

Jia Xie, Yu-pu Hu, Jun-tao Gao, Wen Gao, 2016. Efficient identity-based signature over NTRU lattice. *Frontiers of Information Technology and Electronic Engineering*, 17(2):135-142. <http://dx.doi.org/10.1631/FITEE.1500197>

Efficient identity-based signature over NTRU lattice

Key words: Identity, Signature, Lattice, Number theory
research unit (NTRU lattice)

Contact: Jia Xie

E-mail: xiejia199325@163.com

 ORCID: <http://orcid.org/0000-0002-0894-0369>

Introduction

- 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.
- To improve the signing efficiency and decrease the size of the public key, the identity-based signature over NTRU lattice may be a good attempt by implying rejection sampling technique.
- An efficient identity-based signature over NTRU lattice has been presented in this work.

The IBS over NTRU lattice (I) / master keygen

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 $(f, g), (xf, xg), \dots, (x^{n-1}f, x^{n-1}g)$. 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** $\text{msk} = B = \begin{pmatrix} C(f) & C(g) \\ C(F) & C(G) \end{pmatrix}$ and the master public

key $\text{mpk} = h = g/f \in R_q^\times$

The IBS over NTRU lattice (II) / Extract, Signature, and Verification

Algorithm 5 Extract(B , id)

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

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

Output: $sk_{id} = (s_1, s_2)$

1 if sk_{id} in local storage then

2 return sk_{id} to user id

3 else

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

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

6 $sk_{id} \leftarrow (s_1, s_2)$

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 $H' : \{0,1\}^* \rightarrow \{v \in \{-1, 0, 1\}^N, \|v\|_1 \leq \lambda\}$

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 $\min\left(\frac{D_{\mathbb{Z}^N, s}}{MD_{\mathbb{Z}^N, s, sk_{id} u}}, 1\right)$,

where $M = O(1)$

Algorithm 7 Verification($id, \mu, (z_1, z_2, u)$)

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

Output: 1 or 0

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

2 return 1

3 else

4 return 0

5 end if

The comparison of communication overhead

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

Scheme	Signing key size (bit)	Signature size (bit)
Rückert (2010)	$(m(c+1))^2 \log(\bar{s}\sqrt{(c+1)m})$	$m(c+1) \log(\bar{s}\sqrt{(c+1)m}) + N$
Tian <i>et al.</i> (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 $5N \log q$

The comparison of the concrete instances

Table 2 Comparison of the concrete instances

Instance	N	q	k	λ	Approximate private key size (bit)		Approximate signature size (bit)	
					Tian <i>et al.</i> (2014)	New scheme	Tian <i>et al.</i> (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

Conclusions

- The proposed identity-based signature over NTRU lattice is proven secure even in quantum era.
- The proposed identity-based signature over NTRU lattice is proven more efficient than the other lattice-based IBS and has smaller size of public key.