) = u$.

By simply combining the rejection sampling technique described in Lemma 3, it is obvious that the distribution of z_i is very close to $D_{\mathbb{Z}^N,s}$. Therefore, by Lemma 2, we have $||z_i|| \le 2s\sqrt{N}$ with a probability of at least $1-2^{-N}$. Then, the inequality $||(z_1, z_2)|| \le 2s\sqrt{2N}$ is with an overwhelming probability.

4.2 Analysis of security

Theorem 2 The proposed IBS scheme is existentially unforgeable against adaptively chosen message and adaptively chosen identity attacks in the random oracle model, assuming the hardness of γ-SVP on the NTRU lattice against polynomial time algorithms on the NTRU lattice.

Proof Assuming there is an adversary A which can break the existentially unforgeable IBS scheme with nonnegligible probability $\varepsilon=\varepsilon(N)$, we can construct a polynomial-time challenger C that breaks γ-SVP on the NTRU lattice with a nonnegligible probability close to $\varepsilon=\varepsilon(N)$. The interactions between A and C are described as the following:

1. Set up: taking security parameter N as the input, challenger C randomly chooses a polynomial $h \in R_q^{\times}$ and two hash functions H and H'. Then C sends the public parameters pp=$\{h, H, H'\}$ to the adversary A.

2. Query: adversary A can adaptively query in the following ways. In general, we assume that adversary A has to query the random oracle H for id before it makes the other queries. We assume that A can make hash query H(id) and extract query for identity id only once.

(1) H hash function query (namely, id_i hash function query): at the beginning, C keeps a list of identity queries, ID-list, which is empty initially. For an identity id_i's query, C looks up the ID-list to find id_i. If id_i is found in the list, C provides the hash $H(\mathrm{id}_i)$ corresponding to A. Otherwise, id_i is fresh, and C picks uniformly random $s_{i1}, s_{i2} \in D_{\mathbb{Z}^N,s}$. Then C computes the polynomial $P_{\mathrm{id}_i} = s_{i1} + h * s_{i2}$ and stores (id_i, P_{id_i}, $\mathrm{sk}_{\mathrm{id}_i}=(s_{i1}, s_{i2})$) in the ID-list. Finally, C sends P_{id_i} to A as the response to id_i.

(2) Extract query: given id_i, C looks up the ID-list to find $\mathrm{sk}_{\mathrm{id}_i}$ corresponding to id_i, and sends $\mathrm{sk}_{\mathrm{id}_i}$ to A.

(3) Signature query: to obtain the signature of message $\mu_j \in \{0, 1\}^*$ by the user id_i, A sends (id_i, μ_j) to C. After receiving the query, C looks up the ID-list for $\mathrm{sk}_{\mathrm{id}_i}$ and chooses $y_{j1}, y_{j2} \leftarrow D_{\mathbb{Z}^N,s}$. Then C runs Algorithm 6. Finally, C sends ((z_{j1}, z_{j2}), u_j)= Signature(id_j, μ_j) to A and stores (μ_j, id_i, (y_{j1}, y_{j2}), $\mathrm{sk}_{\mathrm{id}_i}$, u_j, (z_{j1}, z_{j2})) in a list of signature queries, SIGN-list.

(4) H' hash function query: when A sends μ_j to C for H' hash query, C finds the corresponding μ_j in the SIGN-list and sends it to A.

3. Forgery: after finishing the queries listed above, A outputs a forgery $((z'_{j^*1}, z'_{j^*2}), u'_{j^*})$ for $(\mathrm{id}_i, \mu_{j^*})$ with a nonnegligible probability.

Now, without loss of generality, assume that before outputting the attempted forgery signature $((z'_{j^*1}, z'_{j^*2}), u'_{j^*})$, A has made a signature query for $(\mathrm{id}_i, \mu_{j^*})$, where $i \neq j^*$.

Thus, C can solve the SIS on the NTRU lattice as follows:

1. C obtains $\mathrm{sk}_{\mathrm{id}_i}$ and $u'_{j^*}, (y_{j^*1}, y_{j^*2})$ from the SIGN-list.

2. So, $z_{j^*1} = s_{i1} * u_{j^*} + y_{j^*1}$, $z_{j^*2} = s_{i2} * u_{j^*} + y_{j^*2}$, and $z_{j^*1} + z_{j^*2} * h - H(\mathrm{id}_i)u_{j^*}$ are computed by C. Then C checks whether

$$z'_{j^*1} + z'_{j^*2} * h - H(\mathrm{id}_i)u_{j^*} = z_{j^*1} + z_{j^*2} * h - H(\mathrm{id}_i)u_{j^*} = y_{j^*1} + h * y_{j^*2}.$$

Otherwise, there is a collision of hash function H'.

3. If the inequality $(z_{j^*1}, z_{j^*2}) \neq (z'_{j^*1}, z'_{j^*2})$ holds, $(z_{j^*1} - z'_{j^*1}, z_{j^*2} - z'_{j^*2})$ is one solution to SIS on the NTRU lattice.

We analyze the advantage of C in the following. As discussed above, C wins the game if and only if (1) A has successfully given a forgery $((z'_{j^*1}, z'_{j^*2}), u'_{j^*})$ and (2) $(z_{j^*1}, z_{j^*2}) \neq (z'_{j^*1}, z'_{j^*2})$.

Combining Lemma 1 and Property 4 of

Collision-Resistant preimage sampleable functions (Lyubashevsky, 2012), the probability that C can solve the SIS on the NTRU lattice is at least $(1-2^{-\omega(\log N)})\varepsilon$. Using the choice of $\beta = 4s\sqrt{2N}$, we obtain a polynomial time algorithm for γ-SVP on the NTRU lattice with $\gamma=\beta/\lambda_1(\Lambda_{h,q})$, where $\lambda_1(\Lambda_{h,q})$ is the shortest vector of lattice $\Lambda_{h,q}$.

4.3 Efficiency

As known, the efficient lattice-based IBS schemes are those that are secure in the random oracle model, e.g., the IBS schemes proposed by Rückert (2010) and Tian and Huang (2014), respectively.

Table 1 lists the comparison on the communication overhead of the three schemes for the same parameter N. Here, c is the bit length of all identities in the Rückert scheme; λ and k are positive integers; m is an integer, $m>5N\log q$, $\overline{s}=\hat{s}\sqrt{(c+1)m}\omega(\sqrt{\log N})$, $s=N^{5/2}\sqrt{2q}\omega(\sqrt{\log N})$, $\hat{s}=\sqrt{m}\omega(\sqrt{\log N})$, $\hat{\sigma}=12s\lambda m$, $\sigma=12\lambda\hat{s}N$. One can easily find that the signing key size and the signature length of Tian and Huang (2014) are considerably smaller than those of Rückert (2010). Thus, we compare only the concrete instances between the scheme of Tian and Huang (2014) and the new scheme in Table 2, to prove that the new scheme has the shortest signing key and signature size.

In terms of computation complexity, the signing and verification algorithm of the new scheme and the IBS in Tian and Huang (2014) are more efficient because they take only matrix-vector multiplication, integer addition, and hash operations, whereas Rückert (2010)'s scheme needs to run the more complicated presample algorithm.

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

5 Conclusions

With the development of quantum computers, constructing a quantum-secure efficient IBS scheme has become a priority. Lattice is one of the existing quantum-secure cryptographic primitive. However, the existing lattice-based IBS scheme is not entirely satisfactory. We have presented an efficient IBS scheme based on the hardness of the γ-SVP on the NTRU lattice. The proposed scheme is existentially unforgeable in the random oracle model. Moreover, the new IBS scheme is more efficient than other lattice-based IBS schemes.

We intend to investigate the construction of an efficient lattice (hierarchical) IBS scheme, which is strongly existentially unforgeable under adaptively chosen identity and adaptively chosen message attacks in the standard model, in our future work.

Table 1 Comparison of the communication overhead among several lattice-based IBS schemes

Scheme	Signing key size (bit)	Signature size (bit)
Rückert (2010)	$(m(c+1))^2\log(\overline{s}\sqrt{(c+1)m})$	$m(c+1)\log(\overline{s}\sqrt{(c+1)m})+N$
Tian *et al.* (2014)	$mk\log(\hat{s}\sqrt{m})$	$m\log(12\hat{\sigma})+k(\log\lambda+1)$
This work	$2N\log(s\sqrt{N})$	$2N\log(12\sigma)+N(\log\lambda+1)$

N: security parameter; c: bit length of all identities in Rückert (2010)'s scheme; m: an integer larger than $5N\log q$

Table 2 Comparison of the concrete instances

Instance	N	q	k	λ	Approximate private key size (bit)		Approximate signature size (bit)	
					Tian *et al.* (2014)	New scheme	Tian *et al.* (2014)	New scheme
1	512	227	80	28	97 662 557	38 999	2 604 731	54 237
2	512	225	512	14	575 102 845	37 975	2 339 160	51 677
3	512	233	512	14	776 460 530	42 071	805 029 461	55 773
4	512	218	512	14	402 892 589	34 391	1 652 126	48 093
5	512	226	512	14	600 035 269	38 487	2 438 277	52 189

References

Babai, L., 1986. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, **6**(1):1-13. http://dx.doi.org/10.1007/BF02579403

Barreto, P.S.L.M., Libert, B., McCullagh, N., *et al.*, 2005. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. 11th Int. Conf. on the Theory and Application of Cryptology and Information Security, p.515-532. http://dx.doi.org/10.1007/11593447_28

Bernstein, D.J., 2009. Introduction to post-quantum cryptography. *In*: Bernstein, D.J., Buchmann, J., Dahmen, E. (Eds.), Post-Quantum Cryptography. Springer-Verlag, Berlin, p.1-14. http://dx.doi.org/10.1007/978-3-540-88702-7_1

Boneh, D., Franklin, M., 2001. Identity based encryption from the Weil pairing. 21st Annual Int. Cryptology Conf., p.213-229. http://dx.doi.org/10.1007/3-540-44647-8_13

Desmedt, Y., Quisquater, J.J., 1987. Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?). *LNCS*, **263**:111-117. http://dx.doi.org/10.1007/3-540-47721-7_9

Ducas, L., Lyubashevsky, V., Prest, T., 2014. Efficient identity-based encryption over NTRU lattice. 20th Int. Conf. on the Theory and Application of Cryptology and Information Security, p.22-41. http://dx.doi.org/10.1007/978-3-662-45608-8_2

Gentry, C., Peikert, C., Vaikuntanathan, V., 2008. Trapdoors for hard lattices and new cryptographic constructions. 40th Annual ACM Symp. on Theory of Computing, p.197-206. http://dx.doi.org/10.1145/1374376.1374407

Hess, F., 2003. Efficient identity based signature schemes based on pairings. 9th Annual Int. Workshop on Selected Areas in Cryptography, p.310-324. http://dx.doi.org/10.1007/3-540-36492-7_20

Krenn, M., Huber, M., Fickler, R., *et al.*, 2014. Generation and confirmation of a (100×100)-dimensional entangled quantum system. *PNAS*, **111**(17):6243-6247. http://dx.doi.org/10.1073/pnas.1402365111

Li, F.G., Muhaya, F.T.B., Khan, M.K., *et al.*, 2012. Lattice-based signcryption. *Concurr. Comput. Pract. Exp.*, **25**(14):2112-2122. http://dx.doi.org/10.1002/cpe.2826

Liu, Z.H., Hu, Y.P., Zhang, X.S., *et al.*, 2013. Efficient and strongly unforgeable identity-based signature scheme from lattices in the standard model. *Secur. Commun. Network.*, **6**(1):69-77. http://dx.doi.org/10.1002/sec.531

Lyubashevsky, V., 2012. Lattice signatures without trapdoors. 31st Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques, p.738-755. http://dx.doi.org/10.1007/978-3-642-29011-4_43

Maurer, U.M., Yacobi, Y., 1991. Non-interactive public-key cryptography. Workshop on the Theory and Application of Cryptographic Techniques, p.498-507. http://dx.doi.org/10.1007/3-540-46416-6_43

Micciancio, D., Regev, O., 2009. Lattice-based cryptography. *In*: Bernstein, D.J., Buchmann, J., Dahmen, E. (Eds.), Post-Quantum Cryptography. Springer-Verlag, Berlin, p.147-191. http://dx.doi.org/10.1007/978-3-540-88702-7_5

Nguyen, P.Q., Regev, O., 2006. Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures. 24th Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques, p.271-288. http://dx.doi.org/10.1007/11761679_17

Paterson, K.G., Schuldt, J.C.N., 2006. Efficient identity-based signatures secure in the standard model. 11th Australasian Conf. on Information Security and Privacy, p.207-222. http://dx.doi.org/10.1007/11780656_18

Rückert, M., 2010. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles. Proc. 3rd Int. Workshop on PQCrypto, p.182-200. http://dx.doi.org/10.1007/978-3-642-12929-2_14

Shamir, A., 1984. Identity-based cryptosystems and signature schemes. Proc. CRYPTO, p.47-53. http://dx.doi.org/10.1007/3-540-39568-7_5

Shor, P.W., 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, **26**(5):1484-1509. http://dx.doi.org/10.1137/S0097539795293172

Stehlé, D., Steinfeld, R., 2013. Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices. Cryptology ePrint Archive 2013/004. Available from http://eprint.iacr.org/2013/004.

Tanaka, H., 1987. A realization scheme for the identity-based cryptosystem. CRYPTO, p.341-349. http://dx.doi.org/10.1007/3-540-48184-2_29

Tian, M.M., Huang, L.S., 2014. Efficient identity-based signature from lattices. Proc. 29th IFIP TC 11 Int. Conf., p.321-329. http://dx.doi.org/10.1007/978-3-642-55415-5_26

Tian, M.M., Huang, L.S., Yang, W., 2013. Efficient hierachical identity-based signatures from lattices. *Int. J. Electron. Secur. Dig. Forens.*, **5**(1):1-10. http://dx.doi.org/10.1504/IJESDF.2013.054403

Tsuji, S., Itoh, T., 1989. An ID-based cryptosystem based on the discrete logarithm problem. *IEEE J. Sel. Areas Commun.*, **7**(4):467-473. http://dx.doi.org/10.1109/49.17709