

# Forward-Secure Identity-Based Shorter Blind Signature from Lattices

Yanhua Zhang<sup>\*</sup>, Yupu Hu

State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China

## Email address:

yhzhaxidian@163.com (Yanhua Zhang), yphu@mail.xidian.edu.cn (Yupu Hu)

<sup>\*</sup>Corresponding author

## To cite this article:

Yanhua Zhang, Yupu Hu. Forward-Secure Identity-Based Shorter Blind Signature from Lattices. *American Journal of Networks and Communications*. Vol. 5, No. 2, 2016, pp. 17-26. doi: 10.11648/j.ajnc.20160502.12

**Received:** March 27, 2016; **Accepted:** April 6, 2016; **Published:** April 19, 2016

---

**Abstract:** Blind signature (BS) plays one of key ingredients in electronic cash or electronic voting system. However, the key exposures bring out very serious problems in insecure mobile devices. Forward-secure blind signatures preserve the validity of past signatures and prevent a forger from forging past signatures even if current secret key has been compromised. In this paper, we propose the first forward-secure identity-based shorter blind signature scheme from lattices which can resist quantum attack, and prove that our scheme satisfies the security requirements of blindness, unforgeability, and forward secrecy in the random oracle model. Furthermore, we also extend our construction to a forward-secure identity-based shorter blind signature in the standard model.

**Keywords:** Forward-Secure, Blind Signature, Unforgeability, Lattice, Random Oracle Model

---

## 1. Introduction

Blind signature (BS) was first introduced by Chaum [1] to protect the privacy of an individual. In a BS scheme, a signer is requested to sign on a blinded message from a requester. It means the signer knowing nothing about the original message, the requester can unblind the signature to obtain a signature on the original message from the signer. Even the signature on the original message is opened later, the signer cannot link it with the actual signing process. Thus due to the property of strong blindness and untraceability, BS has several significant applications in areas such as electronic cash systems [2] and electronic voting systems [3], etc.

Identity-based signature (IBS) was first introduced by Shamir [4] to reduce the complexity for managing the public key infrastructure. In an IBS scheme, the identity of a signer is regarded as the public key. Then the key generation center (PKC) generates the secret key corresponding to that identity information.

As far as we know, the security of most BS depends on the assumption that the signing secret keys are absolutely secure. However, the key exposures seem more likely to occur in the real life such as the explosive use of mobile, the unprotected

devices. Once the signing secret keys are exposed, no matter the past or the future blind signatures will be compromised. Moreover the key exposures bring out more serious problems in electronic systems in which money is directly involved.

One of the most promising solutions to resolve the key exposure problems is forward-secure. And the concept of non interactive forward-secure was first introduced by Anderson [5] and further formalized by Bellare and Miner [6]. In the model of [6], the whole lifetime of the system is divided into  $N$  time periods labeled  $0, 1, \dots, N-1$ , and a different secret key is used in each time period while the public key remains the same. The initial signing secret key is  $SK_0$  and at the end of time period  $i$ , a new signing secret key  $SK_{i+1}$  is computed for the next time period  $i+1$  using the signing secret key  $SK_i$  and then  $SK_i$  is deleted.

Forward-secure blind signature (FSBS) was introduced by Duc et al. [7] to preserve the validity of past blind signatures and prevent a forger from forging past blind signatures even if current signing secret key has been compromised. A large number of FSBS schemes [8–12] have been proposed so far based on large integer factoring or discrete logarithms.

However, recent studies show that cryptographic schemes based on large integer factoring and discrete logarithms have

been unable to resist quantum attacks. And as one of the most promising candidates for post-quantum cryptography, lattice cryptography has attracted significant interest, due to several potential benefits: asymptotic efficiency, worst-case hardness assumptions, security against quantum computers. To design secure and efficient lattice-based cryptographic constructions are interesting and challenging. With the first signature and identity-based encryption schemes over lattice proved to be secure proposed by Gentry et al. [13], lattice cryptography enters into a rapid development period and large numbers of schemes are constructed, such as public key encryption (PKE) schemes [14–20], identity-based encryption (IBE) schemes [13, 21–27], fully homomorphic encryption schemes [28–32], signature schemes [33–36] and signature schemes with some particular characteristics [37–44].

In this paper, we propose the first forward-secure identity based shorter blind signature (FSIBBS) over lattice. Then, we prove that our construction satisfies security requirements of blindness, forward secrecy, and unforgeability in the random oracle model. Furthermore, we extend the above construction to be a FSIBBS scheme in the standard model

## 2. Preliminaries

### 2.1. Notation

In this paper, the set of real numbers (integers) is denoted by  $\mathbb{R}(\mathbb{Z})$ . The function  $\log$  denotes natural logarithm. Vectors are in column form and denoted by the bold lower-case letter (e.g.,  $\mathbf{x}$ ). The  $i$ -th component of  $\mathbf{x}$  will be denoted by  $x_i$ . We view a matrix as the set of its column vectors and denoted by the bold capital letter (e.g.,  $\mathbf{X}$ ). The Euclidean norm of  $\mathbf{x}$  is denoted as  $\|\mathbf{x}\|$ , and define the norm of  $\mathbf{X}$  as the norm of its longest column (i.e.,  $\|\mathbf{X}\| = \max_i \|\mathbf{x}_i\|$ ). The security parameter throughout this paper is  $n$ , and all other quantities are implicit function of  $n$ . Let  $\text{poly}(n)$  denote an unspecified function  $f(n) = O(n^c)$  for any  $c > 0$ . We use standard notation  $O, \omega$  to classify the growth of functions. If  $f(n) = O(g(n) \cdot \log^c n)$ , we denote it as  $f(n) = \tilde{O}(g(n))$ . And we use  $\text{negl}(n)$  to denote a negligible function  $f(n) = O(n^{-c})$  for  $c > 0$ , and a probability is overwhelming if it is  $1 - \text{negl}(n)$ .

### 2.2. Lattices

Let  $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m\} \in \mathbb{R}^{m \times m}$  be an  $m \times m$  matrix with a list of linearly independent vectors  $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m \in \mathbb{R}^m$ . The lattice  $\Lambda$  generated by  $\mathbf{B}$  is as follows:

$$\Lambda = \mathcal{L}(\mathbf{B}) = \{\mathbf{y} \in \mathbb{R}^m, s.t. \exists \mathbf{s} \in \mathbb{Z}^m, \mathbf{y} = \sum_{i=1}^m s_i \mathbf{b}_i\} \quad (1)$$

Here, we focus on integer lattices, i.e.,  $\mathcal{L}$  is contained in  $\mathbb{Z}^m$ .

**Definition 1** For a prime  $q$ , matrix  $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$  and a vector

$\mathbf{u}$  in  $\mathbb{Z}_q^n$ , define:

$$\Lambda_q(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m, s.t. \exists \mathbf{s} \in \mathbb{Z}_q^n, \mathbf{A}^T \mathbf{s} = \mathbf{e} \bmod q\} \quad (2)$$

$$\Lambda_q^u(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m, s.t. \mathbf{A}\mathbf{e} = \mathbf{u} \bmod q\} \quad (3)$$

$$\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m, s.t. \mathbf{A}\mathbf{e} = \mathbf{0} \bmod q\} \quad (4)$$

**Lemma 1** [45] Let a prime  $q \geq 3$  and  $m \geq 6n \log q$ . There is a probabilistic polynomial-time (PPT) algorithm  $\text{TrapGen}(q, n)$  that outputs two matrices  $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$  and  $\mathbf{T} \in \mathbb{Z}_q^{m \times m}$  such that  $\mathbf{A}$  is statistically close to a uniform matrix in  $\mathbb{Z}_q^{n \times m}$  and  $\mathbf{T}$  is a basis for  $\Lambda_q^\perp(\mathbf{A})$  satisfying  $\|\tilde{\mathbf{T}}\| \leq O(\sqrt{n \log q})$  and  $\|\mathbf{T}\| \leq O(n \log q)$  with all but a negligible probability in  $n$ .

### 2.3. Discrete Gaussian Distributions

For any  $s > 0$ , define the gaussian function on  $\mathbb{R}^m$ , centered at  $\mathbf{c}$  with parameter  $s$ :

$$\forall \mathbf{x} \in \mathbb{R}^m, \rho_{s, \mathbf{c}}(\mathbf{x}) = \exp(-\pi \|\mathbf{x} - \mathbf{c}\|^2 / s^2) \quad (5)$$

For any  $\mathbf{c} \in \mathbb{R}^m$ , real  $s > 0$ ,  $m$ -dimensional lattice  $\Lambda$ , define the discrete gaussian distribution over  $\Lambda$  as:

$$\forall \mathbf{x} \in \mathbb{R}^m, D_{\Lambda, s, \mathbf{c}}(\mathbf{x}) = \frac{\rho_{s, \mathbf{c}}(\mathbf{x})}{\rho_{s, \mathbf{c}}(\Lambda)} = \frac{\rho_{s, \mathbf{c}}(\mathbf{x})}{\sum_{\mathbf{x} \in \Lambda} \rho_{s, \mathbf{c}}(\mathbf{x})} \quad (6)$$

The subscripts  $s$  and  $\mathbf{c}$  are taken to be 1 and  $\mathbf{0}$  (respectively) when omitted.

**Lemma 2** [13] Assume that the columns of matrix  $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$  generate  $\mathbb{Z}_q^n$ , let  $\epsilon \in (0, 1/2)$ ,  $s \geq \eta_\epsilon(\Lambda^\perp(\mathbf{A}))$ . For  $\mathbf{e} \sim D_{\mathbb{Z}_q^m, s}$ , the distribution of syndrome  $\mathbf{u} = \mathbf{A} \cdot \mathbf{e} \bmod q$  is within statistical distance  $2\epsilon$  of uniform over  $\mathbb{Z}_q^n$ . Furthermore, fix  $\mathbf{u} \in \mathbb{Z}_q^n$  and let vector  $\mathbf{t} \in \mathbb{Z}^m$  be an arbitrary solution to  $\mathbf{A}\mathbf{t} = \mathbf{u} \bmod q$ . The conditional distribution of  $\mathbf{e} \sim D_{\mathbb{Z}_q^m, s}$  given  $\mathbf{A} \cdot \mathbf{e} = \mathbf{u} \bmod q$  is  $\mathbf{t} + D_{\Lambda^\perp, s, -\mathbf{t}}$ .

**Definition 2** [46] For any  $m$ -dimensional lattice  $\Lambda$  and real  $\epsilon > 0$ , the smoothing parameter  $\eta_\epsilon$  is the smallest real  $s > 0$  such that  $\rho_{1/s}(\Lambda^* \setminus \{0\}) \leq \epsilon$ .

**Lemma 3** [46] Let  $q > 2$ ,  $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$  and  $0 < \epsilon < 1$ . Let  $\mathbf{T}$  be a basis for  $\Lambda_q^\perp(\mathbf{A})$ ,  $s \geq \|\tilde{\mathbf{T}}\| \cdot \omega(\sqrt{\log m})$ . For  $\mathbf{c} \in \mathbb{R}^m, \mathbf{u} \in \mathbb{Z}_q^n$ :

$$1). \Pr_{\mathbf{x} \sim D_{\Lambda, s, \mathbf{c}}}[\|\mathbf{x} - \mathbf{c}\| > s\sqrt{m}] \leq \frac{1 + \epsilon}{1 - \epsilon} \cdot 2^{-m}.$$

2). There exists a PPT algorithm  $\text{SampleGau}(\mathbf{A}, \mathbf{T}, s, \mathbf{c})$  that returns  $\mathbf{x} \in \Lambda_q^\perp(\mathbf{A})$  drawn from a distribution

statistically close to  $D_{\Lambda_q^\perp(A),s,\epsilon}$ .

3). There exists a PPT algorithm  $\text{SamplePre}(A, T, u, s)$  that returns  $x \in \Lambda_q^\perp(A)$  sampled from a distribution statistically close to  $D_{\Lambda_q^\perp(A),s}$ .

#### 2.4. Useful Facts

In this subsection, we recall several useful facts on lattices in literatures.

**Lemma 4** [21] On input a matrix  $A \in \mathbb{Z}_q^{n \times m}$  and a gaussian parameter  $r > \|T\| \cdot \omega(\sqrt{\log n})$ . There exists a PPT algorithm  $\text{RandBasis}(A, T, r)$  that given a basis  $T$  of  $\Lambda_q^\perp(A)$ , outputs a short basis  $T' \in \mathbb{Z}_q^{n \times m}$  for  $\Lambda_q^\perp(A)$  such that  $\|T'\| \leq r\sqrt{m}$ , and no any information specific to  $T$  is leaked by  $T'$ .

Next, we describe the basis delegation technique proposed by Agrawal et al. [23].

**Lemma 5** Let  $q \geq 3, m > 2n \log q$ ,  $\sigma_R = \sqrt{n \log q} \omega(\sqrt{\log m})$ .  $D_{m \times m}$  denotes distribution on matrices in  $\mathbb{Z}^{m \times m}$  and is defined as  $(D_{\mathbb{Z}^m, \sigma_R})^m$  conditioned on the matrix being invertible. On input  $A \in \mathbb{Z}_q^{n \times m}$ , a invertible matrix  $R$  sampled from  $D_{m \times m}$  or a product of such, a parameter  $\sigma > \|\tilde{T}_A\| \cdot \sigma_R \sqrt{m} \cdot \omega(\log^{3/2} m)$ . There is a PPT algorithm  $\text{BasisDel}(A, R, T_A, \sigma)$  that given a short basis  $T_A$  of  $\Lambda_q^\perp(A)$ , outputs a short basis  $T_B$  for  $\Lambda_q^\perp(B)$ , satisfying  $\|\tilde{T}_B\| \leq \sigma_R / \omega(\sqrt{\log m})$ , where  $B = AR^{-1} \in \mathbb{Z}_q^{n \times m}$ .

#### 2.5. Hardness Assumption

The small integer solution (SIS) problem was suggested to be hard on average by Ajtai [47] and formally defined by Micciancio and Regev [46].

**Definition 3** The SIS problem in Euclidean norm is that given a prime  $q$ , a matrix  $A \in \mathbb{Z}_q^{n \times m}$  and real  $\beta$ , find a non-zero  $m$ -dimensional vector  $e \in \mathbb{Z}^m$  such that  $Ae = 0 \pmod q, \|e\| \leq \beta$ . The average-case  $\text{SIS}_{q,m,\beta}$  problem is defined similarly, where  $A$  is uniformly random.

The problem was shown to be as hard as certain worst-case lattice problems, first by Ajtai [47], then by Micciancio and Regev [46] and Gentry et al. [13].

**Lemma 4** [13] For poly-bounded  $m$ ,  $\beta = \text{poly}(n)$  and prime  $q \geq \beta \omega(\sqrt{n \log n})$ , the average-case  $\text{SIS}_{q,m,\beta}$  problem is as hard as approximating the shortest independent vector problem, among others, in worst-case to within  $\gamma = \beta \tilde{O}(\sqrt{n})$  factors.

### 3. Forward-Secure Identity-Based Blind Signature

We now formalize the definition and security requirements of forward-secure identity-based blind signature (FSIBBS) in Refs. [7, 48]. Here, the whole lifetime of the system is divided into  $N$  time periods labeled  $0, 1, \dots, N-1$ .

#### 3.1. Syntax of FSIBBS

A FSIBBS scheme consists of five algorithms, namely, Setup, Extract, Update, Sign and Verify. All are described as follows:

**FSIBBS-Setup:** A PPT algorithm takes security parameter  $n$  as input, and outputs a master secret key  $msk$  and a master public key  $mpk$  by the private key generator (PKG).

**FSIBBS-Extract:** A PPT algorithm takes  $msk, mpk$  and an identity  $id \in \{0, 1\}^*$  as inputs, and outputs the initial secret key  $sk_{id,0}$ , which is sent to the signer in a secure way.

**FSIBBS-Update:** A PPT algorithm takes  $mpk, msk$  and  $sk_{id,i}$  of the signer with identity  $id$  at the  $i$ -th time period as inputs and outputs a new signing secret key  $sk_{id,i+1}$  for the next time period  $i+1$ , then deletes  $sk_{id,i}$ .

**FSIBBS-Sign:** A PPT algorithm takes a secret key  $sk_{id,i}$  of a signer with identity  $id$  at the  $i$ -th time period and a message  $m$  as inputs,

a. *Blind:* Taking a message  $m$  which to be signed together with a blinding factor  $r$  as inputs, it outputs a blinded message  $M$  of  $m$ .

b. *Sign:* Taking the blinded message  $M$  as input, it outputs a signature  $sig'$  on  $M$ .

c. *Unblind:* Taking the signature  $sig'$  on a blinded message  $M$ , a blinding factor  $r$  as inputs, it outputs the final unblinded signature  $sig$  on  $m$ .

**FSIBBS-Verify:** A deterministic algorithm takes  $mpk$ , and a signer with identity  $id$ , a message  $m$  and a signature  $(i, sig)$  as inputs and outputs "accept" if  $(i, sig)$  is a valid signature or "reject", otherwise.

The correctness is that if  $sig$  is a valid signature generated by  $\text{FSIBBS-Sign}(id, m, i)$ , then we have

$$\text{FSIBBS-Verify}(id, m, i, sig) = \text{"accept"}.$$

#### 3.2. Security Requirements for FSIBBS

We give the security requirements for FSIBBS in [7, 49].

**Blindness:** Let  $S$  be a signer or any adversary that controls the signer and  $U_0, U_1$  be two honest users. A FSIBBS scheme is blind if a PPT dishonest  $S$  wins the following game with a negligible advantage:

a. The PKG generates the master secret key  $msk$ , the master public key  $mpk$ , and a initial signing secret key for  $S$ , whose identity is  $id$  and then  $S$  chooses two messages  $m_0$  and  $m_1$ .

b. The referee chooses a random bit  $b \in \{0,1\}$ , and then  $(m_b, id, mpk)$ ,  $(m_{1-b}, id, mpk)$  are given to  $U_0$ ,  $U_1$  respectively.

c.  $U_0$  and  $U_1$  engage with  $S$  to get signature on  $m_b$  and  $m_{1-b}$ , respectively (Note: not necessary in two different time periods since blindness property must be satisfied for all signatures, not just for signatures issued in one time period).

d.  $U_0$  and  $U_1$  output two valid blind signatures  $(m_b, id, sig_b)$ ,  $(m_{1-b}, id, sig_{1-b})$ , then these signatures are given to  $S$ .

e. Finally,  $S$  outputs a guess  $\tilde{b}$  for  $b$ , and  $S$  wins the game if  $\tilde{b} = b$ .

If the probability that  $S$  wins the above game is no better than the probability of guessing a random bit  $b$  (probability of  $1/2$ ),  $S$  cannot link a signature to its owner. We say that the blindness property is satisfied.

*Unforgeability:* Let  $\mathcal{A}$  be any PPT adversary and  $\mathcal{C}$  be a challenger. A FSIBBS scheme is unforgeable if  $\mathcal{A}$  wins the game with a negligible advantage:

*Setup phase:*  $\mathcal{C}$  runs algorithm FSIBBS-Setup to generate the master secret key  $msk$ , the master public key  $mpk$  and then sends  $mpk$  to  $\mathcal{A}$ .

*Queries phase:*  $\mathcal{A}$  is allowed to make poly-bounded queries as follows:

a. Key Ext query: On receiving a query for the initial signing secret key of a signer with identity  $id$ .  $\mathcal{C}$  returns  $sk_{id,0}$  to  $\mathcal{A}$ .

b. Signing secret key query: On receiving a query of  $(id, j)$ , where  $1 \leq j \leq N-1$ .  $\mathcal{C}$  returns  $sk_{id,j}$  to  $\mathcal{A}$ .

c. Signing query: On receiving a query of  $(id, i, M)$ , where  $1 \leq i \leq N-1$  and  $M$  is a blinded message of  $m$ . Using  $sk_{id,i}$  for the time period  $i$ ,  $\mathcal{C}$  returns  $sig'$  to  $\mathcal{A}$ .

*Forgery phase:* Finally, the adversary  $\mathcal{A}$  outputs a tuple of  $(id^*, i^*, m^*, sig^*)$ . Adversary  $\mathcal{A}$  is considered to be succeed if the following conditions hold:

- FSIBBS-Verify( $id^*, i^*, m^*, sig^*$ ) = "accept".
- $id^*$  has not been issued as a KeyExt query.
- $(id^*, i^*, M^*)$  has not been issued as a signing query, here  $M^*$  is a blinded message of  $m^*$ .

*Forward secrecy:* In the different cryptographic schemes, forward secrecy owns different meanings depending on the security goals for the schemes. In a blind signature context, forward secrecy means that unforgeability of signatures is valid in previous time periods even if current signing secret key of the signer is compromised.

## 4. A FSIBBS Scheme from Lattices

### 4.1. Description of the Scheme

Inspired by the basis delegation technique proposed by Agrawal et al. [23], we construct the first FSIBBS scheme

from lattices. The main steps of our construction are provided as follows:

*FSIBBS-Setup:* On inputting the security parameter  $n$ , a prime  $q \geq 3$ ,  $m \geq 6n \log q$ , and two collision-resistance hash functions  $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^{m \times m}$ , and  $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^n$ . For each time period, the PKG sets two series of gaussian parameters  $\sigma = (\sigma_0, \sigma_1, \dots, \sigma_{N-1})$ ,  $\delta = (\delta_0, \delta_1, \dots, \delta_{N-1})$ . Then, the PKG does as follows:

1). Using algorithm TrapGen( $q, n$ ), the PKG gets a matrix  $A \in \mathbb{Z}_q^{n \times m}$  together with a short basis  $T \in \mathbb{Z}_q^{m \times m}$  for  $\Lambda_q^\perp(A)$ .

2). The PKG outputs the master public key and the master secret key:  $mpk = A \in \mathbb{Z}_q^{n \times m}$ ,  $msk = T \in \mathbb{Z}_q^{m \times m}$ .

*FSIBBS-Extract:* On receiving the identity  $id$  of a signer, the PKG generates the initial signing secret key as follows:

- Let  $R_{id,0} = H_1(id, 0)$ , the PKG gets  $A_{id,0} = A \cdot R_{id,0}^{-1}$ .
- Using algorithm BasisDel( $A, R_{id,0}, T, \sigma_0$ ), the PKG can generate the initial signing secret key  $sk_{id,0} \in \mathbb{Z}_q^{m \times m}$ , and then sends it to the signer in a secure way.

*FSIBBS-Update:* On inputting  $(id, i, sk_{id,i-1})$ , where  $i$  is the current time period,  $sk_{id,i-1}$  is the signing secret key associated with previous time period  $i-1$ . A signer with the identity  $id$  does as follows:

- Let  $R_{id,i-1} = H_1(id, i-1) \cdot H_1(id, i-2) \cdots H_1(id, 0) \in \mathbb{Z}_q^{m \times m}$  and  $A_{id,i-1} = A \cdot R_{id,i-1}^{-1} \in \mathbb{Z}_q^{n \times m}$ .
- Let  $R_i = H_1(id, i) \in \mathbb{Z}_q^{m \times m}$ .
- Using algorithm BasisDel( $A_{id,i-1}, R_i, sk_{id,i-1}, \sigma_i$ ), a singer with an identity  $id$  generates a secret key  $sk_{id,i} \in \mathbb{Z}_q^{m \times m}$  for the time period  $i$ , and then deletes  $sk_{id,i-1}$ .

*FSIBBS-Sign:* On inputting an original message  $m$ , a user requests a signer with an identity  $id$  to make a blind signature. The user interacts with the signer as follows:

- Once receiving a blind signature request, a signer with an identity  $id$  sends current time period  $i$  to the requester.
- Once obtaining current time period  $i$  from a signer with identity  $id$ , the user randomly chooses  $v \leftarrow D_{\mathbb{Z}_q^m, \sigma_R}$ ,  $V \leftarrow D_{n \times n}$ ,

where,  $\sigma_R = \sqrt{n \log q} \cdot \omega(\sqrt{\log m})$ .

- The user computes  $A_{id,i} = A \cdot R_{id,i}^{-1} \in \mathbb{Z}_q^{n \times m}$ , where  $R_{id,i} = H_1(id, i) \cdot H_1(id, i-1) \cdots H_1(id, 0) \in \mathbb{Z}_q^{m \times m}$ .
- The user computes  $u_i = H_2(id, i, m)^T \cdot V + A_{id,i} \cdot v \in \mathbb{Z}_q^n$  as a blinded message of  $m$  and sends it to the signer.
- Using SamplePr( $e(A_{id,i}, sk_{id,i}, u_i, \delta_i)$ ), the signer generates a vector  $sig'_i \in \mathbb{Z}_q^m$ , and sends  $(id, i, u_i, sig'_i)$  to the user.

- Once getting  $(id, i, u_i, sig'_i)$ , the user can compute  $sig_i = (sig'_i - v)V^{-1} \in \mathbb{Z}_q^m$  and outputs the final blind

signature  $(id, i, m, \mathbf{sig}_i)$ .

**FSIBBS-Verify:** On inputting  $(id, i, m, \mathbf{sig}_i)$ , where  $id$  is a signer identity,  $i$  is an index of time period,  $m$  is an original message, and  $\mathbf{sig}_i$  is the corresponding blind signature. Then, the verifier does as follows:

1). To verify that  $\mathbf{sig}_i \in \mathbb{Z}_q^m$  is a small but non-zero vector, which means  $0 < \|\mathbf{sig}_i\| \leq \delta_i \sqrt{m}$ .

2). To verify that  $\mathbf{A}_{id,i} \cdot \mathbf{sig}_i = H_2(id, i, m)^T$ , where

$$\mathbf{A}_{id,i} = \mathbf{A} \cdot \mathbf{R}_{id,i}^{-1}, \text{ and } \mathbf{R}_{id,i} = H_1(id, i) \cdot H_1(id, i-1) \cdots H_1(id, 0).$$

3). If both the above conditions are satisfied, the verifier outputs "accept"; otherwise "reject".

#### 4.2. Security Analysis of Our Construction

We now analysis the security requirements of correctness, blindness, unforgeability, forward secrecy for the proposed FSIBBS construction in the random oracle model.

**Correctness:** If both the user and the signer with a identity  $id$  interacted with each other honestly, then once getting a signature  $(id, i, m, \mathbf{sig})$ , we have the following equations:

$$\begin{aligned} \mathbf{A}_{id,i} \cdot \mathbf{sig} &= \mathbf{A}_{id,i} \cdot (\mathbf{sig}' - \mathbf{v}) \cdot \mathbf{V}^{-1} = \mathbf{A}_{id,i} \cdot \mathbf{sig}' \cdot \mathbf{V}^{-1} - \mathbf{A}_{id,i} \cdot \mathbf{v} \cdot \mathbf{V}^{-1} \\ &= \mathbf{u}_i \cdot \mathbf{V}^{-1} - \mathbf{A}_{id,i} \cdot \mathbf{v} \cdot \mathbf{V}^{-1} = H_2(id, i, m)^T + \mathbf{A}_{id,i} \cdot \mathbf{v} \cdot \mathbf{V}^{-1} - \mathbf{A}_{id,i} \cdot \mathbf{v} \cdot \mathbf{V}^{-1} \\ &= H_2(id, i, m)^T. \end{aligned}$$

So it is clear that the proposed construction is correct.

**Theorem 1** The proposed FSIBBS construction satisfies the blindness property.

**Proof:** We show that the view of an adversarial signer  $S$  with an identity  $id$  is perfectly from the value of  $b$ . From the above game, the PKG generates the master secret key  $msk$ , the master public key  $mpk$  and then sends  $mpk$  to  $S$ .  $S$  chooses two messages  $m_0$  and  $m_1$ .

The referee chooses a random bit  $b \in \{0, 1\}$ .  $(m_b, id, mpk)$ ,  $(m_{1-b}, id, mpk)$  are given to honest users  $U_0$ ,  $U_1$  respectively.  $U_0$  and  $U_1$  interact with  $S$  to get signatures on  $m_b$  and  $m_{1-b}$ .  $U_0$  and  $U_1$  blind  $m_b$  and  $m_{1-b}$  by

$$\mathbf{u}_b = H_2(id, i, m_b)^T \cdot \mathbf{V}_b + \mathbf{A}_{id,i} \cdot \mathbf{v}_b,$$

$$\mathbf{u}_{1-b} = H_2(id, j, m_{1-b})^T \cdot \mathbf{V}_{1-b} + \mathbf{A}_{id,j} \cdot \mathbf{v}_{1-b}.$$

Here  $H_2$  is a collision resistance hash function,  $\mathbf{V}_b$  and  $\mathbf{V}_{1-b}$  are two random matrices sampled from  $D_{n \times n}$ ,  $\mathbf{v}_b$  and  $\mathbf{v}_{1-b}$  are random vectors sampled from  $D_{\mathbb{Z}_q^m, \sigma_R}$ . Due to the property of collision resistance hash function  $H_2$ , and the random matrix  $\mathbf{V}_b$  or  $\mathbf{V}_{1-b}$ ,  $H_2(\cdot)^T \cdot \mathbf{V}_b$  or  $H_2(\cdot)^T \cdot \mathbf{V}_{1-b}$  is perfect independent from the value of  $b$ . From lemma 2, the distribution of  $\mathbf{A}_{id,j} \cdot \mathbf{v}_b$ ,  $\mathbf{A}_{id,j} \cdot \mathbf{v}_{1-b}$  are uniform over  $\mathbb{Z}_q^n$ . So  $\mathbf{u}_b$  and  $\mathbf{u}_{1-b}$  are uniform over  $\mathbb{Z}_q^n$  and indistinguishable. Therefore, we have that the distributions of  $(id, i, \mathbf{u}_b, \mathbf{sig}_b)$  and

$(id, i, \mathbf{u}_{1-b}, \mathbf{sig}_{1-b})$  are perfect independent from the view of  $S$ .

From all the above, the distributions of the view of the signer  $S$  with the identity  $id$  for  $U_0$  and  $U_1$  are equivalent and independent from the value of  $b$ . Therefore the proposed FSIBBS construction satisfies the blindness property.

**Theorem 2** Under the  $SIS_{q,m,\beta}$  assumption, the proposed FSIBBS construction is unforgeability.

**Proof:** Assume that there is an adversary  $\mathcal{A}$  that can forge a valid signature in the proposed construction with a non negligible advantage  $\epsilon$ . Now we construct a challenger  $\mathcal{C}$  that simulates an attack environment and uses the adversary  $\mathcal{A}$  to create a solution for the  $SIS_{q,m,\beta}$  problem with non-negligible advantage  $\epsilon'$ .

$\mathcal{C}$  gets a random instance of the  $SIS_{q,m,\beta}$  problem and is asked to return an admissible solution.

1).  $\mathcal{C}$  is supplied with a matrix  $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$  from the uniform distribution.

2).  $\mathcal{C}$  wants to get a vector  $\mathbf{e} \in \mathbb{Z}_q^m$  such that:  $\mathbf{B}\mathbf{e} = 0 \pmod{q}$ ,  $0 < \|\mathbf{e}\| \leq \beta$ .

First of all, we assume that:

3). For each time period  $i = 0, 1, \dots, N-1$ , the adversary  $\mathcal{A}$  makes poly-bounded  $H_1$  queries on any identity adaptively.

4). Assume that  $\mathcal{A}$  has queried  $H_1$  at time period  $j < i$ , when it makes an  $H_1$  query on any identity at time period  $i$ .

5). Assume that adversary  $\mathcal{A}$  has made all relevant  $H_1$  query beforehand, when it makes a signing secret key query for any signer.

The operations performed between  $\mathcal{A}$  and  $\mathcal{C}$  are as follows:

**Setup phase:**  $\mathcal{C}$  runs algorithm  $\text{TrapGen}(q, n)$  to generate a matrix  $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$  together with a basis  $\mathbf{T} \in \mathbb{Z}_q^{m \times m}$  for  $\Lambda_q^+(\mathbf{A})$ . For each time period,  $\mathcal{C}$  sets two series of gaussian parameters  $\sigma = (\sigma_0, \sigma_1, \dots, \sigma_{N-1})$ ,  $\delta = (\delta_0, \delta_1, \dots, \delta_{N-1})$ . Then  $\mathcal{C}$  publishes the master public key  $mpk = \mathbf{A}$ , and keeps the master secret key  $msk = \mathbf{T}$  secret.

**Queries phase:** Firstly,  $\mathcal{C}$  randomly guesses  $1 \leq i^* \leq N-1$  as the time period when  $\mathcal{A}$  forges a valid blind signature, then  $\mathcal{C}$  simulates the random oracles  $H_1$ ,  $H_2$  as follows. Without loss of generality, assume that  $\mathcal{A}$  has queried  $H_2$  on every message  $m$  for  $id$  and  $i$  before making a blind signature query.  $\mathcal{C}$  maintains five lists in its local storage, namely,  $l_1$ ,  $l_2$ ,  $l_3$ ,  $l_4$  and  $l_5$  list, which are all set to be empty initially.

**$H_1$  queries:** For time period  $i = 0, 1, \dots, N-1$ ,  $\mathcal{A}$  can query  $H_1$  on any identity adaptively. For any  $(id, i)$  query,  $\mathcal{C}$  looks up  $l_1$  list to check if the value of  $H_1$  was previously defined. If it was, the value is returned. Otherwise,  $\mathcal{C}$  randomly samples a low norm matrix  $\mathbf{R}_{id,i} \in \mathbb{Z}_q^{m \times m}$  from  $D_{m \times m}$ , stores  $(id, i, \mathbf{R}_{id,i})$  in  $l_1$  list and returns it to  $\mathcal{A}$ .

**KeyExt queries:**  $\mathcal{A}$  randomly chooses a scalar

$l \in \{1, \dots, Q\}$ , where  $Q$  denotes the maximum number of KeyExt queries,  $\mathcal{C}$  does as follows:

If  $id$  is not the  $l$ -th query,  $\mathcal{A}$  queries on identity  $id$  at the initial time period,  $\mathcal{C}$  looks up  $l_1$  list to find its hash value. If it was previously defined, and the value will be returned.  $\mathcal{C}$  gets  $A_{id,0} = A \cdot H_1(id, 0)^{-1}$  and runs  $\text{BasisDel}(A, H_1(id, 0), T, \sigma_0)$  to generate the initial signing secret key  $sk_{id,0}$  and then sends it to  $\mathcal{A}$ . If it was not defined before,  $\mathcal{C}$  randomly samples a low norm matrix  $R_{id,0} \in \mathbb{Z}_q^{m \times m}$  from  $D_{m \times m}$ , and stores  $(id, 0, R_{id,0})$  in  $l_1$  list and runs algorithm  $\text{BasisDel}(A, R_{id,0}, T, \sigma_0)$  to generate  $sk_{id,0} \in \mathbb{Z}_q^{m \times m}$ , the  $\mathcal{C}$  returns it to  $\mathcal{A}$  and stores  $(id, 0, sk_{id,0})$  in  $l_2$  list.

2). If  $id$  is the  $l$ -th query,  $\mathcal{C}$  aborts the simulations

*Signing secret key queries:*  $\mathcal{A}$  queries the secret key on the signer with identity  $id$  at time period  $i+1$ ,  $\mathcal{C}$  does as follows:

1). If  $id$  is not the  $l$ -th query, for each  $1 \leq i \leq N-1$ , since we have assumed that  $\mathcal{A}$  has made  $H_1$  query on  $(id, j)$  for  $j < i$ . For  $H_1$  query on  $(id, i)$ ,  $\mathcal{C}$  looks up  $l_1$  to find a corresponding low norm matrix  $R_{id,i}$ .  $\mathcal{C}$  runs  $\text{BasisDel}(A_{id,i-1}, R_{id,i}, sk_{id,i-1}, \sigma_i)$  to generate  $A_{id,i} = A \cdot H_1(id, 0)^{-1} \cdots H_1(id, i-1)^{-1} \cdot R_{id,i}^{-1} \in \mathbb{Z}_q^{n \times m}$ , and a signing secret key  $sk_{id,i} \in \mathbb{Z}_q^{m \times m}$ . Then,  $\mathcal{C}$  returns it to  $\mathcal{A}$  and stores  $(id, i, A_{id,i}, sk_{id,i})$  in  $l_3$  list.

1). If  $id$  is the  $l$ -th query,  $\mathcal{C}$  does as follows:

a. If  $i \leq i^*$ ,  $\mathcal{C}$  randomly samples a low norm matrix  $R \in \mathbb{Z}_q^{m \times m}$  from  $D_{m \times m}$ , and returns  $(id, i, A, R)$  to  $\mathcal{A}$  and stores it in  $l_3$  list.

b. If  $i = i^* + 1$ ,  $\mathcal{C}$  runs algorithm  $\text{TrapGen}(q, n)$  to generate a matrix  $A_{id,i^*+1} \in \mathbb{Z}_q^{n \times m}$  together with a basis  $sk_{id,i^*+1} \in \mathbb{Z}_q^{m \times m}$ .  $\mathcal{C}$  returns it to  $\mathcal{A}$  and stores  $(id, i^* + 1, A_{id,i^*+1}, sk_{id,i^*+1})$  in  $l_3$  list.

c. If  $i^* + 1 \leq i \leq N-1$ ,  $\mathcal{C}$  does as before in case that  $id$  is not the  $l$ -th query.

$H_2$  queries: For any  $(id, i, m)$  query,  $\mathcal{C}$  looks up  $l_4$  list to check if the value of  $H_2$  was previously defined. If it was, the value is returned. Otherwise,  $\mathcal{C}$  looks up  $l_1$  list and  $l_3$  list to get  $(id, i, R_{id,i}), (id, i, A_{id,i}, sk_{id,i})$ . If they are found,  $\mathcal{C}$  randomly chooses  $sig_i \leftarrow D_{\mathbb{Z}_q^m, \sigma_R}$ , here  $\sigma_R = \sqrt{n \log q} \omega(\sqrt{\log m})$ , returns  $A_{id,i} sig_i$  to  $\mathcal{A}$  and stores  $(id, i, m, sig_i, A_{id,i} sig_i)$  in  $l_4$  list. If they are not found,  $\mathcal{C}$  regenerates and stores them in  $l_1$  and  $l_3$  list respectively as before and carries on the operation mentioned above. According to lemma 2, this is identity to the uniformly random value of  $H_2(id, i, m)$  in the real system.

*Signing queries:* Once receiving a signing query on  $u$ , a blinded message of  $m$  for a signer with the identity  $id$  at the time period  $i$ , the corresponding blinded factor is  $v_i \in \mathbb{Z}_q^m$

and  $V_i \in \mathbb{Z}_q^{n \times n}$ .  $\mathcal{A}$  and  $\mathcal{C}$  do as follows:

1). If  $id$  is not the  $l$ -th query,  $\mathcal{C}$  will look up  $l_5$  list to find its signing value. If it was previously defined, the value will be returned. And if it was not defined before,  $\mathcal{C}$  runs algorithm  $\text{SamplePr}(\mathcal{A}_{id,i}, sk_{id,i}, u, \delta_i)$  to get the signature  $sig'_i \in \mathbb{Z}_q^m$ .  $\mathcal{C}$  returns it to  $\mathcal{A}$  and stores  $(id, i, u, sig'_i)$  in  $l_5$  list.  $\mathcal{A}$  unblinds  $sig'_i$  to get the final signature  $sig_i = (sig'_i - v_i) \cdot V_i^{-1} \in \mathbb{Z}_q^m$ .

2). If  $id$  is the  $l$ -th query, when  $i^* < i \leq N-1$ ,  $\mathcal{C}$  generates the signature as above. Otherwise,  $\mathcal{C}$  aborts the simulations.

*Forgery phase:* Finally, the adversary  $\mathcal{A}$  outputs a tuple of  $(id^*, t^*, m^*, sig^*)$ . Adversary  $\mathcal{A}$  is considered to be succeed if the following conditions hold:

- 1).  $1 \leq t^* < j$ .
- 2).  $id^*$  has not been issued as a KeyExt query.
- 3).  $(id^*, i^*, u^*)$  has never been issued as a Signing query,  $u^*$  is a blinded message of  $m^*$ , and

$$\text{FSIBBS-Verify}(id^*, t^*, m^*, sig^*) = \text{"accept"}.$$

Once  $\mathcal{A}$  outputs a valid forgery  $(id^*, t^*, m^*, sig^*)$ ,  $\mathcal{C}$  does as follows:

1). To check if  $id^*$  is the  $l$ -th query and  $i^* = t^*$ . If any of them does not hold,  $\mathcal{C}$  aborts its run, otherwise, the view of  $\mathcal{C}$  is perfectly simulated. As we know,  $sig^*$  is a forgery signature such that  $id^*, (id^*, t^*), (id^*, t^*, u^*)$  are all not equal to the queries to KeyExt query, Signing secret key query, and Signing query, here  $u^*$  is a blinded message of  $m^*$ .

Before forging a signature, for query to  $H_2$  on  $(id^*, t^*, m^*)$ ,  $\mathcal{C}$  stores  $(id^*, t^*, m^*, sig^*, A_{id^*,i^*} \cdot sig^*)$  in  $l_4$  list, here  $A_{id^*,i^*} = B$ . By the preimage min-entropy property of the hash family, the min-entropy of  $sig_t^*$  given  $A_{id^*,i^*} \cdot sig_t^*$  (the rest of the view of  $\mathcal{A}$ , which is independent of  $sig_t^*$ ) is  $\omega(\log n)$ , so the signature  $sig_t^* \neq sig^*$  except with a negligible probability  $2^{-\omega(\log n)}$ . We also know that  $\mathcal{A}$  wins the above game only if  $sig^*$  is a valid blind signature on  $(id^*, i^*, u^*)$ ,  $u^*$  is a blinded message of  $m^*$ . Thus, we have:  $0 < \|sig^*\| \leq \delta_i \sqrt{m}$  and  $A_{id^*,i^*} \cdot sig^* = B \cdot sig^* =$

$H_2(id^*, t^*, m^*) = A_{id^*,i^*} \cdot sig_t^* = B \cdot sig_t^*$ . Therefore, we obtain a vector  $e = sig^* - sig_t^*$  as a solution to  $B \cdot e = 0 \pmod q$ .

1). If  $id^*$  is not the  $l$ -th query or  $i^* \neq t^*$ ,  $\mathcal{C}$  will abort its run. From both the above, the success probability of  $\mathcal{C}$  in solving the  $\text{SIS}_{q,m,\beta}$  problem is the same as that of  $\mathcal{A}$  in forging a valid blind signature except for a factor of  $1/QN$

due to the aborting events. Since the advantage of solving the  $SIS_{q,m,\beta}$  problem is negligible, so that the advantage of  $\mathcal{A}$  in forging a valid blind signature is negligible which means that the proposed scheme satisfies the unforgeability property.

**Theorem 3** The proposed construction is forward-secure.

*Proof:* Let the time period  $j < i$ , the user cannot obtain a signature  $(id, j, \mathbf{u}_j, \mathbf{sig}'_j)$  in the time period  $i$ . In time period  $i$ , the user sends blinded message  $\mathbf{u}_j = H_2(id, j, m)^T \cdot \mathbf{V} + \mathbf{A}_{id,j} \cdot \mathbf{v}$  to the signer. Using  $\text{SamplePre}(\mathbf{A}_{id,i}, \mathbf{sk}_{id,i}, \mathbf{u}_j, \delta_i)$ , the signer generates a vector  $\mathbf{sig}'_i \in \mathbb{Z}_q^m$  satisfying  $\mathbf{A}_{id,i} \cdot \mathbf{sig}'_i = \mathbf{u}_j$ . In the unblind phase, the user only obtains  $\mathbf{sig}_i = (\mathbf{sig}'_i - \mathbf{v})V^{-1} \in \mathbb{Z}_q^m$ , which cannot satisfies the equation  $\mathbf{A}_{id,j} \cdot \mathbf{sig}'_i = H_2(id, j, m)^T$ . Therefore, the proposed scheme satisfies the forward secrecy.

**Table 1.** Efficiency comparison.

Schemes	$\ \mathbf{spk}\ $	$\ \mathbf{ssk}\ $	Signature size	Blindness	Forward-secure
[39]	$2nm \log q$	$4m^2 \log q$	$2m \log q + k$	No	No
[40]	$3nm \log q$	$4m^2 \log q$	$(3m+1) \log q$	No	No
[48]	$nm \log q$	$m^2 \log q$	$m \log q + k$	No	Yes
Our	$nm \log q$	$m^2 \log q$	$m \log q + k$	Yes	Yes

## 5. A FSIBBS from Lattices in the Standard Model

In this section, we extend our construction to a FSIBBS scheme from lattices in the standard model. Here, the whole lifetime of the system is also divided into  $N$  time periods. The main steps of our construction are provided as follows:

**FSIBBS-Setup:** On inputting the security parameter  $n$ , a prime  $q \geq 3$ , a integer  $m \geq 6n \log q$ , and a collision-resistance hash function  $H: \{0,1\}^* \rightarrow \{0,1\}^l$ , where  $l = \text{poly}(n)$ . For each time period, the PKG sets two series of gaussian parameters  $\sigma = (\sigma_0, \sigma_1, \dots, \sigma_{N-1})$ , and  $\delta = (\delta_0, \delta_1, \dots, \delta_{N-1})$ . The PKG does as follows:

- 1).  $2lN$  matrices  $\{\mathbf{R}_{i,k}^0, \mathbf{R}_{i,k}^1\}_{0 \leq i \leq N-1, 1 \leq k \leq l} \in \mathbb{Z}_q^{m \times m}$  are sampled from  $D_{m \times m}$  randomly and a nonzero vector  $\mathbf{u}$  is sampled from  $D_{\mathbb{Z}^n, \sigma_R}$ ,  $\sigma_R = \sqrt{n \log q} \cdot \omega(\sqrt{\log m})$  by the PKG. The PKG also draws  $l+1$  independent vectors  $\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_l \in \mathbb{Z}_q^n$ .
- 2). Using algorithm  $\text{TrapGen}(q, n)$ , the PKG gets a matrix  $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$  together with a short basis  $\mathbf{T} \in \mathbb{Z}_q^{m \times m}$  for  $\Lambda_q^\perp(\mathbf{A})$ .
- 3). The PKG outputs the master public key and the master secret key:

$$\text{mpk} = \left\{ \mathbf{A}, \{\mathbf{R}_{i,k}^0, \mathbf{R}_{i,k}^1\}_{0 \leq i \leq N-1, 1 \leq k \leq l}, \mathbf{u}, \{\mathbf{c}_i\}_{0 \leq i \leq l} \right\}, \text{msk} = \mathbf{T}.$$

**FSIBBS-Extract:** On receiving the identity  $id$  of a signer,

### 4.3. Efficiency Comparison

In this subsection, we will compare the sizes of the signing public key, the signing secret key and the signature with three classical IBS schemes from lattices in Refs. [39–40, 48]. The details of the efficiency comparison are described in Table 1. We denote  $\mathbf{spk}$  and  $\mathbf{ssk}$  as the signing public key and signing secret key. Assume that the random number is  $k$ , and for consistency, we also assume that the size of time period in the proposed construction is  $k$ . Table 1 shows that the sizes of  $\mathbf{spk}$ ,  $\mathbf{ssk}$  and the signature in the proposed FSIBBS scheme is the same as that in Ref. [48], and much shorter than that in Refs. [39–40]. Meanwhile, the proposed construction enjoys the blindness property, which can provide perfect anonymity and the forward secrecy property, which can resolve the key exposure problems.

the PKG generates the initial secret key  $\mathbf{sk}_{id,0}$  as follows:

- 1). Let  $\mathbf{h}_0 = H(id, 0) \in \{0,1\}^l$ , the PKG computes

$$\mathbf{R}_{id,0} = \mathbf{R}_{0,l}^{\mathbf{h}_{0,l}} \cdot \mathbf{R}_{0,l-1}^{\mathbf{h}_{0,l-1}} \cdots \mathbf{R}_{0,1}^{\mathbf{h}_{0,1}} \in \mathbb{Z}_q^{m \times m}, \mathbf{A}_{id,0} = \mathbf{A} \cdot \mathbf{R}_{id,0}^{-1} \in \mathbb{Z}_q^{n \times m}.$$

- 2). Using algorithm  $\text{BasisDel}(\mathbf{A}, \mathbf{R}_{id,0}, \mathbf{T}, \sigma_0)$ , the PKG can generate the initial signing secret key  $\mathbf{sk}_{id,0} \in \mathbb{Z}_q^{m \times m}$  and sends it to the signer in a secure way.

**FSIBBS-Update:** On inputting  $(id, i, \mathbf{sk}_{id,i-1})$ , where  $i$  is the current time period,  $\mathbf{sk}_{id,i-1}$  is the signing secret key associated with the time period  $i-1$ . A signer with the identity  $id$  does as follows:

- 1) Let  $\mathbf{h}_{i-1} = H(id, i-1) \in \{0,1\}^l$ , the signer computes

$$\mathbf{R}_{id,i-1} = \mathbf{R}_{i-1,l}^{\mathbf{h}_{i-1,l}} \cdots \mathbf{R}_{i-1,1}^{\mathbf{h}_{i-1,1}}, \mathbf{A}_{id,i-1} = \mathbf{A} \cdot (\mathbf{R}_{id,i-1} \cdots \mathbf{R}_{id,0})^{-1} \in \mathbb{Z}_q^{n \times m}.$$

- 2) Let  $\mathbf{h}_i = H(id, i)$ ,  $\mathbf{R}_{id,i} = \mathbf{R}_{i,l}^{\mathbf{h}_{i,l}} \cdots \mathbf{R}_{i,1}^{\mathbf{h}_{i,1}} \in \mathbb{Z}_q^{m \times m}$ .

- 3) Using algorithm  $\text{BasisDel}(\mathbf{A}_{id,i-1}, \mathbf{R}_{id,i}, \mathbf{sk}_{id,i-1}, \sigma_i)$ , the signer generates the signing secret key  $\mathbf{sk}_{id,i} \in \mathbb{Z}_q^{m \times m}$  for time period  $i$ , and then deletes  $\mathbf{sk}_{id,i-1}$ .

**FSIBBS-Sign:** On inputting the message  $\mathbf{m} \in \{0\} \times \{0,1\}^l$ , a user requests the signer with the identity  $id$  to make a blind signature. The user then interacts with the signer as follows:

- 1). Once receiving a blind signature request, a signer with identity  $id$  sends the current time period  $i$  to the requester.

- 2). Once obtaining current time period  $i$  from a signer with identity  $id$ , the user randomly chooses

$\mathbf{v} \leftarrow D_{\mathbb{Z}^m, \sigma_R}, \mathbf{V} \leftarrow D_{n \times n}$ , where,  $\sigma_R = \sqrt{n \log q} \cdot \omega(\sqrt{\log m})$ .

3). Let  $\mathbf{h}_i = H(id, i) \in \{0, 1\}^l$ , the user computes matrices

$$\mathbf{R}_{id,i} = \mathbf{R}_{i,l}^{h_{i,l}} \cdots \mathbf{R}_{i,1}^{h_{i,1}}, \quad \mathbf{A}_{id,i} = \mathbf{A} \cdot (\mathbf{R}_{id,i} \cdots \mathbf{R}_{id,0})^{-1} \in \mathbb{Z}_q^{n \times m}.$$

4). The user computes  $\mathbf{u}_i = \sum_{i=0}^l (-1)^{m_i} \cdot \mathbf{c}_i^T \cdot \mathbf{V} + \mathbf{A}_{id,i} \cdot \mathbf{v}$  as a blinded message of  $m$  and sends it to the signer.

5). Using  $\text{SamplePre}(\mathbf{A}_{id,i}, \mathbf{sk}_{id,i}, \mathbf{u}_i, \delta_i)$ , the signer gets a vector  $\mathbf{sig}'_i \in \mathbb{Z}_q^m$ , and sends  $(id, i, \mathbf{u}_i, \mathbf{sig}'_i)$  to the user.

6). Once getting  $(id, i, \mathbf{u}_i, \mathbf{sig}'_i)$ , the user computes a vector  $\mathbf{sig}_i = (\mathbf{sig}'_i - \mathbf{v})\mathbf{V}^{-1} \in \mathbb{Z}_q^m$ , and outputs the final blind signature  $(id, i, m, \mathbf{sig}_i)$ .

*FSIBBS-Verify*: On inputting  $(id, i, m, \mathbf{sig}_i)$ ,  $id$  is a signer identity,  $i$  is an index of time period,  $m$  is an original message and  $\mathbf{sig}_i$  is the corresponding blind signature. Then the verifier does as follows:

1). To verify that  $\mathbf{sig}_i$  is a small but non-zero vector, which means  $0 < \|\mathbf{sig}_i\| \leq \delta_i \sqrt{m}$ .

2). To verify that  $\mathbf{A}_{id,i} \cdot \mathbf{sig}_i = \sum_{i=0}^l (-1)^{m_i} \cdot \mathbf{c}_i^T \in \mathbb{Z}_q^n$ , where  $\mathbf{A}_{id,i} = \mathbf{A} \cdot (\mathbf{R}_{id,i} \cdots \mathbf{R}_{id,0})^{-1} \in \mathbb{Z}_q^{n \times m}$ ,  $\mathbf{R}_{id,i} = \mathbf{R}_{i,l}^{h_{i,l}} \cdots \mathbf{R}_{i,1}^{h_{i,1}} \in \mathbb{Z}_q^{m \times m}$ .

3). If both the above conditions are satisfied, the verifier outputs "accept"; otherwise "reject".

## 6. Conclusion

The key exposures bring out very serious problem in some insecure mobile devices. Forward-secure blind signatures preserve the validity of past blind signatures and prevent a forger from forging past blind signatures even if the current signing secret key has been compromised. In this paper, we used basis delegation technique to construct the first FSIBBS scheme over lattice and proved its security requirements of blindness, unforgeability and forward secrecy in the random oracle model. Compared with three IBS schemes from lattice, our construction enjoys a shorter public key, secret key and signature. What is more, our scheme can deal with the key exposure problems even in the post-quantum cryptographic era. Furthermore, we also extended our scheme to a FSIBBS scheme in the standard model. In the future work, we attempt to give a security analysis of our second construction.

## Acknowledgements

This paper is supported by the Nature Science Foundation of China (61472309).

## References

- [1] D. Chaum, "Blind signatures for untraceable payments," Proceedings of the Cryptology Conference (CRYPTO'82): Santa Barbara, CA, USA, pp. 199–203, August 23–25, 1982
- [2] D. Chaum, "Untraceable electronic cash," Proceedings of the Cryptology Conference (CRYPTO'88). Santa Barbara, CA, USA, vol. 403, pp. 319–327, August 21–25, 1988
- [3] S. B. Wang, H. Fan, and G. H. Cui, "A proxy blind signature schemes based DLP and applying in e-voting," Proceedings of the International Conference on Electronic commerce (ICEC'05). Xi'an, China, pp. 641–645, August 15–17, 2005
- [4] A. Shamir, "Identity-based cryptosystem and signature schemes," Proceedings of the Cryptology Conference (CRYPTO'84). Santa Barbara, CA, USA, vol. 196, pp. 47–53, August 19–22, 1984
- [5] R. Anderson, "Two remarks on public key cryptology (invited lecture)," Proceedings of the ACM conference on Computer and Communications Security (CCS'97). Zurich, Switzerland, pp. 135–147, May 21–24, 1997
- [6] M. Bellare and S. K. Miner, "A forward-secure digital signature scheme," Proceedings of the Cryptology Conference (CRYPTO'99). Santa Barbara, CA, USA, vol. 1666, pp. 431–438, August 15–19, 1999
- [7] D. N. Duc, J. H. Cheon, and K. Kim, "A forward-secure blind signature scheme based on the strong RSA assumption," Proceedings of the International Conference on Information and Communications Security (ICICS'03). Huhehaote, China, vol. 2836, pp. 11–21, October 10–13, 2003
- [8] Y. P. Lai and C. C. Chang, "A simple forward secure blind signature scheme based on master keys and blind signatures," Proceedings of the International Conference on Advanced Information Networking and Applications (AINA'05). Taipei, Taiwan, vol. 2, pp. 139–144, March 28–30, 2005
- [9] H. F. Huang and C. C. Chang, "A new forward-secure blind signature scheme," Journal of Engineering and Applied Sciences. 1st ed., vol. 2, 2007, pp. 230–235
- [10] J. Yu, F. Y. Kong, and G. W. Li, "Forward-secure multi-signature, threshold signature and blind signature schemes," Journal of Networks. 6rd ed., vol. 5, 2010, pp. 634–641
- [11] X. Zhang and H. H. Hang, "A new forward-secure blind signature scheme," Journal of Wuhan University: Natural Science Edition. 5rd ed., vol. 57, 2010, pp. 434–438. (in Chinese)
- [12] J. J. He, F. Sun, and C. D. Qi, "A forward-secure blind signature scheme based on quadratic residue," Computer Applications & Software. 7rd ed., vol. 30, 2013, pp. 54–56. (in Chinese)
- [13] C. Gentry, C. Peikert, and V. Vaikuntanathan, "How to use a short basis: trapdoors for hard lattices and new cryptographic constructions," Proceedings of the ACM Symposium on Theory of Computing (STOC'08). Victoria, BC, Canada, pp. 197–206, May 17–20, 2008
- [14] O. Regev, "On lattices, learning with errors, random linear codes and cryptography," Proceedings of the ACM Symposium on Theory of Computing (STOC'05). Maryland, USA, pp. 84–93, May 21–24, 2005
- [15] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'10). French Riviera, vol. 6110, pp. 1–23, May 30–June 3, 2010



- [16] D. Stehlé and R. Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices," *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'11)*. Tallinn, Estonia, vol. 6632, pp. 27–47, May 15–19, 2011
- [17] D. Micciancio and C. Peikert, "Trapdoors for lattices: simpler, tighter, faster, smaller," *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'12)*. Cambridge, UK, vol. 7237, pp. 700–718, April 15–19, 2012
- [18] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattice," *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'13)*. Athens, Greece, vol. 7881, pp. 1–17, May 26–30, 2013
- [19] C. Peikert, "Lattice cryptography for the Internet," *Proceedings of the International Conference on Post-Quantum Cryptography (PQCRYPTO'14)*. Waterloo, ON, Canada, vol. 8772, pp. 197–219, October 1–3, 2014
- [20] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Predicate encryption for circuits from LWE," *Proceedings of the Cryptology Conference (CRYPTO'10)*. Santa Barbara, CA, USA, vol. 9216, pp. 503–523, August 16–20, 2015
- [21] D. Cash, D. Hofheinz, E. Kiltz, et al, "Bonsai trees, or how to delegate a lattice basis," *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'10)*. French Riviera. vol. 6110, pp. 523–552, May 30–June 3, 2010
- [22] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H)IBE in the standard model," *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'10)*. French Riviera. vol. 6110, pp. 553–572, May 30–June 3, 2010
- [23] S. Agrawal, D. Boneh, and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," *Proceedings of the Cryptology Conference (CRYPTO'10)*. Santa Barbara, CA, USA, vol. 6223, pp. 98–115, August 15–19, 2010
- [24] S. Agrawal S, D. M. Freeman, V. Vaikuntanathan, "Functional encryption for inner product predicates from learning with errors," *Proceedings of the International Conference on the Theory and Application of Cryptology and information security (ASIACRYPT'11)*. Seoul, South Korea, vol. 7073, pp. 22–41, December 4–8, 2011
- [25] S. Agrawal, X. Boyen, V. Vaikuntanathan, et al, "Functional encryption for threshold functions (or fuzzy IBE) from lattices," *Proceedings of the International Conference on Practice and Theory in Public Key Cryptography (PKC'12)*. Darmstadt, Germany, vol. 7279, pp. 280–297, May 21–23, 2012
- [26] R. Bendlin, S. Krehbiel, and C. Peikert, "How to share a lattice trapdoor: threshold protocols for signatures and (H)IBE," *Proceedings of the International Conference on Applied Cryptography and Network Security (ACNS'13)*. Banff, AB, Canada, pp. 218–236, vol. 7954, June 25–28, 2013
- [27] L. Lucas, V. Lyubashevsky, and T. Prest, "Efficient identity based encryption over NTRU lattices," *Proceedings of the International Conference on the Theory and Application of Cryptology and information security (ASIACRYPT'14)*. Kaoshiung, Taiwan, vol. 8874, pp. 22–41, December 7–11, 2014
- [28] C. Gentry, "Fully homomorphic encryption using ideal lattices," *Proceedings of the ACM Symposium on Theory of Computing (STOC'09)*. Bethesda, USA. pp. 169–178, May 31–June 2, 2009
- [29] C. Gentry, "Toward basing fully homomorphic encryption on worst-case hardness," *Proceedings of the Cryptology Conference (CRYPTO'10)*. Santa Barbara, CA, USA, vol. 6223, pp. 116–137, August 15–19, 2010
- [30] J. H. Cheon, J. S. Coron, J. Kim, et al, "Batch fully homomorphic encryption over integer," *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'13)*. Athens, Greece, vol. 7881, pp. 315–335, May 26–30, 2013
- [31] J. S. Coron, T. Lepoint, and M. Tibouchi, "Scale-invariant fully homomorphic encryption over the integers," *Proceedings of the International Conference on Practice and Theory in Public Key Cryptography (PKC'14)*. Buenos Aires, Argentina, vol. 6056, pp. 311–328, March 26–28, 2014
- [32] K. Nuida and K. Kurosawa, "(Batch) fully homomorphic encryption over integers for non-binary message spaces," *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'15)*. Sofia, Bulgaria, vol. 9056, pp. 537–555, April 26–30, 2015
- [33] X. Boyen, "Lattice mixing and vanishing trapdoors: a framework for fully secure short signature and more," *Proceedings of the International Conference on Practice and Theory in Public Key Cryptography (PKC'10)*. Paris, France, vol. 6056, pp. 499–517, May 26–28, 2010
- [34] V. Lyubashevsky, "Lattice signatures without trapdoors," *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'12)*. Cambridge, UK, vol. 7237, pp. 738–755, April 15–19, 2012
- [35] L. Lucas, A. Durmus, T. Lepoint, et al, "Lattice signatures and bimodal gaussians," *Proceedings of the Cryptology Conference (CRYPTO'13)*. Santa Barbara, CA, USA, vol. 8042, pp. 40–56, August 18–22, 2013
- [36] L. Lucas and D. Micciancio, "Improved short lattice signatures in the standard model," *Proceedings of the Cryptology Conference (CRYPTO'14)*. Santa Barbara, CA, USA, vol. 8616, pp. 335–352, August 17–21, 2014
- [37] S. D. Gordon, J. Katz, and V. Vaikuntanathan, "A group signature scheme from lattice assumptions," *Proceedings of the International Conference on the Theory and Application of Cryptology and information security (ASIACRYPT'10)*. Singapore, vol. 6477, pp. 395–412, December 5–9, 2010
- [38] M. Rückert, "Lattice-based blind signatures," *Proceedings of the International Conference on the Theory and Application of Cryptology and information security (ASIACRYPT'10)*. Singapore, vol. 6477, pp. 413–430, December 5–9, 2010
- [39] M. Rückert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," *Proceedings of the International Conference on Post-Quantum Cryptography (PQCRYPTO'10)*. Darmstadt, Germany, vol. 6061, pp. 182–200, May 25–28, 2010
- [40] Z. H. Liu, Y. P. Hu, X. S. Zhang, et al, "Efficient and strongly unforgeable identity-based signature scheme from lattice in the standard model," *Security & Communication Networks*, 1st ed., vol. 6, 2013, pp. 69–77

- [41] R. E. Bansarkhani and J. Buchmann, "Towards lattice based aggregate signatures," Proceedings of the International Conference on Cryptology in Africa, Marrakesh, Morocco. 2014, vol. 8469, pp. 336–355, May 28–30, 2014
- [42] A. Langlois, S. Ling, K. Nguyen, et al, "Lattice-based group signature scheme with verifier-local revocation," Proceedings of the International Conference on Practice and Theory in Public-Key Cryptography (PKC'14). Buenos Aires, Argentina, vol. 8383, pp. 345–361, March 26–28, 2014
- [43] S. Ling, K. Nguyen, and H. X. Wang, "Group signature from lattices: simpler, tighter, shorter, ring-based," Proceedings of the International Conference on Practice and Theory in Public-Key Cryptography (PKC'15). Gaithersburg, MD, USA, vol. 9020, pp. 427–449, March 30–April 1, 2015
- [44] P. Q. Nguyen, J. Zhang, and Z. F. Zhang, "Simpler efficient group signature from lattices," Proceedings of the International Conference on Practice and Theory in Public-Key Cryptography (PKC'15). Gaithersburg, MD, USA, vol. 9020, pp. 401–426 March 30–April 1, 2015
- [45] J. Alwen and C. Peiker, "Generating shorter bases for hard random lattices," Journal of Theory of Computing Systems. 3rd ed., vol. 48, 2011, pp. 535–553
- [46] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," SIAM Journal on Computing Archive, 1rd ed., vol. 37, 2007, pp. 267–302
- [47] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," Proceedings of the ACM Symposium on Theory of Computing (STOC'96). Philadelphia, Pa, USA, pp. 99–108, May 22–24, 1996
- [48] X. J. Zhang, C. X. Xu, C. H. Jin, et al, "Efficient forward secure identity-based shorter signature from lattice," Computers and Electrical Engineering, 6rd ed., vol. 40, 2014, pp. 1963–1971
- [49] N. A. Ebri, J. Baek, A. Shoufan, et al, "Efficient generic construction of forward-secure identity-based signature," Proceedings of the International Conference on Availability, Reliability and Security (ARES'12). Washington, DC, USA, vol. 329, pp. 55–64, August 20–24, 2012