Open Access Library Journal
2021, Volume 8, e7126
ISSN Online: 2333-9721
ISSN Print: 2333-9705

An Efficient Identity-Based Forward Secure Signature Scheme from Lattices

Guang Wu, Ruwei Huang

School of Computer, Electronics and Information, Guangxi University, Nanning, China
Email: 1187235806@qq.com

How to cite this paper: Wu, G. and Huang, R.W. (2021) An Efficient Identity-Based Forward Secure Signature Scheme from Lattices. *Open Access Library Journal*, **8**: e7126.
https://doi.org/10.4236/oalib.1107126

Received: December 29, 2020
Accepted: January 26, 2021
Published: January 29, 2021

Abstract

With the use of a large number of mobile devices, the problem of key leakage becomes more and more serious. In view of the excellent characteristics of lattice cipher and forward-secure digital signature scheme, the construction of identity-based forward-secure digital signature based on lattice technology has become a research hotspot. However, the identity-based forward secure digital signature scheme on the existing grid has the disadvantage of excessive signature length. This paper uses the technique (without trapdoors) of Lyubashevsky and extended Samplepre, an efficient identity-based forward secure signature scheme from lattice is proposed. Its security is based on the Small Integer Solution (SIS) difficulty assumption, and the strong non-forgery of the signature scheme is achieved. The analysis results show that, compared with the existing schemes, the key and signature are smaller in size, more efficient in computing, able to resist quantum attacks, and more practical.

Subject Areas

Information and Communication: Security, Privacy, and Trust

Keywords

Identity-Based Signature, Lattice, Forward Security, Without Trapdoors, Small Integer Solution (SIS)

1. Introduction

1.1. Background of This Study

The identity-based signature scheme (IBS) was first proposed by Shamir [1] in 1984 and is a public key encryption system. So far, most traditional identity-based signature schemes [2]-[7] have been proposed based on the bilinear or

quadratic residual assumption.

Although the existing traditional identity-based signature schemes are very efficient and the types can basically meet the needs of most applications, such signature schemes have obvious security flaws. Shor [8] pointed out that the prime number decomposition and discrete logarithm problems based on traditional cryptography can be broken by quantum computers in polynomial time. This means that once quantum computers become a reality, the existing public key cryptography will be compromised and will no longer be secure. Ajtai [9] proved that the difficulty of the difficult problem on the lattice under the random instance is equivalent to the difficulty under the worst instance; in addition, the grid public key cryptographic algorithm is simple, efficient, and suitable for low-power devices. There are no effective algorithms, including quantum algorithms, which can solve difficult problems on the grid. In recent years, lattice-based cryptosystems have achieved fruitful results in applications such as digital signatures [10] [11] [12], hierarchical identity-based encryption schemes (HIBE) [13], and fully homomorphic encryption [14].

In 1997, Anderson *et al.* [15] first proposed the idea of forward secure signature, Bellare and Miner [16] further proposed more practical algorithms, and gave a formal definition of forward-secure digital signature and its security. More forward secure digital signature algorithms [17] [18] are proposed. However, there are few researches on identity-based forward security digital signature algorithms. Liu proposed the first identity-based forward secure digital signature algorithm in [19], however, he did not give a formal definition and formal security proof. Yu *et al.* gave the formal definition and security proof of an identity-based forward secure digital signature algorithm in literature [20], but the algorithm required a large number of bilinear pairing operations and was not suitable for mobile devices with limited computing power. Ebri [21] gave the general construction algorithm of forward secure digital signature algorithm based on identity, and simplified the definition of security. However, all of the above are based on the assumptions of difficult problems in traditional cryptography and cannot resist quantum computer attacks.

Zhang [22] proposed the first identity-based forward secure digital signature scheme (FSIBS), whose main idea is based on the layered identity-based signature scheme of Ruckert [23].

1.2. Contributions of This Article

In this paper, in the random oracle model, based on the assumption of small integers to solve difficult problems, we prove that our scheme is unforgeable against adaptive identity selection and selection message attacks. In addition, Zhang's scheme uses the lattice proxy algorithm of literature [24] to update the signature key, keeping the dimensionality unchanged. In our research, we combine the trapdoor-free signature with the trapdoor base to realize the identity-based signature design that does not rely on the expansion of the lattice dimension, which will not bring large calculation, communication or storage

overhead, and is more efficient. Our signature key size and signature size are much shorter. In this way, our scheme can be applied to post-quantum communication more efficiently.

1.3. The Structure of the Organization

The rest of this paper is arranged as follows: In the second section, we give the prerequisite knowledge to be used in this paper; in the third section, the formal definition and security model of our FSIBS scheme are given. In the fourth section, the algorithm description and security proof of our scheme are given. In the fifth section, the performance comparison of the scheme is given. Finally, we conclude our work in section 6.

2. Prerequisite Knowledge

2.1. Description of Related Symbols

For a positive integer n, use $[n]$ to represent the set $\{1,2,\cdots,n\}$. For any character string a and b, $|a|$ represents the bit length of a, and $a\|b$ represents the concatenation of two characters a and b, and $a \oplus b$ represents their exclusive OR operation.

2.2. Definitions and Tools Related to Cryptography

Definition 2.1 (Hash function) Hash function is a one-way function with compression characteristics. Its input is a string of arbitrary length, and its output is a string of fixed length, namely $H \square\{0,1\}^* \to \{0,1\}^n$. It is mainly used for message authentication and digital signature.

A common tool used in cryptography is: Random Oracle. At present, in the provable security discussion of many cryptographic algorithms, the hash function is regarded as a random oracle. This basic idea comes from the literature [25]. Fiat and Shamir [26] first transformed an identification algorithm into a signature algorithm under a random oracle model. Later, Bellare and Rogaway formally proposed a random oracle model in [27], and constructed a general proof framework for cryptographically provable security statements under the random oracle model.

2.3. Theoretical Basis of Lattice Cipher

Definition 2.2 (integer lattice), let $B = [b_1, b_2, \cdots, b_m] \in Z^{m\times m}$ is an $m \times m$ -dimensional invertible matrix. It consists of m linearly independent vectors $b_1, b_2, \cdots, b_m \in Z^m$. The m-dimensional integer lattice generated by matrix B is:

$$\Lambda = \left\{ y \in Z^m \mid y = Bc = \sum_{i=1}^{m} c_i b_i, c \in Z^m \right\} \tag{1}$$

2.4. Discrete Gaussian Distribution

Definition 2.3 for any real parameter $s > 0, c \in R^m$ as the center, the discrete Gaussian distribution density function of lattice Λ is defined as:

$$\forall x \in \Lambda, \rho_{s,c}(x) = \exp\left(-\pi \frac{\|x-c\|^2}{s^2}\right) \tag{2}$$

Let $\rho_{s,c}(\Lambda) = \sum_{x\in\Lambda} \rho_{s,c}(x), \Lambda$, the discrete Gaussian distribution on Λ is defined as:

$$\forall y \in \Lambda, D_{\Lambda,s,c}(y) = \frac{\rho_{s,c}(y)}{\rho_{s,c}(\Lambda)} \tag{3}$$

Lemma 2.1 (Properties of Discrete Gaussian Distribution on Lattice [11] [28]). Let prime number $q \geq 3$, integer $m \geq 2n\log q$, T is a set of basis of lattice $\Lambda_q^{\perp}(A)$, Gaussian parameter $s \geq \|\tilde{T}\|\omega\left(\sqrt{\log m}\right)$. Then for any vector $y \in Z_q^n$, there are the following results:

1) $\Pr\left[x \leftarrow D_{\Lambda,s,c}(x) : \|x\| > s\sqrt{m}\right] \leq negl(n)$;

2) For a randomly selected matrix $A \in Z_q^{n\times m}$, if $e \leftarrow G_{Z^m,s}$, then we have a statistical distribution of $y = Ae \pmod q$ close to the uniform distribution on Z_q^n.

2.5. Difficult Questions on Grid

Definition 2.4 (Small integer solution problem) Let the parameters n and m be positive integers, q be prime numbers, and given a small real number $\beta > 0$. A is a randomly selected matrix on $Z_q^{n\times m}$. The SIS problem is to find a short vector v on the lattice $\Lambda_q^{\perp}(A)$, namely $Av = 0 \pmod q$, so that its norm satisfies $\|v\| \leq \beta$.

2.6. Basic Algorithm on Grid

Lemma 2.2 (TrapGen generation algorithm, TrapGen [29]) There is a probability polynomial time algorithm TrapGen. The algorithm inputs integers $q \geq 2$ and $m \geq 5n\log q$, and outputs a matrix $A \in Z_q^{n\times m}$ and a short basis $T_A \in Z_q^{m\times m}$ of lattice $\Lambda_q^{\perp}(A)$ in polynomial time. Make A statistically close to the uniform distribution $Z_q^{m\times m}$, and the short basis $T_A \in Z_q^{m\times m}$ satisfies $\|\widetilde{T_A}\| \leq O\left(\sqrt{n\log q}\right)$.

In 2008, scholars such as Gentry constructed the pre-image sampling function (PSF) in the literature [11]. This technology plays an important role in the construction of the lattice encryption algorithm.

Lemma 2.3 (Original image sampling algorithm) Let the integer $m \geq n$, q be a prime number, and $\Lambda_q^{\perp}(A)$ is a lattice defined by the matrix $A \in Z_q^{n\times m}$. The matrix $T_A \in Z_q^{m\times m}$ is a short basis of the lattice $\Lambda_q^{\perp}(A)$. If the parameter $s \geq \|\widetilde{T_A}\|\omega\left(\sqrt{\log m}\right)$, then there is a polynomial time algorithm $\text{SamplePre}(A, T_A, s, u)$ for all $u \in Z_q^n$. It can output a vector $v \in \Lambda^u(A)$ drawn from a distribution statistically close to $D_{\Lambda,s,c}(x)$.

According to Lemma 2.1, we know that an original image v corresponding to the vector $u \in Z_q^n$ extracted by the original image sampling algorithm SamplePre will satisfy $\|v\| \leq s\sqrt{m}$ with an overwhelming probability.

The above SamplePre algorithm is only for the case of a vector. In many cases,

we need to calculate a pre-image with a smaller norm corresponding to a matrix. Therefore, we need to extend the algorithm to a more general situation. Here we refer to the definition of the general Gaussian distribution given by Tian [30].

Definition 2.5 (General Discrete Gaussian Distribution) Let the integer $m \geq n$, q be a prime number, and k is a positive integer, we define $k < n \leq m$, so that the matrix U satisfies the smaller norm. For any real number $s > 0$ and matrix $A \in Z_q^{n\times m}$ and $U = [u_1, u_2, \cdots, u_k] \in Z_q^{n\times k}$, define the distribution $G\Lambda^u(A)_{,s} = G\Lambda^{u_1}(A)_{,s} \times \cdots \times G\Lambda^{u_k}(A)_s$.

According to Lemma 2.1, we know that a vector x randomly selected from the distribution $G\Lambda^u(A)_{,s}$ will satisfy $\|x\| \leq s\sqrt{m}$ with an overwhelming probability. Therefore, it is not difficult to obtain that the matrix X randomly selected from the distribution $G\Lambda^u(A)_{,s}$ will also satisfy $\|X\| = \max(\|x_i\|) \leq s\sqrt{m}$ with an overwhelming probability. If we can find an algorithm, it can output a matrix V for any input matrix U, so that $AV = U \pmod q$ and the distribution statistics of matrix V are close to $G\Lambda^u(A)_{,s}$, according to our analysis of the distribution $G\Lambda^u(A)_{,s}$, this algorithm is the general pre-image sampling algorithm we require. This algorithm is recorded as the SampleMat algorithm.

Lemma 2.4 (General Original Image Sampling Algorithm) Let the integer $m \geq n$, q be a prime number, and k is a positive integer. Here we define $k < n \leq m$ so that the matrix U satisfies the smaller norm. $\Lambda^{\perp}(A)$ is a lattice defined by matrix A, and matrix $T_A \in Z_q^{m\times m}$ is a short basis of lattice $\Lambda_q^{\perp}(A)$. Parameter $s \geq \|\widetilde{T_A}\| \omega(\sqrt{\log m})$, then for any matrix $U \in Z_q^{n\times k}$, there is a polynomial time algorithm $\mathrm{SampleMat}(A, T_A, s, U)$, it can extract a matrix $V \in Z_q^{m\times k}$ from a distribution statistically close to $G\Lambda^u(A)_{,s}$ to satisfy $AV = U \pmod q$.

Definition 2.6 (Discrete normal distribution) Let the parameter $\sigma > 0$ and the center $c \in R^m$, then the continuous normal distribution in the space R^m is $\rho_{\sigma,c}^m(x) = (2\pi\sigma^2)^{-\frac{m}{2}} \exp\left(-\frac{\|x-c\|^2}{2\sigma^2}\right)$. Let $\rho_{\sigma,c}^m(Z^m) = \sum_{x\in Z^m} \rho_{\sigma,c}^m(x)$. Define the discrete normal distribution with $c \in Z^m$ as the center and σ parameter in Z^m as $D_{\sigma,c}^m(x) = \rho_{\sigma,c}^m(x) / \rho_{\sigma,c}^m(Z^m)$. For the convenience of notation, we abbreviate $\rho_{\sigma,0}^m$ and $D_{\sigma,0}^m$ as ρ_σ^m and D_σ^m, respectively.

Literature [29] [31] on two basic properties of discrete normal distribution:

Lemma 2.5. For any real number $\sigma > 0$ and integer $m > 0$, we have:

1) $\Pr[x \leftarrow D_\sigma^1 : |x| > 12\sigma] < 2^{-100}$;

2) $\Pr[x \leftarrow D_\sigma^m : \|x\| > 2\sigma\sqrt{m}] < 2^{-m}$;

Lemma 2.6. For any vector $v \in Z^m$ and positive real number α, if $\sigma = \omega(\|v\|\sqrt{\log m})$, we have: $\Pr[x \leftarrow D_\sigma^m : D_\sigma^m(x) / D_{\sigma,v}^m(x) = O(1)] = 1 - 2^{\omega(\log m)}$

More specifically, if $\sigma = \alpha\|v\|$, then

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

In view of the complicated calculation of the sampling technique of Genntry

et al. [11], Lyubashevsky [31] proposed a signature algorithm that does not require sampling operations on the grid. The technique used in this algorithm is called the non-sampling technique. At present, the non-sampling technology has gradually become an important technology of the social lattice signature scheme. Its core idea is to force the distribution of the output signature to be independent of the signature key s_k of the signer by outputting candidate signatures probabilistically.

This paper needs to use the general bifurcation lemma when proving the security of the signature scheme. Bellare and Neven [32] gave the following general bifurcation lemma.

Lemma 2.7 (General Bifurcation Lemma) Let q be a positive integer, and H is a set with $h \geq 2$ elements. Let $\mathcal{JG}$ be a parameter generation algorithm, B is a random algorithm, the input of B is $\{x, h_1, \cdots, h_q\}$, and the output is (J, σ), where $x \in \{0, \cdots, q\}$ $h_i \in H\left(i \in [q]\right)$. Let the acceptance probability acc of Algorithm B be the probability of $J \geq 1$ in the experiment
$EXP = \left\{x \leftarrow \mathcal{JG}; h_1, \cdots, h_q \leftarrow H; (J, \sigma) \leftarrow \mathcal{B}\left(x, h_1, \cdots, h_q\right)\right\}$.

3. Formal Definition and Security Model

This article first provides a formal definition of an identity-based forward secure digital signature algorithm. According to the literature [21], this paper also sets the time period to be associated with the signature private key information, which can be determined by each signing user, and the algorithm is more flexible. In order to set the initial signature private key, PKG needs to set the time period and the signer's identity information in advance. The identity-based forward secure digital signature algorithm consists of the following five sub-algorithms:

FSIBSSetup: The key generation algorithm is a probabilistic polynomial time algorithm, the input is the security parameter κ, the output is the system master key *msk*, and the public parameter *mpk*;

FSIBSExtract: The identity-based key proposal algorithm is a probabilistic polynomial time algorithm. The input is the public parameter *mpk*, the master key *msk*, and the user's identity information $id \in \{0,1\}^*$, where $id = id \,||\, T$, ID is the user's real identity, and T is the time period preset by the system. The output of the algorithm is the initial private key $SK_{id||0}$ corresponding to the identity information *id*, which is transmitted to the user through a secure channel.

FSIBSUpdate: The key update algorithm is a probabilistic polynomial time algorithm. The input is the current time *i*, the user's identity information *id*, and the user's private key at this moment $Sk_{id||i}$, and the output is the next time $i+1$ private key $Sk_{id||i+1}$.

FSIBSSign: The signature algorithm is a probabilistic polynomial time algorithm. The input is the current time *i*, the user's identity information *id*, and the user's private key at this time $Sk_{id||i}$, the message *M*, the digital signature of the output message *M sig*.

FSIBSVerify: The verification algorithm is a deterministic algorithm. Input the user's identity information *id*, time *i*, information *M*, and digital signature *sig*. If *sig* is valid, the algorithm output is 1, otherwise the output is 0.

The correctness of the scheme: If the signature *sig* is a valid signature of message *M*, then $\text{FSIBSVerify}_{mpk}\left(id, i, M, sig\right)=1$.

The following introduces the security model of the identity-based forward secure digital signature algorithm. The FSIBS algorithm defined in this article is unforgeability in the case of adaptive identity selection and adaptive selection message attacks.

Setup: Challenger C sets the system public parameters *mpk*, and sends *mpk* to opponent F.

Queries: At this stage, opponent F makes the following queries:

UserKeyExt: Adversary F makes an inquiry about identity information $id\left(id = ID \| T\right)$. Challenger C generates a signature private key for identity information *id* $SK_{id\|0}$, and sends it to opponent F;

Breaking oracle: When receiving an inquiry (*id*, *j*) from the opponent F. Where $id = ID \| T$, $1 \le j \le T$, challenger C returns the signature private key at time *j* $SK_{id\|j}$ to opponent F;

Signing oracle: When receiving an inquiry $\left(id, i, M\right)$ from adversary F, using the signature private key at time *i* $SK_{id\|i}$, challenger C generates a digital signature sig about message *M*.

After each moment, the adversary F can choose to execute the signature query at the next moment, or execute the corresponding forgery.

Forgery phase: In this phase, after polynomial time, the adversary F ends the above-mentioned inquiry phase, and then uses the knowledge he has acquired to forge a signature of the user whose identity is id^* to the message $M^* sig^*$, the opponent F can win the game if and only if the following conditions are true:

1) $\text{FSIBSVerify}_{mpk}\left(id^*, i^*, M^*, sig^*\right)=1, 1 \le i^* < j$;

2) The adversary F has never asked about the identity id^*;

3) The opponent F has never signed $\left(id^*, i^*, M^*\right)$.

4. Description of Forward Secure Digital Signature Algorithm Based on Identity on Grid

In this section, we present the forward secure digital signature algorithm (FSIBS) based on the identity on the grid. Set the required parameters of the program: Prime number $q \ge 3$, positive real number $M \approx e$, positive integer $m > 5n\log q, k, \lambda$, real number $\tilde{L} = O\left(\sqrt{n\log q}\right)$, Gaussian parameter $s = \breve{L} \cdot \omega\left(\sqrt{\log n}\right)$ and real number $\sigma = 12s\lambda m$. The system defines two secure hash functions $H_1 : \{0,1\}^* \to Z_q^{n\times k} \sim D_{n\times k}$;

$H : \{0,1\}^* \to \left\{v : v \in \{-1,0,1\}^k, \|v\|_1 \le \lambda\right\}$. Below we give an identity-based forward secure digital signature algorithm under the random oracle model:

FSIBSSetup: Based on the security parameter *n*, PKG runs the algorithm

$\mathrm{TrapGen}(q,n)$ to generate a matrix $A \in Z_q^{n\times m}$, and a short basis $T_A \in Z_q^{m\times m}$ of the lattice $\Lambda_q^{\perp}(A)$, and satisfy $\left\|\widetilde{T_A}\right\| \le O\left(\sqrt{n\log q}\right)$. The system outputs public parameters $mpk = \{A, H, H_1\}$, and keeps the secret master key $msk = T_A$.

FSIBSExtract: the received user's identity information $id = ID \| T$, where *ID* is the user's real identity, and T is the preset time period associated with the signature private key. PKG uses its own master key *msk* to generate the user's original private key $SK_{id\|0}$.

1) Let $R_{id\|0} = H_1(id \| 0) \in Z_q^{n\times k}$, calculate $A_{id\|0} = A\left(R_{id\|0}\right)^{-1}$;

2) PKG runs the algorithm $\mathrm{SampleMat}\left(A, T_A, s, H_1(id \| 0)\right)$ to generate $SK_{id\|0}$ as the user's original private key, and then secretly sends it to the user through a secure channel. According to the nature of the algorithm SampleMat, we know that the key $SK_{id\|0}$ satisfies $A_{id\|0} \cdot SK_{id\|0} = H_1(id \| 0)$ and $\left\|SK_{id\|0}\right\| \le s\sqrt{m}$.

FSIBSUpdate: Given $\left(id, i, SK_{id\|i-1}\right)$, where $id = ID \| T$, i is this moment. $SK_{id\|i-1}$ is the signature private key of $i-1$ at the previous moment, the user performs the following steps:

For $i = 1$ to T, the execution is as follows:

1) If $i = 1$, set $SK_{id\|0}$ as the user's original signature private key;

2) Calculate $R_{id\|i-1} = H_1(id \| i-1)\cdots H_1(id \| 0) \in Z_q^{n\times k}$, $A_{id\|i-1} = A\left(R_{id\|i-1}\right)^{-1}$ as the public key at time $i-1$.

3) Let $R_i = H_1(id \| i)$, calculate $SK_{id\|i} \leftarrow \mathrm{SampleMat}\left(A_{id\|i-1}, T_A, s, H_1(id \| i)\right)$.

4) Output $SK_{id\|i}$.

FSIBSSign: Given (id, i, M), where $id = ID \| T$, i is the moment, M is the message to be signed, the user performs the following operations:

1) First choose a $y_i \leftarrow D_\sigma^m$;

2) Calculate $c_i = H\left(A_{id\|i} y_i, M\right)$ and $z_i = SK_{id\|i} \cdot c_i + y_i$;

3) With the probability $\min\left(1, \dfrac{D_\sigma^m(z_i)}{MD_{\sigma, Sk_{id\|i}c}^m(z_i)}\right)$, output the signature $sig = (z_i, c_i)$. If there is no signature output, the algorithm is repeated until there is a signature output.

FSIBSVerify: Given (id, i, M, sig), enter the system's public parameters *mpk*, message *M*, signature $sig = (z_i, c_i)$, and identity $id = ID \| T$, if $c_i = H\left(A_{id\|i} z_i - H_1(id \| i) c_i, M\right)$ and $\|z_i\| \le 2\sigma\sqrt{m}$, then output Accept.

Theorem 4.1 the identity-based forward secure digital signature scheme proposed in this section satisfies the correctness.

Proof: According to the construction of the above signature scheme, we know

$$\begin{aligned} A_{id\|i} z_i - H_1(id \| i) c_i &= A_{id\|i} z_i - A_{id\|i} \cdot SK_{id\|i} c_i \\ &= A_{id\|i}\left(z_i - SK_{id\|i} c_i\right) \\ &= A_{id\|i} y_i \end{aligned}$$

So we have $H\left(A_{id\|i} z_i - H_1(id \| i) c_i, M\right) = H\left(A_{id\|i} y_i, M\right) = c_i$. In addition, according to Lemma 2.6 of the unsampling technique, we know that the distri-

bution of z_i is very close to D_σ^m. Therefore, according to Lemma 2.5, we know that z_i will satisfy $\|z_i\| \le 2\sigma\sqrt{m}$ with a probability of not less than $1-2^{-m}$.

5. Proof of Safety

In this section, we mainly prove that under the random oracle model, the identity-based forward secure digital signature algorithm on the lattice can resist the unforgeability in the case of adaptive identity selection and adaptive selection message attacks.

Theorem 5.1 under the random oracle model, if the adversary F breaks the security of the identity-based forward secure digital signature scheme on the lattice with a non-negligible probability ε. Then there is an algorithm C to solve the SIS difficult problem with a non-negligible probability ε'.

Proof: Assuming that there is an opponent F that forges a digital signature with a non-negligible probability ε, below we construct an algorithm C to solve the SIS difficulty problem by running the opponent F as a subroutine and with a non-negligible probability ε'. Assume as follows:

1) For each time $i = 0,1,\cdots,T$, the adversary F adaptively performs a polynomial H1 query about the user's identity.

2) When the adversary F performs the H1 query about the identity at time i, we assume that it has performed the H1 query before the time i.

When adversary F executes an inquiry about the user's signature private key, we assume that it has executed the related H1 inquiry.

Setup: Algorithm C sets the corresponding public parameters, and sends the system public parameters $mpk = \{A, H, H_1\}$ to the adversary F, and the secret master key $msk = T_A$.

Attack Phase: First, algorithm C randomly guesses $i^* \left(1 \le i^* \le T\right)$ as the forged signature of opponent F at this moment. Without loss of generality, suppose that the adversary F has made an H query about (id, i, M) before asking about the digital signature of (id, i, M). C creates four lists, L_1, L_2, L_3, L_4, respectively, and the initial values of the four lists are all empty.

H1 query: For any $i = 0,1,\cdots,T$, C maintains a list of H1 queries $L_1 = (id \| i, Q_i)$ (where Q_i represents the H1 hash function value of $id|1$. The initial value of the list is empty. Adversary F makes H1 query to $id|1$. If $(id \| i, Q_i)$ is in the list, C will pass Q_i as the result of responding to H1 query to opponent F. Otherwise, C randomly selects a $R_i \sim D_{n\times k}$, sends R_i as the result of the response to the H1 query to the opponent F, and adds $(id \| i, R_i)$ to the list L1.

UserkeyExt: Adversary F randomly selects $\ell \in \{1,2,\cdots,Q\}$, where Q is defined as the maximum number of queries about UserkeyExt. Algorithm C performs the following steps:

Adversary F makes H1 query on $id|0$, and C queries the list to find $(id \| 0, Q_0)$, $Q_0 = H_1(id \| 0)$. C runs the algorithm SampleMat$\left(A, T_A, s, H_1(id \| 0)\right)$ to generate $SK_{id\|0}$ as the user's original pri-

vate key, and then secretly sends it to the adversary F through a secure channel. And separately store $\left(id \| 0, Q_0, SK_{id\|0}\right)$ in list L2 for subsequent use.

If *id* is the ℓ query, C terminates the operation.

Signing secret key queries: When the adversary F executes the enquiry about the signature private key of (*id*, *i*), C provides the adversary F with the signature private key at time *i* in the following manner $SK_{id\|i}$.

If *id* is not in the ℓ query, the execution steps are as follows: For each time $i \in [T]$, assume in advance that the H1 query about $id \| j$ before time *i* has been responded, where $j < i$. For each inquiry about the signature private key of $id \| i$, C calculates $A_{id\|i-1} = A\left(H_1\left(id \| 0\right)\right)^{-1}\left(H_1\left(id \| 1\right)\right)^{-1}\cdots\left(H_1\left(id \| i-1\right)\right)^{-1}$, let $R_i = H_1\left(id \| i\right)$. Calculate $SK_{id\|i} \leftarrow \text{SampleMat}\left(A_{id\|i-1}, T_A, s, H_1\left(id \| i\right)\right)$, as the user signature private key at time *i*, the user public key at time *i* is specifically expressed as follows:
$A_{id\|i} = A\left(H_1\left(id \| 0\right)\right)^{-1}\left(H_1\left(id \| 1\right)\right)^{-1}\cdots\left(H_1\left(id \| i-1\right)\right)^{-1} R_i^{-1}$. Finally, C returns $SK_{id\|i}$ to opponent F, and stores $\left(id \| i, A_{id\|i}, SK_{id\|i}\right)$ to list L3.

If *id* is the ℓ query, C executes as follows:

If $i \le i^*$, then C chooses a random uniform matrix $W \in Z_q^{n\times k}$ to the opponent F.

If $i = i^* + 1$, C runs the trapdoor generation algorithm $\text{TrapGen}\left(q, n\right)$ to generate a matrix $A_{id\|i^*+1} \in Z_q^{n\times m}$, and the corresponding trapdoor short base $SK_{id\|i^*+1} \in Z_q^{m\times m}$. Then C returns $SK_{id\|i^*+1}$ to opponent F, and finally C stores $\left(id \| i^* + 1, A_{id\|i^*+1}, SK_{id\|i^*+1}\right)$, to list L3.

If $i^* + 1 \le i \le T$, then C executes the same steps as if *id* was not in the ℓ query.

H query: For a different $\left(id, i, M\right)$, C first verifies whether it has been asked before, and if it has been asked, it returns the corresponding value. Otherwise, C queries the lists L_1 and L_3 to see if it can find $\left(id \| i, H_1\left(id \| i\right)\right)$ and $\left(id \| i, A_{id\|i}, SK_{id\|i}\right)$. If they can all be found, randomly select a vector $y_i \leftarrow D_\sigma^m$, and C runs the algorithm: $c_i = H\left(A_{id\|i} y_i, M\right)$ and $z_i = SK_{id\|i} \cdot c_i + y_i$, C with probability $\min\left(1, \dfrac{D_\sigma^m\left(z_i\right)}{MD_{\sigma, Sk_{id\|i}c}^m\left(z_i\right)}\right)$ output the signature $sig = \left(z_i, c_i\right)$ to the opponent F. Store $\left(id, i, M, sig\right)$ to list L4. If none of them are found, C generates and stores the corresponding values in the lists L1 and L3 as before, and then continues with the above steps.

Sign queries: Adversary F makes a signature query about each information $\left(id, i, M\right)$, and C answers the query as follows:

If *id* is not in the ℓ query, the steps are as follows: C query list L4 to see if $\left(id, i, M, sig\right)$ can be found, if it can be found in the list, C returns the digital signature sig of message *M* at time *i*. Otherwise, C queries lists L1 and L3 respectively to see if it can find $H_1\left(id \| i\right)$ and $SK_{id\|i}$. If not found, C generates these values as before, and finally C runs the algorithm: $c_i = H\left(A_{id\|i} y_i, M\right)$ and $z_i = SK_{id\|i} \cdot c_i + y_i$. C outputs the signature $sig = \left(z_i, c_i\right)$ to the opponent F

with probability $\min\left(1, \frac{D_\sigma^m(z_i)}{MD_{\sigma, Sk_{id||i}}^m(z_i)}\right)$. And store (id, i, M, sig) to list L4.

If *id* is the ℓ query, the execution steps are as follows: if $i^* < i \le T$, then C generates the corresponding digital signature as before. Otherwise, C terminates the operation.

Breaking queries: The adversary asks about the signature private key of a specific identity and time (*id*, *j*). If *id* is not in the ℓ query, C queries list L3 and provides the signature private key $SK_{id||j}$ at time *j* to opponent F. If *id* is the ℓ query and $j = i^*$, then C terminates the operation.

Forgery Phase: At this stage, adversary F outputs identity id^*, time t^*, message M^*, signature sig^*, and the forgery of adversary F is successful if and only if the following conditions are met simultaneously:

1) $\text{FSIBSVerify}_{mpk}(id^*, i^*, M^*, sig^*) = 1, 1 \le i^* < j$;

2) The adversary F has never asked about the identity id^*;

3) Rival F has never signed (id^*, i^*, M^*).

Once the adversary F outputs the forged digital signature, C performs the following steps:

First check whether id^* is the ℓ query, and check whether $t^* = i^*$ holds. If any of the conditions are not met, C terminates the operation.

The SIS problem that Algorithm C hopes to solve is to find a non-zero vector $x \in Z^m$ that satisfies $\|x\| \le (4\sigma + 2s\lambda)\sqrt{m}$ so that $Ax = 0 \pmod q$. C calls opponent F again and runs the above simulation process again. According to the general bifurcation lemma [32], the adversary F outputs a new forged digital signature (c', z') about the identity id^* and the message M^* with a non-negligible probability. Make $c^* \ne c'$, and $A_{id||i} z^* - H_1(id \,||\, i) c^* = A_{id||i} z' - H_1(id \,||\, i) c'$. Substituting $H_1(id \,||\, i) = A_{id||i} \cdot SK_{id||i}$ into the above formula, and combining similar terms, we can get:

$$\begin{aligned} & A_{id||i} z^* - H_1(id \,||\, i) c^* - A_{id||i} z' + H_1(id \,||\, i) c' \\ & = A_{id||i}\left(z^* - z' + SK_{id||i} c' - SK_{id||i} c^*\right) = 0 \end{aligned}$$

According to the legality of the signature, we know that $\|z^*\|$, $\|z'\| \le 2\sigma\sqrt{m}$. At the same time, according to the above simulation parameter generation process, we also know that $\|SK_{id||i} c'\|$, $\|SK_{id||i} c^*\| \le s\lambda\sqrt{m}$ holds with overwhelming probability.

Obviously, if $\|z^* - z' + SK_{id||i} c' - SK_{id||i} c^*\| \ne 0$, we get one of the above SIS problems solution. Therefore, we need to prove that the probability of $z^* - z' + SK_{id||i} c' - SK_{id||i} c^* \ne 0$ is not negligible.

Because $c^* \ne c'$, there is $c_i^* \ne c_i'$. In addition, according to the minimum entropy property of the original image given in the literature [32]. We know that there is a high probability that there is a signature private key $SK_{id||i}^*$, so that in addition to the *i*-th column, $SK_{id||i}^*$ and $SK_{id||i}$ is exactly the same. And $A_{id||i} SK_{id||i} = A_{id||i} SK_{id||i}^*$.

Table 1. Scheme performance comparison.

algorithm	UPK	USK	Signature length
[23]	$2mn\log q$	$4m^2\log q$	$2m\log q$
[31]	$mn\log q$	$m^2\log q$	$m\log q$
This article scheme	$mn\log q$	$mk\log q$	$m\log 12\sigma$

Because $z^* - z' + SK^*_{id\|\|i}\left(c' - c^*\right) - \left(z^* - z' + SK_{id\|\|i}\left(c' - c^*\right)\right) = \left(SK^*_{id\|\|i} - SK_{id\|\|i}\right)\left(c' - c^*\right) \neq 0$. Therefore, if $z^* - z' + SK^*_{id\|\|i}\left(c' - c^*\right) = 0$, then $z^* - z' + SK_{id\|\|i}\left(c' - c^*\right) \neq 0$ must be true. In addition, we know that the signature keys $SK^*_{id\|\|i}$ and $SK_{id\|\|i}$ play exactly the same role in the simulation process. Therefore, the adversary F does not know which signature key algorithm C uses in the simulation process. Therefore, $\Pr\left[z^* - z' + SK_{id\|\|i}\left(c' - c^*\right) \neq 0\right] \geq 0.5$, and we have completed the proof of the theorem.

Here we compare with the classic algorithm in literature [22] [23], in which literature [22] constructs the first identity-based forward secure digital signature algorithm on the grid. Literature [23] proposed the most famous lattice identity-based hierarchical identity signature algorithm so far. Define UPK as the size of the user's public key, and USK as the size of the user's private key. The bit length of the elements in Z_q is expressed as $\log q$. In these algorithms, the master public key and the master private key are respectively $Z_q^{n\times m}$, $Z_q^{m\times m}$, and no more comparison between them. **Table 1** shows the performance comparison between the programs.

According to the definition 2.5, we know that $k < n \leq m$, so the signature private key and signature length in our scheme are smaller than those in [22] [23]. In addition, the cumbersome Samplepre algorithm and lattice delegation technology used in the literature [22] require large calculation, communication, and storage costs, and are less efficient. Therefore, our program has certain advantages.

6. Conclusion

This paper combines Lyubashevsky [31]'s trap-free signature and extended pre-image sampling function technology to design an efficient (FSIBS) scheme. Under the random oracle model, the hypothesis based on small integers to solve difficult problems proves that our scheme is unforgeable against adaptive selection identity and adaptive selection message attacks, without the cumbersome Samplepre algorithm and lattice delegation technology. Compared with the existing scheme, the signature private key and signature length are shorter, which has certain practicability. How to extend our program to the standard model is our next research goal.

Acknowledgements

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped improve the quality of the paper. This work is supported by the National Natural Science Foundation of China (No. 6206070270).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Shamir, A. (1984) Identity-Based Cryptosystems and Signature Schemes. In: *Proceedings of Workshop on the Theory and Application of Cryptographic Techniques*, Springer Press, Paris, 47-53. https://doi.org/10.1007/3-540-39568-7_5

[2] Hess, F. (2002) Efficient Identity Based Signature Schemes Based on Pairings. In: *Proceedings of International Workshop on Selected Areas in Cryptography*, Springer Press, Newfoundland, 310-324. https://doi.org/10.1007/3-540-36492-7_20

[3] Yi, X. (2003) An Identity-Based Signature Scheme from the Weil Pairing. *IEEE Communications Letters*, **7**, 76-78. https://doi.org/10.1109/LCOMM.2002.808397

[4] Barreto, P.S.L.M., Libert, B., McCullagh, N., *et al.* (2005) Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps. In: *Proceedings of International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Chennai, 515-532. https://doi.org/10.1007/11593447_28

[5] Chai, Z., Cao, Z. and Dong, X. (2007) Identity-Based Signature Scheme Based on Quadratic Residues. *Science in China Series F: Information Sciences*, **50**, 373-380. https://doi.org/10.1007/s11432-007-0038-1

[6] Xiong, H., Hu, J., Chen, Z., *et al.* (2011) On the Security of an Identity Based Multi-Proxy Signature Scheme. *Computers & Electrical Engineering*, **37**, 129-135. https://doi.org/10.1016/j.compeleceng.2011.01.006

[7] Yang, P., Cao, Z. and Dong, X. (2011) Fuzzy Identity Based Signature with Applications to Biometric Authentication. *Computers & Electrical Engineering*, **37**, 532-540. https://doi.org/10.1016/j.compeleceng.2011.04.013

[8] Shor, P.W. (1999) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*, **41**, 303-332. https://doi.org/10.1137/S0036144598347011

[9] Ajtai, M. (1996) Generating Hard Instances of Lattice Problems. In: *Proceedings* of *the* 28*th Annual ACM Symposium on Theory of Computing*, ACM Press, New York City, 99-108. https://doi.org/10.1145/237814.237838

[10] Lyubashevsky, V. and Micciancio, D. (2008) Asymptotically Efficient Lattice-Based Digital Signatures. In: *Proceedings of Theory of Cryptography Conference*, ACM Press, New York, 37-54. https://doi.org/10.1007/978-3-540-78524-8_3

[11] Gentry, C., Peikert, C. and Vaikuntanathan, V. (2008) Trapdoors for Hard Lattices and New Cryptographic Constructions. In: *Proceedings of the* 40*th Annual ACM Symposium on Theory of Computing*, ACM Press, Victoria, 197-206. https://doi.org/10.1145/1374376.1374407

[12] Cash, D., Hofheinz, D., Kiltz, E., *et al.* (2010) Bonsai Trees, or How to Delegate a Lattice Basis. In: *Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer Press, Tallinn, 523-552. https://doi.org/10.1007/978-3-642-13190-5_27

[13] Agrawal, S., Boneh, D. and Boyen, X. (2010) Efficient Lattice (H) IBE in the Standard Model. In: *Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer Press, Tallinn, 553-572. https://doi.org/10.1007/978-3-642-13190-5_28

[14] Gentry, C. (2009) Fully Homomorphic Encryption Using Ideal Lattices. In: *Proceedings of the* 51*st Annual ACM Symposium on Theory of Computing*, ACM Press, Phoenix, 169-178. https://doi.org/10.1145/1536414.1536440

[15] Anderson, R. (1997) Two Remarks on Public Key Cryptology (Invited Lecture). In: *Proceedings of the ACM Conference on Computer and Communications*, ACM Press, Zurich, 135-147.

[16] Bellare, M. and Miner, S.K. (1999) A Forward-Secure Digital Signature Scheme. In: *Proceedings of Annual International Cryptology Conference*, Spring Press, Santa Barbara, 431-448. https://doi.org/10.1007/3-540-48405-1_28

[17] Yu, J., Kong, F., Cheng, X., *et al.* (2011) Forward-Secure Identity-Based Public-Key Encryption without Random Oracles. *Fundamenta Informaticae*, **111**, 241-256. https://doi.org/10.3233/FI-2011-562

[18] Chen, X., Zhang, F., Tian, H., *et al.* (2011) Discrete Logarithm Based Chameleon Hashing and Signatures without Key Exposure. *Computers & Electrical Engineering*, **37**, 614-623. https://doi.org/10.1016/j.compeleceng.2011.03.011

[19] Liu, Y., Yin, X. and Qiu, L. (2008) ID-Based Forward-Secure Signature Scheme from the Bilinear Pairings. In: *Proceedings of International Symposium on Electronic Commerce and Security*, IEEE Press, Guangzhou, 179-183. https://doi.org/10.1109/ISECS.2008.220

[20] Yu, J., Hao, R., Kong, F., *et al.* (2011) Forward-Secure Identity-Based Signature: Security Notions and Construction. *Information Sciences*, **181**, 648-660. https://doi.org/10.1016/j.ins.2010.09.034

[21] Al Ebri, N., Baek, J., Shoufan, A., *et al.* (2013) Forward-Secure Identity-Based Signature: New Generic Constructions and Their Applications. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, **4**, 32-54.

[22] Zhang, X., Xu, C., Jin, C., *et al.* (2014) Efficient Forward Secure Identity-Based Shorter Signature from Lattice. *Computers & Electrical Engineering*, **40**, 1963-1971. https://doi.org/10.1016/j.compeleceng.2013.12.003

[23] Rückert, M. (2010) Strongly Unforgeable Signatures and Hierarchical Identity-Based Signatures from Lattices without Random Oracles. In: *Proceedings of International Workshop on Post-Quantum Cryptography*, Springer Press, Darmstadt, 182-200. https://doi.org/10.1007/978-3-642-12929-2_14

[24] Agrawal, S., Boneh, D. and Boyen, X. (2010) Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE. In: *Proceedings of Annual Cryptology Conference*, Springer, Press, Santa Barbara, 98-115. https://doi.org/10.1007/978-3-642-14623-7_6

[25] Goldreich, O., Goldwasser, S. and Micali, S. (1984) On the Cryptographic Applications of Random Functions. In: *Proceedings of Workshop on the Theory and Application of Cryptographic Techniques*, Springer Press, Paris, 276-288. https://doi.org/10.1007/3-540-39568-7_22

[26] Fiat, A. and Shamir, A. (1986) How to Prove Yourself: Practical Solutions to Identi-

fication and Signature Problems. In: *Proceedings of Conference on the Theory and Application of Cryptographic Techniques*, Springer Press, Saragossa, 186-194. https://doi.org/10.1007/3-540-47721-7_12

[27] Bellare, M. and Rogaway, P. (1993) Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols. In: *Proceedings of the* 1*st ACM Conference on Computer and Communications Security*, ACM Press, Fairfax, 62-73. https://doi.org/10.1145/168588.168596

[28] Micciancio, D. and Regev, O. (2007) Worst-Case to Average-Case Reductions Based on Gaussian Measures. *SIAM Journal on Computing*, **37**, 267-302. https://doi.org/10.1137/S0097539705447360

[29] Alwen, J. and Peikert, C. (2011) Generating Shorter Bases for Hard Random Lattices. *Theory of Computing Systems*, **48**, 535-553. https://doi.org/10.1007/s00224-010-9278-3

[30] Tian, M. and Huang, L. (2013) Lattice-Based Message Recovery Signature Schemes. *International Journal of Electronic Security and Digital Forensics*, **5**, 257-269. https://doi.org/10.1504/IJESDF.2013.058658

[31] Lyubashevsky, V. (2012) Lattice Signatures without Trapdoors. In: *Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer Press, Minneapolis, 738-755. https://doi.org/10.1007/978-3-642-29011-4_43

[32] Bellare, M. and Neven, G. (2006) Multi-Signatures in the Plain Public-Key Model and a General Forking Lemma. In: *Proceedings of the* 13*th ACM Conference on Computer and Communications Security*, ACM Press, Taiwan, 390-399. https://doi.org/10.1145/1180405.1180453