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

# Novel efficient identity-based signature on lattices*

Jiang-shan CHEN†‡[1,2], Yu-pu HU[1], Hong-mei LIANG[2], Wen GAO[3]

[1]*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China*

[2]*School of Mathematics and Statistics, Minnan Normal University, Zhangzhou 363000, China*

[3]*School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710061, China*

†E-mail: JSChen@mnnu.edu.cn

Received June 27, 2019; Revision accepted Nov. 14, 2019; Crosschecked May 28, 2020; Published online July 2, 2020

**Abstract:** With the rapid development of electronic information technology, digital signature has become an indispensable part of our lives. Traditional public key certificate cryptosystems cannot overcome the limitations of certificate management. Identity-based cryptosystems can avoid the certificate management issues. The development of quantum computers has brought serious challenges to traditional cryptography. Post-quantum cryptography research is imperative. At present, almost all post-quantum identity-based signature (IBS) schemes are constructed using Gaussian sampling or trapdoor technologies. However, these two technologies have a great impact on computational efficiency. To overcome this problem, we construct an IBS scheme on lattices by employing Lyubashevsky's signature scheme. Based on the shortest vector problem on lattices, our scheme does not use Gaussian sampling or trapdoor technologies. In the random oracle model, it is proved that our scheme is strongly unforgeable against adaptive chosen messages and identity attacks. The security level of our scheme is strongly unforgeable, which is a higher level than the existential unforgeability of other schemes. Compared with other efficient schemes, our scheme has advantages in computation complexity and security.

**Key words:** Identity-based signature; Lattice; Strong unforgeability; Random oracle model
https://doi.org/10.1631/FITEE.1900318 **CLC number:** TN918.4

## 1 Introduction

With the development of information technology, artificial intelligence is becoming ever more pervasive in almost all aspects of our lives, such as e-commerce, Internet of Things, cloud services, smart devices, and unmanned aerial vehicles (Karam et al., 2012; Al Sharif et al., 2016; Al-Sharif et al., 2016; Hamdi et al., 2016; Baker et al., 2019; Iqbal et al., 2019). However, there are different levels of security issues in these areas. The core of these security issues is ultimately cryptographic. With the development of quantum computers, traditional cryptography has been greatly challenged and impacted. There is a lot of research on post-quantum cryptography. Lattice-based cryptography is one of the popular post-quantum cryptographies, and has attracted a lot of attention.

The identity-based signature (IBS) was first proposed by Shamir (1985). Identity-based cryptosystems are alternatives to traditional certificate-based cryptosystems. In an identity-based cryptosystem, user's private key is generated by the private key generator (PKG), and the public key is the user's public information (such as identity and email). Because public keys do not require authentication, the use of identity-based cryptosystems is becoming widespread. IBS is one of the important applications.

Since it was first proposed by Shamir (1985),

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (Nos. 61672412 and 61972457), the National Cryptography Development Fund of China (No. MMJJ20170104), and the Young and Middle-Aged Teacher Education Research Project of Fujian Province, China (Nos. JT180308 and JAT190372)

ORCID: Jiang-shan CHEN, https://orcid.org/0000-0002-2469-1307

several IBS schemes have been proposed (Fiat and Shamir, 1987; Choon and Cheon, 2002; Hess, 2003; Barreto et al., 2005; Paterson and Schuldt, 2006). They almost all work under the hardness assumptions of the algebraic number theory. With the development of quantum computers, they become insecure. There is an increasing amount of research on post-quantum cryptography to protect against quantum algorithm attacks. The aforementioned lattice system performs well against quantum algorithm attacks, and is a research hotspot.

Rückert (2010) first proposed two IBS schemes based on lattices in the random oracle model and standard model. Then, several lattice-based IBS schemes have been constructed. Gu et al. (2012) proposed an IBS scheme and an identity-based blind signature scheme based on lattices. These schemes are existentially unforgeable based on the hardness of the small integer solution (SIS) problem of lattices in the random oracle model. Liu et al. (2013) proposed an IBS scheme and a hierarchical IBS (HIBS) scheme based on the SIS problem in the standard model. Tian et al. (2013) proposed an HIBS scheme based on the SIS problem in the random oracle model. Tian and Huang (2014) presented a lattice-based IBS scheme based on the SIS problem in the random oracle model. Xie et al. (2016) proposed an IBS scheme based on number theory research unit (NTRU) lattice in the random oracle model. Among these schemes, Tian and Huang (2014)'s and Xie et al. (2016)'s schemes are relatively efficient. In addition, because of the advantages of identity-based cryptosystems, several signature schemes (Wei et al., 2014; Gao et al., 2017a, 2017b; Zhang et al., 2018a, 2018b; Zhao and Tian, 2018) with special properties have been proposed.

Lyubashevsky (2009) constructed a signature scheme based on the hardness of finding the approximate shortest vector within a factor of $\tilde{O}(n^2)$ in the random oracle model. Inspired by Lyubashevsky (2009), we construct a novel IBS scheme based on lattices. The main contributions of our scheme are as follows:

1. By employing Lyubashevsky's scheme twice, we construct an IBS scheme based on the hardness of finding the approximate shortest vector problem.

2. Our scheme does not use Gaussian sampling or trapdoor technologies, which would take up much computing resource.

3. In the random oracle model, it is proved that our scheme is strongly unforgeable against adaptive chosen message and identity.

Compared with other schemes, our scheme has advantages of low computation complexity and high security.

## 2 Preliminaries

Notations used in this paper are listed in Table 1.

**Table 1 Symbol description**

| Notation | Description |
|---|---|
| $\mathbb{R}(\mathbb{Z})$ | Set of real numbers (integers) |
| $p$ | A prime such that $p=3 \bmod 8$ |
| $n$ | A power of 2 |
| $m$ and $d$ | Integers |
| $\mathbb{Z}_p$ | Quotient ring $\mathbb{Z}/p\mathbb{Z}$ |
| $x^n+1$ | Irreducible polynomial |
| Letter with tilde, such as $\tilde{a}$ and $\tilde{Y}$ | Polynomial |
| Bold and italics lowercase letter with hat, such as $\hat{\boldsymbol{a}}$ | Vector of polynomial |
| $R$ | Ring $\mathbb{Z}_p[x]/\langle x^n+1\rangle$ |
| $D$ | Subset of $R$ |
| $\|\cdot\|_\infty$ | Infinity norm $\ell_\infty$ |
| $\mathcal{H}$ | Function family |
| $H$ | Hash function |
| $\mu$ | Message |

### 2.1 Lattices

**Definition 1** (Lattice) Let $\boldsymbol{B}\in\mathbb{R}^{n\times m}$ be a matrix constructed by $m$ linearly independent vectors $\{\boldsymbol{b}_1,\boldsymbol{b}_2,...,\boldsymbol{b}_m\}$. The lattice $\mathcal{L}$ generated by $\boldsymbol{B}$ is defined as

$$\mathcal{L}(\boldsymbol{B})=\{\boldsymbol{Bx}:\boldsymbol{x}\in\mathbb{Z}^m\}.$$

Let $\Lambda$ be an $(x^n+1)$-cyclic lattice (Micciancio, 2007) such that if any vector $(a_1,a_2,\ldots,a_n)\in\Lambda$, then the vector $(a_n,a_1,a_2,\ldots,a_{n-1})$ also in $\Lambda$.

**Definition 2** ($\mathrm{SVP}_\gamma(\Lambda)$ problem) Given a lattice $\Lambda$ and a rational number $\gamma\geq 1$, the goal of the $\mathrm{SVP}_\gamma(\Lambda)$ problem is to find a vector $\boldsymbol{v}$ such that $\|\boldsymbol{v}\|_\infty\leq\gamma\lambda_1(\Lambda)$, where $\lambda_1(\Lambda)$ is the smallest $\ell_\infty$ norm of any vector in $\Lambda$.

### 2.2 Lattice-based collision-resistant hash function

Let $n$ be any power of 2 and $R$ be the ring $\mathbb{Z}_p[x]/\langle x^n+1\rangle$. Now, we review the definition of

the hash function family (Lyubashevsky, 2009).

**Definition 3** (Family of hash functions) For $D \subset R$ and any integer $m$, $\mathcal{H}(R, D, m) = \{h_{\hat{\boldsymbol{a}}} : h_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{z}}) = \hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{z}}, \hat{\boldsymbol{a}} \in R^m, \hat{\boldsymbol{z}} \in D^m\}$ is the hash function family, where all operations are executed in the ring $\mathbb{Z}_p[x]/\langle x^n + 1\rangle$.

Given an element $h \in \mathcal{H}(R, D, m)$, for any $\hat{\boldsymbol{y}}, \hat{\boldsymbol{z}} \in R^m$ and $\tilde{c} \in R$, two equations, i.e., $h(\hat{\boldsymbol{y}} + \hat{\boldsymbol{z}}) = h(\hat{\boldsymbol{y}}) + h(\hat{\boldsymbol{z}})$ and $h(\hat{\boldsymbol{y}}\tilde{c}) = h(\hat{\boldsymbol{y}})\tilde{c}$, hold.

**Definition 4** (Collision problem Col$(h, D)$) Given $D \subset R$ and an element $h \in \mathcal{H}(R, D, m)$, the goal of Col$(h, D)$ is to find two distinct vectors $\hat{\boldsymbol{z}}_1, \hat{\boldsymbol{z}}_2 \in D^m$ such that $h(\hat{\boldsymbol{z}}_1) = h(\hat{\boldsymbol{z}}_2)$.

It was shown in Lyubashevsky and Micciancio (2006) that Col$(h, D)$ is as hard as SVP$_\gamma$ for any $(x^n + 1)$-cyclic lattice. Define $D = \{\tilde{g} \in R : \|\tilde{g}\|_\infty \leq d\}$ for integer $d$. $\mathcal{H}(R, D, m)$ is defined such that $m > \dfrac{\log p}{\log 2d}$ and $p \geq 4dmn^{1.5} \log n$. We have the following theorem:

**Theorem 1** (Lyubashevsky, 2009) If there exists a polynomial time algorithm that can solve the Col$(h, D)$ problem for a random $h \in \mathcal{H}(R, D, m)$ with a non-negligible probability, then there exists a polynomial time algorithm that can solve SVP$_\gamma(\Lambda)$ for every $(x^n + 1)$-cyclic lattice $\Lambda$, where $\gamma = 16dmn \log^2 n$.

### 2.3 Security model

Unforgeability against strong adversaries of the IBS scheme is defined by the following game:

**Game** Adversary $\mathcal{A}$ interacts with challenger $\mathcal{C}$ as follows:

1. Setup

$\mathcal{C}$ runs the setup algorithm to obtain the system parameters (params), master public key (mpk), and master secret key (msk). Then, $\mathcal{C}$ sends params and mpk to $\mathcal{A}$ and keeps msk secret.

2. Queries

$\mathcal{A}$ can make the following three types of queries to $\mathcal{C}$:

(1) Hash query

$\mathcal{A}$ can request the hash value for any input. $\mathcal{C}$ returns the corresponding value.

(2) Extract query

$\mathcal{A}$ can request the private key for any identity ID. $\mathcal{C}$ returns the private key of identity ID.

(3) Sign query

$\mathcal{A}$ can request the signature for any input in the form of $(\mathrm{ID}, \mu)$, where $\mu$ is a message. $\mathcal{C}$ returns a valid signature corresponding to $(\mathrm{ID}, \mu)$.

3. Forgery

$\mathcal{A}$ outputs a signature sig$^*$ on the message $\mu^*$ with regard to the identity ID$^*$. $\mathcal{A}$ wins the game if and only if (1) verify(params, sig$^*$, $\mu^*$, ID$^*$)=1, (2) ID$^*$ is never requested in extract query, and (3) (sig$^*$, $\mu^*$) is not returned by sign query.

**Definition 5** (Strong unforgeability) An IBS scheme is strongly unforgeable if the success probability of any polynomially bounded adversary in the above game is negligible.

## 3 Identity-based signature scheme based on lattices

In this section, we describe the IBS scheme and analyze its correctness, security, and efficiency.

### 3.1 Construction

Our IBS scheme without trapdoors works as follows:

1. Setup$(n)$

Given a security parameter $n$ as a power of 2, set $m = \log n$, $d = mn^{1.5} \log n$, and $p$ as a prime larger than $4d^2$ such that $p = 3 \bmod 8$. It is easy to verify that $m > \dfrac{\log p}{\log 2d}$ and $p \geq 4dmn^{1.5} \log n$ when $n > 4$. Then, these parameters define the sets of $R = \mathbb{Z}_p[x]/\langle x^n + 1\rangle$, $D = \{\tilde{g} \in R : \|\tilde{g}\|_\infty \leq d\}$, $D_h = \{\tilde{g} \in R : \|\tilde{g}\|_\infty \leq 1\}$, $D_s = \{\tilde{g} \in R : \|\tilde{g}\|_\infty \leq n^{0.5} \log n\}$, and $D_z = \{\tilde{g} \in R : \|\tilde{g}\|_\infty \leq d - n^{0.5} \log n\}$, and the function family $\mathcal{H}(R, D, m)$. Pick a hash function $h$ randomly from the family $\mathcal{H}(R, D, m)$. Select a random oracle hash function $H : \{0, 1\}^* \to D_h$. Pick $\hat{\boldsymbol{s}}_0$ randomly from $D_s^m$ and compute $\tilde{S} = h(\hat{\boldsymbol{s}}_0)$.

Output PKG's secret key msk $= \hat{\boldsymbol{s}}_0$, PKG's public key mpk $= \tilde{S}$, and the public parameters params $= \{n, m, p, R, D, D_h, D_s, D_z, h, H\}$.

2. Extract(params, msk, ID)

Given params, msk, and identity ID $\in \{0, 1\}^*$, the calculation is as follows:

(1) Choose $\hat{\boldsymbol{r}}_{\mathrm{ID}} \xleftarrow{\$} D^m$ and compute $\tilde{Q}_{\mathrm{ID}} = h(\hat{\boldsymbol{r}}_{\mathrm{ID}})$;

(2) Calculate $\tilde{e} = H(\mathrm{ID}, \tilde{Q}_{\mathrm{ID}})$ and $\hat{\boldsymbol{s}}_{\mathrm{ID}} = \hat{\boldsymbol{s}}_0\tilde{e} + \hat{\boldsymbol{r}}_{\mathrm{ID}}$;

(3) If $\hat{\boldsymbol{s}}_{\mathrm{ID}} \notin D_z^m$, then go to step (1);

(4) Return $(\hat{\boldsymbol{s}}_{\mathrm{ID}}, \tilde{Q}_{\mathrm{ID}})$ to the user with identity ID, where $\hat{\boldsymbol{s}}_{\mathrm{ID}}$ is secret and $\tilde{Q}_{\mathrm{ID}}$ is public.

Users can verify the correctness of the secret key $\mathrm{sk}_{\mathrm{ID}} = \hat{\boldsymbol{s}}_{\mathrm{ID}}$ by checking if $\hat{\boldsymbol{s}}_{\mathrm{ID}} \in D_z^m$ and $h(\hat{\boldsymbol{s}}_{\mathrm{ID}}) = \tilde{S}\tilde{e} + \tilde{Q}_{\mathrm{ID}}$, where $\tilde{e} = H(\mathrm{ID}, \tilde{Q}_{\mathrm{ID}})$.

3. Sign(params, $\mathrm{sk}_{\mathrm{ID}}$, $\mu$)

Given params, message $\mu \in \{0,1\}^*$, and signing key $\mathrm{sk}_{\mathrm{ID}}$, the calculation is as follows:

(1) Choose $\hat{\boldsymbol{y}} \xleftarrow{\$} D_s^m$ and compute $\tilde{Y} = h(\hat{\boldsymbol{y}})$;

(2) Calculate $\tilde{c} = H(\mu, \tilde{Y}, \tilde{Q}_{\mathrm{ID}})$ and $\hat{\boldsymbol{z}} = \hat{\boldsymbol{y}}\tilde{c} + \hat{\boldsymbol{s}}_{\mathrm{ID}}$;

(3) If $\hat{\boldsymbol{z}} \notin D_z^m$, then go to step (1);

(4) Output the signature sig $= (\hat{\boldsymbol{z}}, \tilde{Y})$.

4. Verify(params, sig, $\mu$, ID)

Given params, signature sig $= (\hat{\boldsymbol{z}}, \tilde{Y})$, message $\mu$, and identity ID, the signature is accepted if and only if $\hat{\boldsymbol{z}} \in D_z^m$ and $h(\hat{\boldsymbol{z}}) = \tilde{Y}\tilde{c} + \tilde{S}\tilde{e} + \tilde{Q}_{\mathrm{ID}}$, where $\tilde{c} = H(\mu, \tilde{Y}, \tilde{Q}_{\mathrm{ID}})$ and $\tilde{e} = H(\mathrm{ID}, \tilde{Q}_{\mathrm{ID}})$.

### 3.2 Correctness

It is easy to verify the correctness of the signature by

$$\begin{aligned} h(\hat{\boldsymbol{z}}) &= h(\hat{\boldsymbol{y}}\tilde{c} + \hat{\boldsymbol{s}}_{\mathrm{ID}}) \\ &= h(\hat{\boldsymbol{y}}\tilde{c} + \hat{\boldsymbol{s}}_0\tilde{e} + \hat{\boldsymbol{r}}_{\mathrm{ID}}) \\ &= h(\hat{\boldsymbol{y}}\tilde{c}) + h(\hat{\boldsymbol{s}}_0\tilde{e}) + h(\hat{\boldsymbol{r}}_{\mathrm{ID}}) \\ &= h(\hat{\boldsymbol{y}})\tilde{c} + h(\hat{\boldsymbol{s}}_0)\tilde{e} + h(\hat{\boldsymbol{r}}_{\mathrm{ID}}) \\ &= \tilde{Y}\tilde{c} + \tilde{S}\tilde{e} + \tilde{Q}_{\mathrm{ID}}. \end{aligned}$$

### 3.3 Security

**Lemma 1** Suppose that there exists a polynomial time adversary $\mathcal{A}$ who can output a valid forgery of the proposed scheme with probability $\varepsilon$. By employing the power of $\mathcal{A}$, we can construct an algorithm $\mathcal{B}$ that obtains a solution to $\mathrm{Col}(h, D)$ with a probability of at least $\dfrac{1-\mathrm{e}^{-1}}{2t_{\mathrm{H}}}\varepsilon$, where e is the base of natural logarithm and $t_{\mathrm{H}}$ is the maximum number of hash queries by $\mathcal{A}$.

**Proof** Assume that there exits an adversary $\mathcal{A}$ that can output a valid forgery for our IBS scheme with non-negligible probability $\varepsilon$. Using $\mathcal{A}$, we construct a polynomial time algorithm $\mathcal{B}$ that outputs a solution to $\mathrm{Col}(h, D)$ with a non-negligible probability.

$\mathcal{B}$ runs the setup algorithm to generate params, mpk, and msk, and sends params and mpk to adversary $\mathcal{A}$. Then $\mathcal{B}$ simulates all oracles as follows:

1. Hash query

$\mathcal{B}$ maintains initial empty list $L_1$ in the form of $(\mathrm{ID}_i, \tilde{Q}_{\mathrm{ID}_i}, \tilde{e}_i)$ and $L_2$ in the form of $(\mu_i, \tilde{Y}_i, \tilde{Q}_{\mathrm{ID}_i}, \tilde{c}_i)$. When $\mathcal{A}$ makes a query on $(\mathrm{ID}_i, \tilde{Q}_{\mathrm{ID}_i})$, $\mathcal{B}$ checks the list $L_1$. If $(\mathrm{ID}_i, \tilde{Q}_{\mathrm{ID}_i}, \tilde{e}_i)$ exists, $\mathcal{B}$ returns $\tilde{e}_i$ to $\mathcal{A}$. Otherwise, $\mathcal{B}$ randomly chooses $\tilde{e}_i \in D_h$ and returns it to $\mathcal{A}$, and adds $(\mathrm{ID}_i, \tilde{Q}_{\mathrm{ID}_i}, \tilde{e}_i)$ to $L_1$. When $\mathcal{A}$ makes query on $(\mu_i, \tilde{Y}_i, \tilde{Q}_{\mathrm{ID}_i})$, $\mathcal{B}$ checks the list $L_2$. If $(\mu_i, \tilde{Y}_i, \tilde{Q}_{\mathrm{ID}_i}, \tilde{c}_i)$ exists, $\mathcal{B}$ returns $\tilde{c}_i$ to $\mathcal{A}$. Otherwise, $\mathcal{B}$ randomly chooses $\tilde{c}_i \in D_h$ and returns it to $\mathcal{A}$, and adds $(\mu_i, \tilde{Y}_i, \tilde{Q}_{\mathrm{ID}_i}, \tilde{c}_i)$ to $L_2$.

2. Extract query

$\mathcal{B}$ maintains an initial empty list $L_3$ in the form of $(\mathrm{ID}_i, \mathrm{sk}_{\mathrm{ID}_i}, \tilde{Q}_{\mathrm{ID}_i}, \tilde{e}_i)$. When $\mathcal{A}$ makes query on $(\mathrm{ID}_i, \mathrm{sk}_{\mathrm{ID}_i}, \tilde{Q}_{\mathrm{ID}_i})$, $\mathcal{B}$ checks the list $L_3$. If $(\mathrm{ID}_i, \mathrm{sk}_{\mathrm{ID}_i}, \tilde{Q}_{\mathrm{ID}_i}, \tilde{e}_i)$ exists, $\mathcal{B}$ returns $(\mathrm{sk}_{\mathrm{ID}_i}, \tilde{Q}_{\mathrm{ID}_i})$ to $\mathcal{A}$. Otherwise, $\mathcal{B}$ randomly chooses $\tilde{e}_i \in D_h$ and $\mathrm{sk}_{\mathrm{ID}_i} \in D_z^m$, computes $\tilde{Q}_{\mathrm{ID}_i} = h(\mathrm{sk}_{\mathrm{ID}_i}) - \mathrm{mpk}\tilde{e}_i$, returns $(\mathrm{sk}_{\mathrm{ID}_i}, \tilde{Q}_{\mathrm{ID}_i})$ to $\mathcal{A}$, and adds $(\mathrm{ID}_i, \tilde{Q}_{\mathrm{ID}_i}, \tilde{e}_i)$ to $L_1$ and $(\mathrm{ID}_i, \mathrm{sk}_{\mathrm{ID}_i}, \tilde{Q}_{\mathrm{ID}_i}, \tilde{e}_i)$ to $L_3$.

3. Sign query

$\mathcal{B}$ maintains an initial empty list $L_4$ in the form of $(\mathrm{ID}_i, \mu_i, \hat{\boldsymbol{z}}_i, \tilde{Y}_i, \tilde{c}_i)$. When $\mathcal{A}$ makes query on $(\mathrm{ID}_i, \mu_i)$, $\mathcal{B}$ checks the list $L_4$. If $(\mathrm{ID}_i, \mu_i, \hat{\boldsymbol{z}}_i, \tilde{Y}_i, \tilde{c}_i)$ exists, $\mathcal{B}$ returns $(\hat{\boldsymbol{z}}_i, \tilde{Y}_i)$ to $\mathcal{A}$. Otherwise, $\mathcal{B}$ checks the list $L_3$. If $(\mathrm{ID}_i, \mathrm{sk}_{\mathrm{ID}_i}, \tilde{Q}_{\mathrm{ID}_i}, \tilde{e}_i)$ does not exist, $\mathcal{B}$ makes query on $(\mathrm{ID}_i, \mathrm{sk}_{\mathrm{ID}_i}, \tilde{Q}_{\mathrm{ID}_i})$ by itself. $\mathcal{B}$ obtains the secret key $(\mathrm{sk}_{\mathrm{ID}_i}, \tilde{Q}_{\mathrm{ID}_i})$ of identity $\mathrm{ID}_i$. Then, $\mathcal{B}$ randomly selects $\hat{\boldsymbol{y}}_i \in D_s^m$ and $\tilde{c}_i \in D_h$, sets $\tilde{Y}_i = h(\hat{\boldsymbol{y}}_i)$ and $\hat{\boldsymbol{z}}_i = \hat{\boldsymbol{y}}_i\tilde{c}_i + \mathrm{sk}_{\mathrm{ID}_i}$, returns $(\mu_i, \hat{\boldsymbol{z}}_i, \tilde{Y}_i)$ to $\mathcal{A}$, and adds $(\mu_i, \tilde{Y}_i, \tilde{Q}_{\mathrm{ID}_i}, \tilde{c}_i)$ to $L_2$ and $(\mathrm{ID}_i, \mu_i, \hat{\boldsymbol{z}}_i, \tilde{Y}_i, \tilde{c}_i)$ to $L_4$.

**Forgery** $\mathcal{A}$ outputs a valid forgery $(\mu^*, \hat{\boldsymbol{z}}_1^*, \tilde{Y}^*, \tilde{Q}_{\mathrm{ID}^*}, \tilde{e}_1^*, \tilde{c}^*)$ about identity $\mathrm{ID}^*$ with non-negligible probability $\varepsilon$, where $(\mathrm{ID}_i, \mathrm{sk}_{\mathrm{ID}_i}, \tilde{Q}_{\mathrm{ID}_i})$ is never requested in extract query and $(\mu^*, \hat{\boldsymbol{z}}_1^*, \tilde{Y}^*)$ is not returned by sign query. According to the forking lemma in Pointcheval and Stern (2000), $\mathcal{A}$ can output two valid forgeries $(\mu^*, \hat{\boldsymbol{z}}_1^*, \tilde{Y}^*, \tilde{Q}_{\mathrm{ID}^*}, \tilde{e}_1^*, \tilde{c}^*)$ and $(\mu^*, \hat{\boldsymbol{z}}_2^*, \tilde{Y}^*, \tilde{Q}_{\mathrm{ID}^*}, \tilde{e}_2^*, \tilde{c}^*)$ such that $\tilde{e}_1^* \neq \tilde{e}_2^*$ with probability $\varepsilon' \geq \dfrac{1-\mathrm{e}^{-1}}{t_{\mathrm{H}}}\varepsilon$.

In this case, $h(\hat{\boldsymbol{z}}_1^*) = \tilde{Y}^*\tilde{c}^* + \tilde{S}\tilde{e}_1^* + \tilde{Q}_{\mathrm{ID}^*}$ and $h(\hat{\boldsymbol{z}}_2^*) = \tilde{Y}^*\tilde{c}^* + \tilde{S}\tilde{e}_2^* + \tilde{Q}_{\mathrm{ID}^*}$. Thus, it is easy to obtain $h(\hat{\boldsymbol{z}}_1^* - \mathrm{msk}\tilde{e}_1^*) = h(\hat{\boldsymbol{z}}_2^* - \mathrm{msk}\tilde{e}_2^*)$, where $\hat{\boldsymbol{z}}_1^* - \mathrm{msk}\tilde{e}_1^* \neq \hat{\boldsymbol{z}}_2^* - \mathrm{msk}\tilde{e}_2^*$ with a probability of at least 0.5. Now, we have a collision for $h$ with probability $\varepsilon'/2 \geq \dfrac{1-\mathrm{e}^{-1}}{2t_{\mathrm{H}}}\varepsilon$.

According to Theorem 1 in Section 2.2 and

Lemma 1 in Section 3.3, we can obtain the following theorem:

**Theorem 2** Our IBS scheme is strongly unforgeable against adaptive chosen message and identity attacks in the random oracle model, assuming the hardness of $\mathrm{SVP}_\gamma(\Lambda)$ for every $(x^n+1)$-cyclic lattice $\Lambda$.

### 3.4 Efficiency

As far as we know, the most efficient IBS schemes on lattices in the random oracle model were proposed by Tian and Huang (2014) and Xie et al. (2016). The scheme in Xie et al. (2016) is based on NTRU lattices. The memory requirement of the scheme based on NTRU lattices is always lower than that based on a general lattice. Thus, the size of the scheme in Xie et al. (2016) is smaller than that of our scheme. The size of our scheme is smaller than that of the scheme proposed by Tian and Huang (2014). Comparison of the scheme size is shown in Table 2. Here, $n$ is a security parameter, $\lambda$, $k$, $m'$, and $m$ are positive integers, $p$ and $q$ are primes, $m' > 5n\log q$, $m = \log n$, $\hat{s} = n^{2.5}\sqrt{2q}\omega(\sqrt{n})$, $s = O(\sqrt{n\log q})\omega(\sqrt{\log n})$, $\hat{\sigma} = 12\lambda\hat{s}n$, $\sigma = 12s\lambda m'$, $d = m^2n^{1.5}$, and $p = 4d^2$. Table 3 shows the approximate sizes of the concrete instances.

However, the Gaussian sampling algorithm was employed in the extract algorithm of the scheme in Xie et al. (2016). In Tian and Huang (2014), not only the Gaussian sampling algorithm but also the trapdoor generation algorithm was employed. However, there is no sampling or trapdoor generation algorithm in our scheme. The computation complexity of our scheme is lower than those of other schemes. Furthermore, their schemes are existentially unforgeable against adaptive chosen message and identity attacks in the random oracle model. Our scheme is strongly unforgeable against adaptive chosen message and identity attacks in the random oracle model. Comparison of the computation complexity and security is shown in Table 4.

**Table 4 Comparison of the computation complexity and security**

| Scheme | Gaussian sampling | Trapdoor generation | Security |
|---|---|---|---|
| Xie et al. (2016)'s | Yes | Yes | EU-CMA |
| Tian and Huang (2014)'s | Yes | Yes | EU-CMA |
| Ours | No | No | SU-CMA |

Therefore, our scheme is not optimal in size, but has lower computation complexity and higher security.

## 4 Conclusions

By studying Lyubashevsky's scheme, we can know how the lattice-based signature scheme avoids using the sampling or trapdoor technique. Thus, we have constructed a new IBS scheme based on lattices. Our scheme does not use the sampling or trapdoor technique. This makes our scheme more computationally efficient than prior schemes. We have proved that our scheme is strongly unforgeable against adaptive chosen message and identity attacks in the random oracle model. Based on our scheme, other signature schemes with special properties can be constructed. At present, our identity-based blind signature scheme based on lattices is already under preparation.

**Table 2 Comparison of the scheme size**

| Scheme | Signing key size (bit) | Signature size (bit) |
|---|---|---|
| Xie et al. (2016)'s | $2n\log(\hat{s}\sqrt{n})$ | $2n\log(12\hat{\sigma})+n(\log\lambda+1)$ |
| Tian and Huang (2014)'s | $m'k\log(s\sqrt{m'})$ | $m'\log(12\sigma)+\lambda(\log k+1)$ |
| Ours | $mn\log(2d)+n\log p$ | $mn\log(2d)+n\log p$ |

**Table 3 Approximate sizes of the concrete instances**

| Instance | $n$ | $k$ | $\lambda$ | $q$ | $p$ | Signing key size (bit) | | Signature size (bit) | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Tian and Huang (2014) | This work | Tian and Huang (2014) | This work |
| 1 | 512 | 80 | 30 | $2^{27}$ | $2^{43}$ | 97 348 883 | 117 738 | 2 603 000 | 117 738 |
| 2 | 512 | 512 | 30 | $2^{25}$ | $2^{45}$ | 573 255 678 | 118 762 | 2 399 338 | 118 762 |
| 3 | 512 | 512 | 30 | $2^{33}$ | $2^{47}$ | 773 966 620 | 119 786 | 3 218 019 | 119 786 |

## Contributors

Jiang-shan CHEN designed the research. Jiang-shan CHEN and Hong-mei LIANG processed the data. Jiang-shan CHEN drafted the manuscript. Wen GAO helped organize the manuscript. Jiang-shan CHEN and Yu-pu HU revised and finalized the paper.

## Compliance with ethics guidelines

Jiang-shan CHEN, Yu-pu HU, Hong-mei LIANG, and Wen GAO declare that they have no conflict of interest.

## References


Al Sharif S, Al Ali M, Al Reqabi N, et al., 2016. Magec: an image searching tool for detecting forged images in forensic investigation. 8th IFIP Int Conf on New Technologies, Mobility and Security, p.1-6. https://doi.org/10.1109/NTMS.2016.7792460

Al-Sharif S, Iqbal F, Baker T, et al., 2016. White-hat hacking framework for promoting security awareness. 8th IFIP Int Conf on New Technologies, Mobility and Security, p.1-6. https://doi.org/10.1109/NTMS.2016.7792489

Baker T, Asim M, MacDermott Á, et al., 2019. A secure fog-based platform for SCADA-based IoT critical infrastructure. *Softw Pract Exp*, 50:503-518. https://doi.org/10.1002/spe.2688

Barreto PSLM, Libert B, McCullagh N, et al., 2005. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. Int Conf on Theory and Application of Cryptology and Information Security, p.515-532. https://doi.org/10.1007/11593447_28

Choon JC, Cheon JH, 2002. An identity-based signature from gap Diffie-Hellman groups. Int Workshop on Public Key Cryptography, p.18-30. https://doi.org/10.1007/3-540-36288-6_2

Fiat A, Shamir A, 1987. How to prove yourself: practical solutions to identification and signature problems. Conf on the Theory and Application of Cryptographic Techniques, p.186-194. https://doi.org/10.1007/3-540-47721-7_12

Gao W, Hu YP, Wang BC, et al., 2017a. Identity-based blind signature from lattices. *Wuhan Univ J Nat Sci*, 22(4):355-360. https://doi.org/10.1007/s11859-017-1258-x

Gao W, Hu YP, Wang BC, et al., 2017b. Identity-based blind signature from lattices in standard model. Int Conf on Information Security and Cryptology, p.205-218. https://doi.org/10.1007/978-3-319-54705-3_13

Gu CX, Chen L, Zheng YH, 2012. ID-based signatures from lattices in the random oracle model. Int Conf on Web Information Systems and Mining, p.222-230. https://doi.org/10.1007/978-3-642-33469-6_31

Hamdi D, Iqbal F, Baker T, et al., 2016. Multimedia file signature analysis for smartphone forensics. 9th Int Conf on Developments in eSystems Engineering, p.130-137. https://doi.org/10.1109/DeSE.2016.22

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

Iqbal F, Yankson B, AlYammahi MA, et al., 2019. Drone forensics: examination and analysis. *Int J Electron Secur Dig Forens*, 11(3):245-264. https://doi.org/10.1504/IJESDF.2019.10020543

Karam Y, Baker T, Taleb-Bendiab A, 2012. Security support for intention driven elastic cloud computing. 6th UKSim/AMSS European Symp on Computer Modeling and Simulation, p.67-73. https://doi.org/10.1109/EMS.2012.17

Liu ZH, Hu YP, Zhang XS, et al., 2013. Efficient and strongly unforgeable identity-based signature scheme from lattices in the standard model. *Secur Commun Netw*, 6(1):69-77. https://doi.org/10.1002/sec.531

Lyubashevsky V, 2009. Fiat-Shamir with aborts: applications to lattice and factoring-based signatures. Int Conf on the Theory and Application of Cryptology and Information Security, p.598-616. https://doi.org/10.1007/978-3-642-10366-7_35

Lyubashevsky V, Micciancio D, 2006. Generalized compact knapsacks are collision resistant. Int Colloquium on Automata, Languages, and Programming, p.144-155. https://doi.org/10.1007/11787006_13

Micciancio D, 2007. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Comput Compl*, 16(4):365-411. https://doi.org/10.1007/s00037-007-0234-9

Paterson KG, Schuldt JCN, 2006. Efficient identity-based signatures secure in the standard model. Australasian Conf on Information Security and Privacy, p.207-222. https://doi.org/10.1007/11780656_18

Pointcheval D, Stern J, 2000. Security arguments for digital signatures and blind signatures. *J Cryptol*, 13(3):361-396. https://doi.org/10.1007/s001450010003

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

Shamir A, 1985. Identity-based cryptosystems and signature schemes. Proc Advances in Cryptology, p.47-53. https://doi.org/10.1007/3-540-39568-7_5

Tian MM, Huang LS, 2014. Efficient identity-based signature from lattices. 29th ICT Systems Security and Privacy Protection, p.321-329. https://doi.org/10.1007/978-3-642-55415-5_26

Tian MM, Huang LS, Yang W, 2013. Efficient hierarchical identity-based signatures from lattices. *Int J Electron Secur Dig Forens*, 5(1):1-10. https://doi.org/10.1504/IJESDF.2013.054403

Wei BD, Du YS, Zhang H, et al., 2014. Identity based threshold ring signature from lattices. 8th Int Conf on Network and System Security, p.233-245. https://doi.org/10.1007/978-3-319-11698-3_18

Xie J, Hu YP, Gao JT, et al., 2016. Efficient identity-based signature over NTRU lattice. *Front Inform Technol Electron Eng*, 17(2):135-142. https://doi.org/10.1631/FITEE.1500197

Zhang YH, Gan Y, Yin YF, et al., 2018a. Efficient lattice FIBS for identities in a small universe. 1st Int Conf on Frontiers in Cyber Security, p.83-95. https://doi.org/10.1007/978-981-13-3095-7_7

Zhang YH, Gan Y, Yin YF, et al., 2018b. Fuzzy identity-based signature from lattices for identities in a large universe. Int Conf on Cloud Computing and Security, p.573-584.

Zhao GM, Tian MM, 2018. A simpler construction of identity-based ring signatures from lattices. 12th Int Conf on Provable Security, p.277-291. https://doi.org/10.1007/978-3-030-01446-9_16