Research Article

A Fuzzy Identity-Based Signature Scheme from Lattices in the Standard Model

Chunli Yang,^{1,2} Shihui Zheng,^{1,2} Licheng Wang,^{1,2} Miaomiao Tian,³
Lize Gu,^{1,2} and Yixian Yang^{1,2}

¹ National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, P.O. Box 126, Beijing 100876, China

² Information Security Center, Beijing University of Posts and Telecommunications, P.O. Box 126, Beijing 100876, China

³ School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China

Correspondence should be addressed to Shihui Zheng; shihuizh@gmail.com

Received 14 May 2014; Revised 24 July 2014; Accepted 28 July 2014; Published 14 August 2014

Academic Editor: Antonina Pirrotta

Copyright © 2014 Chunli Yang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A fuzzy identity-based signature (FIBS) scheme allows a user with identity ID to issue a signature that could be verified with identity ID' if and only if ID and ID' lie within a certain distance. To obtain an FIBS scheme that can resist known quantum attacks, we use the double-trapdoor technique from ABB10a for secret key extracting and the vanishing trapdoor technique from Boyen10 for message signing. In addition, in order to reflect the functionality of fuzziness, Shamir secret sharing scheme is also used in our construction. In this paper, we propose an FIBS scheme from lattices and prove that this new scheme achieves strong unforgeability under selective chosen-identity and adaptive chosen-message attacks (SU-sID-CMA) in the standard model. To the best of our knowledge, our scheme is not only the first FIBS scheme from lattices without random oracles but also the first FIBS scheme that achieves strong unforgeability.

1. Introduction

In order to overcome certificates management problem in traditional public key cryptography, Shamir first put forward the concept of identity-based public key cryptography [1] in 1985; that is, the public key of an identity can be easily computed from his identity information. The first efficient and secure identity-based public key encryption (IBE) scheme was given by Boneh and Franklin in [2]. However, identity string for each identity is not unique, while biometric characteristics (e.g., fingerprints, faces, irises, etc.) are unique. Therefore, identity's biometric characteristics can be used as public keys. Biometric keys have many advantages: hard to guess, forget, copy, share, and forge. However, biometric measurements are noisy, and there are many different measurements to the same biometric.

Sahai and Waters first introduced the concept of fuzzy identity-based encryption (FIBE) [3] in 2005. In an FIBE scheme, a user using the secret key, which the identity ID

described as an attribute set att , can decrypt a ciphertext encrypted with the public key att' if and only if att and att' lie within a certain distance judged by some metric. Thus, an FIBE scheme involves an error tolerance parameter between the identities. In 2007, Baek et al. [4] put forward two FIBE schemes; these new schemes provided public parameters whose size was independent of the number of attributes in each identity and had beautiful structures, which made the key extraction and encryption more efficient than the scheme [3]. In [5], Goyal et al. showed that FIBE can also be regarded as a type of application of attribute based encryption (ABE).

Yang et al. [6] first introduced the concept of fuzzy identity-based signature (FIBS) and constructed an FIBS scheme based on scheme [3]. A fuzzy identity-based signature (FIBS) scheme allows a user with identity ID to issue a signature that could be verified with identity ID' if and only if ID and ID' lie within a certain distance judged by some metric. A number of FIBS schemes have been put forward in recent years, such as [7–11]. However, all of these schemes

not only are based on hard number theoretical problems (e.g., integer factorization, discrete logarithm, and bilinear pairings), which are vulnerable to quantum computer attacks [12], but also achieved existential unforgeability. Existential unforgeability is only a basic requirement for a signature scheme; it means that an adversary is allowed to forge a new different signature of the same message. Strong unforgeability means that it prevents forging of signatures on messages that could have been signed previously. Cryptologists prefer to design digital signature schemes that can achieve strong unforgeability.

In recent years, lattice-based cryptographic systems have attained a great interest for postcryptology, as the systems have the ability to resist the known quantum analysis (e.g., Shor algorithm analysis [12]). Furthermore, the systems also enjoy great promise because of having a very strong security proof based on worst-case hardness, relatively efficient implementations, and great simplicity due to the structure and linearity of lattices. Many cryptographic schemes are based on the learning with errors (LWE) problem and small integer solution (SIS) problem, for example, public key encryption schemes [13, 14], digital signatures [15, 16], identity-based encryption [17, 18], fully homomorphic encryption [19, 20], and so on.

Meanwhile, researchers are always concerned with fuzzy identity-based signature (FIBS) scheme from lattices. An FIBS scheme from lattices was first proposed by Yao and Li [21] in 2013. The paper pointed out the defect of security model in [6] and put forward a more reasonable security model for FIBS scheme. In addition, authors also presented an FIBS scheme based on the SIS problem hardness assumption. However, the scheme could only achieve the standard of existentially unforgeable against adaptively chosen message and identity (EU-ACMIA) attacks in the random oracles. However, considering Canetti's critical statement on provable security reduction based on random oracles [22] and the risk of random oracle model [23], it is a meaningful and relatively safe direction to design cryptographic schemes that are not in the random oracle model.

Based on the security model of [21], we use the double-trapdoor technique from ABB10a for secret key extracting, the vanishing trapdoor technique from Boyen10 for message signing, and Shamir secret sharing scheme [24]. We propose a new FIBS scheme that achieves strong unforgeability against selective chosen-identity and adaptive chosen-message attacks (SU-sID-CMA) in the standard model. To the best of our knowledge, our scheme is the first FIBS scheme from lattices without random oracles and achieves strong unforgeability.

The rest of this paper is organised as follows. In Section 2, we introduce some preliminaries about SIS problem and some algorithms that will be used in our construction and security proof. The model of FIBS and security notations are given in Section 3. In Section 4, we present our main result that is an FIBS scheme from SIS. The security proof and parameters analysis are presented in Section 5. We give the performance analysis and simulations in Section 6. In Section 7, we present the conclusions and open problem for the future.

2. Preliminaries

2.1. Notation. We denote the set of integers and real numbers by $\mathbb{Z}$ and $\mathbb{R}$, respectively. For a positive integer n , $[n]$ denotes the set $\{1, 2, \dots, n\}$. The vectors are denoted by lower-case bold letters (e.g., $\mathbf{x}$), matrices by upper-case bold letters (e.g., $\mathbf{A}$), and the Gram-Schmidt orthogonalization of $\mathbf{A}$ by $\tilde{\mathbf{A}}$. We write $\|\mathbf{x}\|$ for the Euclidean norm of $\mathbf{x}$ and $\|\mathbf{X}\| = \max_i \|\mathbf{x}_i\|$ for the length of a matrix $\mathbf{X}$. We use standard O , o for denoting the growth of functions. The notation $\text{poly}(n)$ denotes a function $f(n) = O(n^c)$ for some constant c . $\text{negl}(n)$ denotes some unspecified function $f(n)$ such that $f(n) = o(n^{-c})$ for constant c , and describing such a function is negligible. We also describe that a probability is overwhelming if it is $1 - \text{negl}(n)$. The base of logarithm function is 2.

2.2. Lattice and Small Integer Solution (SIS) Problem

Definition 1 (see [25]). An n -dimensional lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$. Formally, let $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ consist of n linearly independent vectors. The lattice generated by $\mathbf{B}$ is

$$\Lambda = \mathcal{L}(\mathbf{B}) = \left\{ \mathbf{B}\mathbf{x} = \sum_{i=1}^n x_i \mathbf{b}_i \mid \mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{Z}^n \right\}. \quad (1)$$

Here $\mathbf{B}$ is called a basis for the lattice $\Lambda = \mathcal{L}(\mathbf{B})$.

For any basis $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$, let $\tilde{\mathbf{B}} = \{\tilde{\mathbf{b}}_1, \tilde{\mathbf{b}}_2, \dots, \tilde{\mathbf{b}}_n\}$ denote its Gram-Schmidt orthogonalization of basis $\mathbf{B}$. It is iteratively defined as follows: $\tilde{\mathbf{b}}_1 = \mathbf{b}_1$, and $\tilde{\mathbf{b}}_i$ is the component of $\mathbf{b}_i$ orthogonal to $\text{span}(\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_{i-1})$ for $i = 2, 3, \dots, n$.

Definition 2 (see [25]). Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ for some q , m, n , its q -ary lattice is defined as follows:

$$\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} = \mathbf{0} \bmod q\}. \quad (2)$$

We also define the coset for any $\mathbf{y} \in \mathbb{Z}_q^n$ that is generated by the columns of $\mathbf{A}$ as

$$\Lambda_q^\mathbf{y}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} = \mathbf{y} \bmod q\}. \quad (3)$$

Definition 3 (see [26]). Given any vector $\mathbf{c}$ and real $s > 0$, a Gaussian function on $\mathbb{R}^n$ centered at $\mathbf{c}$ with parameter s is defined by

$$\rho_{s,\mathbf{c}}(\mathbf{x}) = e^{-\pi\|\mathbf{x}-\mathbf{c}\|^2/s^2}. \quad (4)$$

For any vector $\mathbf{c}$, real $s > 0$, and n -dimensional lattice Λ , the discrete Gaussian distribution over Λ is defined as follows:

$$\forall \mathbf{x} \in \Lambda, \quad \mathcal{D}_{\Lambda,s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}, \quad (5)$$

where $\rho_{s,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x} \in \Lambda} \rho_{s,\mathbf{c}}(\mathbf{x})$.

Definition 4 (small integer solution (SIS) problem [26]). Given an integer q , a real $\beta > 0$, and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$,

the goal of $\text{SIS}_{n,m,q,\beta}$ is to find a vector $\mathbf{z} \in \mathbb{Z}^m$ for satisfying $\mathbf{z} \in \Lambda_q^\perp(\mathbf{A}) \setminus \{0\}$ and $\|\mathbf{z}\| \leq \beta$, where $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} = \mathbf{0} \bmod q\}$.

Proposition 5 (hardness of SIS problem [26]). *Given security parameter n , any poly-bounded m , $\beta = \text{poly}(n)$, and any prime $q \geq \beta \cdot \omega(\sqrt{n \log n})$, the average-case problem $\text{SIS}_{n,m,q,\beta}$ is as hard as approximating the SIVP problem in the worst case to within certain $\gamma = \beta \cdot \tilde{O}(\sqrt{n})$ factors.*

2.3. Some Algorithms. We recall some algorithms for our construction and security proof later.

Lemma 6 (see [27]). *Let $q \geq 3$ be odd and $m = \lceil 6n \log q \rceil$. There is a probabilistic polynomial time algorithm $\text{TrapGen}(q, n)$ that outputs a pair $(\mathbf{A} \in \mathbb{Z}_q^{n \times m}, \mathbf{T}_\mathbf{A} \in \mathbb{Z}^{m \times m})$ such that $\mathbf{A}$ is statistically close to a uniform matrix in $\mathbb{Z}_q^{n \times m}$ and $\mathbf{T}_\mathbf{A}$ is a basis for $\Lambda_q^\perp(\mathbf{A})$ satisfying*

$$\|\tilde{\mathbf{T}}_\mathbf{A}\| \leq O(\sqrt{n \log q}), \quad \|\mathbf{T}_\mathbf{A}\| \leq O(n \log q) \quad (6)$$

with all but negligible probability in n .

For simplicity, we let $L = O(\sqrt{n \log q})$ denote the maximum Gram-Schmidt norm of a basis produced by $\text{TrapGen}(q, n)$.

Lemma 7 (see [15, 26]). *Let $q \geq 2$ and $\mathbf{A}$ be a matrix in $\mathbb{Z}_q^{n \times m}$ with $m > n$. Let $\mathbf{T}_\mathbf{A}$ be a basis for $\Lambda_q^\perp(\mathbf{A})$ and $\sigma \geq \|\tilde{\mathbf{T}}_\mathbf{A}\| \omega(\sqrt{\log m})$. Then for any $\mathbf{u} \in \mathbb{Z}_q^n$,*

- (1) $\Pr[\mathbf{x} \sim \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), \sigma} : \|\mathbf{x}\| > \sigma \sqrt{m}] \leq \text{negl}(n)$;
- (2) *there is a probabilistic polynomial time algorithm $\text{SamplePre}(\mathbf{A}, \mathbf{T}_\mathbf{A}, \mathbf{u}, \sigma)$ that returns $\mathbf{x} \in \Lambda_q^\perp(\mathbf{A})$ sampled from a distribution statistically close to $\mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), \sigma}$.*

Lemma 8 (see [18]). *Let $q > 2$, $m > n$, and $\sigma > \|\tilde{\mathbf{T}}_\mathbf{B}\| s_\mathbf{R} \omega(\sqrt{\log m})$. There exists a polynomial time algorithm $\text{SampleRight}(\mathbf{A}, \mathbf{B}, \mathbf{R}, \mathbf{T}_\mathbf{B}, \mathbf{u}, \sigma)$ that takes a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times k}$, a rank n matrix $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$, a matrix $\mathbf{R} \in \mathbb{Z}^{k \times m}$, and a short basis $\mathbf{T}_\mathbf{B}$ of $\Lambda_q^\perp(\mathbf{B})$ as inputs and outputs a vector $\mathbf{e} \in \mathbb{Z}^{m+k}$ distributed statistically close to $\mathcal{D}_{\Lambda_q^\perp(\mathbf{F}_2), \sigma}$, where $\mathbf{F}_2 := \mathbf{A}(\mathbf{A}\mathbf{R} + \mathbf{B})$ and $s_\mathbf{R} := \|\mathbf{R}\| = \sup_{\|\mathbf{x}\|=1} \|\mathbf{R}\mathbf{x}\|$.*

Lemma 9 (see [18]). *There exists a polynomial time algorithm $\text{SampleBasisLeft}(\mathbf{A}, \mathbf{M}, \mathbf{T}_\mathbf{A}, 0, \sigma)$ that takes a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m_1}$, a matrix $\mathbf{M} \in \mathbb{Z}_q^{n \times m_2}$, and a short basis $\mathbf{T}_\mathbf{A}$ of $\Lambda_q^\perp(\mathbf{A})$ as inputs and outputs a basis $\mathbf{T}_{\mathbf{F}_1}$ of $\Lambda_q^\perp(\mathbf{F}_1)$ with $\sigma > \|\tilde{\mathbf{T}}_\mathbf{A}\| \omega(\sqrt{\log(m_1 + m_2)})$ and $\|\tilde{\mathbf{T}}_{\mathbf{F}_1}\| = \|\tilde{\mathbf{T}}_\mathbf{A}\|$, where $\mathbf{F}_1 := \mathbf{A}\mathbf{M}$.*

Lemma 10 (see [18]). *There exists a polynomial time algorithm $\text{SampleBasisRight}(\mathbf{A}, \mathbf{B}, \mathbf{R}, \mathbf{T}_\mathbf{B}, 0, \sigma)$ that takes matrices $\mathbf{A} \in \mathbb{Z}_q^{n \times k}$, $\mathbf{M} \in \mathbb{Z}_q^{n \times m}$, and $\mathbf{R} \in \{1, -1\}^{k \times m}$ and a short basis $\mathbf{T}_\mathbf{B}$ of $\Lambda_q^\perp(\mathbf{B})$ as inputs and outputs a basis $\mathbf{T}_{\mathbf{F}_2}$ of $\Lambda_q^\perp(\mathbf{F}_2)$ with $\sigma > \|\tilde{\mathbf{T}}_\mathbf{B}\| s_\mathbf{R} \omega(\sqrt{\log(m)})$ and $\|\tilde{\mathbf{T}}_{\mathbf{F}_2}\| \leq \|\tilde{\mathbf{T}}_\mathbf{B}\| (s_\mathbf{R} + 1)$, where $\mathbf{F}_2 := \mathbf{A}(\mathbf{A}\mathbf{R} + \mathbf{B})$.*

3. The Model of FIBS

We recall the notation of FIBS scheme and security model from [21] in this section. A fuzzy identity-based signature scheme consists of four algorithms as follows.

- (i) *Setup*(1^n): this probabilistic algorithm takes a security parameter 1^n as an input and outputs the public parameters PP that contain an error tolerance parameter d and master key MK.
- (ii) *Extract*(MK, ID): this probabilistic algorithm takes the master key MK and an identity ID as inputs and outputs a secret key sk_{ID} for identity ID.
- (iii) *Sign*(PP, sk_{ID} , μ): this probabilistic algorithm takes public parameters PP, a private key sk_{ID} associated with ID, and a message μ as inputs and outputs the signature $\sigma_{\text{ID}, \mu}$ on message μ for identity ID.
- (iv) *Verify*(ID', μ , $\sigma_{\text{ID}, \mu}$): this deterministic algorithm takes identity ID' such that $|\text{ID} \cap \text{ID}'| \geq d$, the message μ , and the corresponding signature $\sigma_{\text{ID}, \mu}$ as inputs and returns a bit b , where $b = 1$ means that the signature is valid.

For correctness purposes, for any fixed ID, and arbitrary ID' such that $|\text{ID} \cap \text{ID}'| \geq d$, it holds that

$$\Pr[\text{Verify}(\text{ID}', \mu, \text{Sign}(\text{sk}_{\text{ID}}, \mu)) = 1] = 1 - \text{negl}(n). \quad (7)$$

We consider the security model of FIBS scheme as strong unforgeable against selective chosen-identity and adaptive chosen-message attacks (SU-sID-CMA). Strong unforgeability under adaptive chosen message attacks (SU-CMA) is stronger than existential unforgeability (EU-CMA) in the sense that the adversary is not restricted by the security model artificially. In EU-CMA, the adversary is only allowed to output a signature for a fresh message $m^* \neq m_i$, where the signature of m_i was known by adversary, while, the SU-CMA adversary is also allowed to output a fresh signature for one of the m_i .

Let $\mathcal{A}$ be an adversary assumed to be a probabilistic turing machine taking a security parameter n as an input. Consider the following game in which $\mathcal{A}$ interacts with a challenger $\mathcal{C}$.

- (i) *Init*: the adversary $\mathcal{A}$ declares the target identity $\text{ID}^* = (\text{id}_1^*, \text{id}_2^*, \dots, \text{id}_l^*)$.
- (ii) *Setup*: the challenger $\mathcal{C}$ runs the *Setup* phase of the algorithm and tells the public parameters to adversary $\mathcal{A}$.
- (iii) *Queries*: the adversary $\mathcal{A}$ launches a number of different queries for the challenger $\mathcal{C}$.

- (1) *Extract query*: the adversary $\mathcal{A}$ issues private key queries for any identities η_i , where $|\eta_i \cap \text{ID}^*| < d$.
- (2) *Sign query*: the adversary $\mathcal{A}$ can ask for the signature of any identities η_i on any message μ .

- (iv) *Forgery*: the adversary $\mathcal{A}$ outputs $(\text{ID}^*, \mu^*, \sigma_{\text{ID}^*, \mu^*})$. $\mathcal{A}$ succeeds if the following conditions hold:

- (1) *Verify*: $(ID^*, \mu^*, \sigma_{ID, \mu^*}) = 1$;
- (2) for any tuple $(ID, \mu, \sigma_{ID, \mu})$ that is generated during the Sign queries, we have (a) $|ID^* \cap ID| \geq d$ and $\mu \neq \mu^*$ or (b) $|ID^* \cap ID| < d$.

We define $\mathcal{A}'$'s success probability by

$$\text{Adv}_{\text{FIBS}, \mathcal{A}'}^{\text{SU-sID-CMA}}(n) = \Pr \left[\left(\text{Verify}(ID^*, \mu^*, \sigma_{ID, \mu^*}) \right) = 1 \right]. \quad (8)$$

A fuzzy identity-based signature (FIBS) scheme is said to be SU-sID-CMA secure if $\text{Adv}_{\text{FIBS}, \mathcal{A}'}^{\text{SU-sID-CMA}}(n)$ is negligible in the security parameter n .

More stronger security model, strong unforgeability against adaptive chosen-identity and adaptive chosen-message attacks (SU-aID-CMA), can be obtained from SU-sID-CMA by a generic transformation that uses Chameleon hash function [28].

4. The FIBS Construction

Our construction is made of four algorithms as follows. In Section 5.1, we will further analyse the parameters.

- (i) *Setup*(1^n): this is a probabilistic algorithm that takes security parameter n as an input and sets the parameters $(l, d, k, q, m, s_1, s_2)$, where l is the identity size, d ($d < l$) is the error tolerance parameters, k is the length of message, $q = \text{poly}(n)$ is a prime, $m > 6n \log q$ is the dimension of lattice, and s_1 and s_2 are Gaussian parameters; then the algorithm performs the following steps.

- (1) Use algorithm *TrapGen* for generating matrices $\mathbf{A}_{i,b} \in \mathbb{Z}_q^{n \times m}$ and corresponding trapdoors $\mathbf{S}_{i,b} \in \mathbb{Z}^{m \times m}$, where $i \in [l]$, $b \in \{0, 1\}$, and $\|\tilde{\mathbf{S}}_{i,b}\| \leq O(\sqrt{n \log q}) = L$.
- (2) Select uniformly random matrices $\mathbf{B}_i, \mathbf{C}_i$ from $\mathbb{Z}_q^{n \times m}$, where $i \in [l]$. Draw $k + 1$ independent matrices $\mathbf{D}_j$ from $\mathbb{Z}_q^{n \times m}$ for $j \in \{0, 1, 2, \dots, k\}$. Select a random nonzero vector $\mathbf{y} \in \mathbb{Z}_q^n$.
- (3) Let $H : \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q^{n \times n}$ be the full rank differences map as defined in [18].
- (4) Output public parameters $\text{PP} = (\{\mathbf{A}_{i,b}\}_{i \in [l], b \in \{0, 1\}}, \{\mathbf{B}_i\}_{i \in [l]}, \{\mathbf{C}_i\}_{i \in [l]}, \{\mathbf{D}_j\}_{j \in \{0, 1, 2, \dots, k\}}, \mathbf{y}, H)$ and master secret key $\text{MK} = (\{\mathbf{S}_{i,b}\}_{i \in [l], b \in \{0, 1\}})$.

- (ii) *Extract*(MK, ID): this is a probabilistic algorithm that takes the master key MK and an identity $\text{ID} = (\text{id}_1, \text{id}_2, \dots, \text{id}_l) \in \{0, 1\}^l$ as inputs and then performs the following steps.

- (1) Call algorithm $\mathbf{S}'_{i, \text{id}_i} \leftarrow \text{SampleBasisLeft}(\mathbf{A}_{i, \text{id}_i}, \mathbf{B}_i + H(\text{ID}, \text{id}_i, i)\mathbf{C}_i, \mathbf{S}_{i, \text{id}_i}, 0, s_1)$ for all $i \in [l]$ (the id_i can be first expanded to $\{0, 1\}^*$, hashing it to $\mathbb{Z}_q^n$ using a collision resistant hash). Let $\mathbf{F}_{i, \text{id}_i} = \mathbf{A}_{i, \text{id}_i} \|\mathbf{B}_i + H(\text{ID}, \text{id}_i, i)\mathbf{C}_i$; then $\mathbf{F}_{i, \text{id}_i} \mathbf{S}'_{i, \text{id}_i} = 0 \pmod{q}$.

- (2) Output the secret key $\text{sk}_{\text{ID}} = (\mathbf{S}'_{1, \text{id}_1}, \mathbf{S}'_{2, \text{id}_2}, \dots, \mathbf{S}'_{l, \text{id}_l})$ for identity ID .

- (iii) *Sign*($\text{PP}, \text{sk}_{\text{ID}}, \mu$): this is a probabilistic algorithm that takes public parameters PP , a private key sk_{ID} associated with ID , and a message μ as inputs and then performs the following steps.

- (1) For every coordinate of $\mathbf{y}$, construct l shares of $y_1, y_2, \dots, y_n$ independently using a Shamir secret-sharing scheme. Namely, for each $i \in [n]$, choose a uniformly random polynomial $p_i(x) \in \mathbb{Z}_q[x]$ of degree $d - 1$ such that $p_i(0) = y_i$. Construct the i th share vector $\hat{\mathbf{y}}_i = (p_1(i), p_2(i), \dots, p_n(i)) \in \mathbb{Z}_q^n$. Thus for all $I \subseteq [l]$ satisfying $|I| \geq d$, we can compute fractional Lagrangian coefficients L_i such that $\mathbf{y} = \sum_{i \in I} L_i \hat{\mathbf{y}}_i \pmod{q}$.
- (2) For message $\mu \in \{0, 1\}^k$, let $\mathbf{D}_\mu = \sum_{j=0}^k (-1)^{\mu[j]} \mathbf{D}_j \times \mathbf{D}_j$, where $\mu[0] = 0$.
- (3) For $i \in [l]$, randomly choose $\sigma_{i2} \leftarrow \mathbf{D}_{\mathbb{Z}^m, s_2, 0}$.
- (4) Run algorithm $\sigma_{i1} \leftarrow \text{SamplePre}(\mathbf{F}_{i, \text{id}_i}, \mathbf{S}'_{i, \text{id}_i}, \hat{\mathbf{y}}_i - \mathbf{D}_\mu \sigma_{i2}, s_2)$. Let $\sigma_i = (\sigma_{i1}, \sigma_{i2})$.
- (5) Output signature $\sigma_{\text{ID}, \mu} = (\mu, (\sigma_1, \sigma_2, \dots, \sigma_l), \text{ID})$.

- (iv) *Verify*($\text{ID}', \mu, \sigma_{\text{ID}, \mu}$): this is a deterministic algorithm that takes identity ID' , a message μ , and a signature $\sigma_{\text{ID}, \mu}$ as inputs and then performs the following steps.

- (1) Let $I \subseteq [l]$ denote the set of matching bits in ID and ID' .
- (2) If $|I| < d$, output $\perp$.
- (3) Otherwise, compute $\mathbf{F}_{i, \text{id}_i} = \mathbf{A}_{i, \text{id}_i} \|\mathbf{B}_i + H(\text{ID}, \text{id}_i, i)\mathbf{C}_i$ for all $i \in [l]$ and $\mathbf{D}_\mu = \sum_{j=0}^k (-1)^{\mu[j]} \mathbf{D}_j$. If (a) $\|\sigma_i\| \leq s_2 \sqrt{3m}$ for all $i \in [l]$ and (b) $\sum_{i \in I} L_i (\mathbf{F}_{i, \text{id}_i} \|\mathbf{D}_\mu\| \sigma_i) = \sum_{i \in I} L_i \hat{\mathbf{y}}_i = \mathbf{y}$, where $L_i = \prod_{i \in I, j \neq i} ((0 - j)/(i - j))$ is the corresponding fractional Lagrangian coefficient, then accept the signature $\sigma_{\text{ID}, \mu}$. Otherwise, reject the signature $\sigma_{\text{ID}, \mu}$.

Remark 11. In the verification equality, the only role of ID' is to compute the subset I . The $\mathbf{F}_{i, \text{id}_i}$ equals $\mathbf{A}_{i, \text{id}_i} \|\mathbf{B}_i + H(\text{ID}, \text{id}_i, i)\mathbf{C}_i$ instead of $\mathbf{A}_{i, \text{id}_i} \|\mathbf{B}_i + H(\text{ID}', \text{id}_i, i)\mathbf{C}_i$. This can be explained that the identity ID is a part of the signature $\sigma_{\text{ID}, \mu}$. Designing a more graceful scheme such that the verification equality needs neither ID nor ID' directly (like scheme based on pairing [6]) is our further research direction.

5. Correctness and Security

5.1. Correctness and Parameters. For proving the consistency of the scheme, we only consider the case $|I| < d$, where I is the matching bits set of ID and ID' . First, we give the correctness of our scheme.

According to Lemma 7, we know that, for every $i \in [l]$, $\|\sigma_{i1}\| \leq s_2 \sqrt{2m}$ and $\|\sigma_{i2}\| \leq s_2 \sqrt{m}$. Thus, $\|\sigma_i\| = \|\sigma_{i1}\| \leq \sqrt{\|\sigma_{i1}\|^2 + \|\sigma_{i2}\|^2} = s_2 \sqrt{3m}$.

On the other hand, for every $i \in [l]$, vector σ_{i1} satisfies $\mathbf{F}_{i,\text{id}_i} \sigma_{i1} = \hat{\mathbf{y}}_i - \mathbf{D}_\mu \sigma_{i2}$ from Lemma 7. In other words, $(\mathbf{F}_{i,\text{id}_i} \|\mathbf{D}_\mu\|)(\sigma_{i1}) = \hat{\mathbf{y}}_i$. Therefore, for subset I , $\sum_{i \in I} L_i (\mathbf{F}_{i,\text{id}_i} \|\mathbf{D}_\mu\|) \sigma_i = \sum_{i \in I} L_i \hat{\mathbf{y}}_i = \mathbf{y}$.

Secondly, for the scheme working correctly, we must satisfy the following conditions.

- (i) Algorithm *TrapGen* can operate, so $m \geq 6n \log q$.
- (ii) Algorithm *SampleBasisLeft* used in *Extract* phase can operate; that is, $s_1 \geq L\omega(\sqrt{\log(2m)})$, where $L = O(\sqrt{n \log q})$.
- (iii) Algorithm *SamplePre* used in *Sign* phase can operate; that is, $s_2 \geq L\omega(\sqrt{\log(2m)})$, where $L = O(\sqrt{n \log q})$.

Taking n as a security parameter, let δ satisfy $n^\delta > \lceil \log q \rceil = O(\log n)$. The parameters (m, s_1, s_2) are set as follows: $m = 6n^{1+\delta}$, $s_1 = s_2 = m\omega(\sqrt{\log(2m)})$.

5.2. Security

Theorem 12. *The FIBS scheme is SU-sID-CMA in the standard model under the hardness assumption SIS problem. Let $\mathcal{A}$ be an adversary that makes at most q_e extract queries and q_s signature queries and produces a successful forgery against our FIBS scheme with probability ϵ ; then there exists an algorithm $\mathcal{B}$ that solves the $\text{SIS}_{n,lm,q,\beta}$ problem with probability $\epsilon' \geq [(1/2)(1 - (1/3)^l) + (1/2)] \cdot (1/q) \cdot (1 - ((q_e + q_s)/q))\epsilon$, where $\beta = 2s_2 l \sqrt{m}(1 + 12\sqrt{2m})(1 + s_2 \sqrt{m(k+1)})$.*

Proof. We prove this theorem by playing the classical provable secure game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.

- (i) *Init*: let ID^* be the identity that $\mathcal{A}$ intends to attack. The challenger $\mathcal{C}$ is invoked on a random SIS instance $\mathbf{A} \in \mathbb{Z}_q^{n \times lm}$ and is asked to return an admissible solution $\mathbf{e}_0 \in \mathbb{Z}^{lm}$ such that $\mathbf{A}\mathbf{e}_0 = 0 \pmod{q}$ and $0 \neq \|\mathbf{e}_0\| \leq \beta$.
- (ii) *Setup*: the challenger $\mathcal{C}$ generates the public parameters PP as follows.
 - (a) Parse SIS instance $\mathbf{A}$ as matrix $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_l \in \mathbb{Z}_q^{n \times m}$, choose randomly l uniformly random matrices $\mathbf{A}'_1, \mathbf{A}'_2, \dots, \mathbf{A}'_l \in \mathbb{Z}_q^{n \times m}$.
 - (b) Let $\mathbf{A}_{i,\text{id}_i^*} = \mathbf{A}_i$, $\mathbf{A}_{i,1-\text{id}_i^*} = \mathbf{A}'_i$ for $i \in [l]$.
 - (c) Choose randomly l vectors $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_l$ from $\mathcal{D}_{\mathbb{Z}^m, s_2}$. Let $\hat{\mathbf{y}}_i = \mathbf{A}_{i,\text{id}_i^*} \mathbf{x}_i$ and regard $\hat{\mathbf{y}}_i$ as i th share vector of $\mathbf{y}$. According to Shamir secret-sharing scheme, there exist fractional Lagrangian coefficients L_i for recovering $\mathbf{y}$; that is, $\mathbf{y} = \sum_{i \in I} L_i \hat{\mathbf{y}}_i \pmod{q}$ for all $I \subseteq [l]$ satisfying $|I| \geq d$.

(d) Run the algorithm *TrapGen* for generating the matrices $\mathbf{C}_i, \mathbf{E}_i$ and corresponding trapdoors $\mathbf{S}_{\mathbf{C}_i}, \mathbf{S}_{\mathbf{E}_i}$. Let $\mathbf{R}_i$ be a $m \times m$ matrix chosen at random from $\{-1, 1\}^{m \times m}$ for $i \in [l]$, and let $\mathbf{R}'_j$ be a $2m \times m$ matrix sampling each column from $\mathcal{D}_{\mathbb{Z}^{2m}, s_2}$ for $j \in [k]$ independently.

(e) Pick k uniformly random scalars $h_1, h_2, \dots, h_k \in \mathbb{Z}_q$ and fix $h_0 = 1 \in \mathbb{Z}_q$. Set $\mathbf{B}_i = \mathbf{A}_{i,\text{id}_i} \mathbf{R}_i - H_1(\text{ID}^*, \text{id}_i^*, i) \mathbf{C}_i$ and $\mathbf{D}_j = \mathbf{F}_{i,\text{id}_i} \mathbf{R}'_j + h_j \mathbf{E}_i$, where $\mathbf{F}_{i,\text{id}_i} = \mathbf{A}_{i,\text{id}_i} \|\mathbf{B}_i + H(\text{ID}, \text{id}_i, i) \mathbf{C}_i$.

- (iii) *Extract queries*: the adversary $\mathcal{A}$ issues private key queries for any identity ID satisfying $|\text{ID} \cap \text{ID}^*| < d$. Considering a query for the private key of an identity ID , $\mathcal{C}$ does not know the master key $\{\mathbf{S}_{i,b}\}_{i \in [l], b \in \{0,1\}}$. For responding to a private key query for ID , the challenger uses the trapdoors $\mathbf{S}_{\mathbf{C}_i}$ to produce short basis for $\Lambda_q^\perp(\mathbf{F}_{i,\text{id}_i})$, where $\mathbf{F}_{i,\text{id}_i} = \mathbf{A}_{i,\text{id}_i} \|\mathbf{B}_i + H(\text{ID}, \text{id}_i, i) \mathbf{C}_i = \mathbf{A}_{i,\text{id}_i} \|\mathbf{A}_{i,\text{id}_i} \mathbf{R}_i + (H(\text{ID}, \text{id}_i, i) - H(\text{ID}^*, \text{id}_i^*, i)) \mathbf{C}_i$. For $|\text{ID} \cap \text{ID}^*| < d$, $H(\text{ID}, \text{id}_i, i) - H(\text{ID}^*, \text{id}_i^*, i)$ is nonsingular and therefore $\mathbf{S}_{\mathbf{C}_i}$ is also a trapdoor for $\Lambda_q^\perp(\mathbf{M}_{i,\text{id}_i})$, where $\mathbf{M}_{i,\text{id}_i} = (H(\text{ID}, \text{id}_i, i) - H(\text{ID}^*, \text{id}_i^*, i)) \mathbf{C}_i$. The challenger can now respond to the private key query by running $\mathbf{S}'_{i,\text{id}_i} \leftarrow \text{SampleBasisRight}(\mathbf{A}_{i,\text{id}_i}, \mathbf{M}_{i,\text{id}_i}, \mathbf{R}_i, \mathbf{S}_{\mathbf{C}_i}, 0, s_1)$ and sending $(\mathbf{S}'_{1,\text{id}_1}, \mathbf{S}'_{2,\text{id}_2}, \dots, \mathbf{S}'_{l,\text{id}_l})$ to the adversary $\mathcal{A}$.
- (iv) *Sign queries*: the adversary $\mathcal{A}$ asks signature for any identities on any message. Consider a query for a signature of ID on message μ .

(a) If $|\text{ID} \cap \text{ID}^*| = l$, that is, $\text{ID} = \text{ID}^*$, then the challenger $\mathcal{C}$ will try to construct a signature as aforementioned for extracting query using trapdoors $\mathbf{S}_{\mathbf{E}_i}$. Then, for every $i \in [l]$, $\mathbf{F}_{i,\text{id}_i} = \mathbf{A}_{i,\text{id}_i} \|\mathbf{B}_i + H(\text{ID}, \text{id}_i, i) \mathbf{C}_i = \mathbf{A}_{i,\text{id}_i} \|\mathbf{A}_{i,\text{id}_i} \mathbf{R}_i$. Compute the matrix $\mathbf{R}_\mu = \sum_{j=0}^k (-1)^{\mu[j]} \mathbf{R}'_j$ and the scalar $h_\mu = \sum_{j=0}^k (-1)^{\mu[j]} h_j$. Note that $\mathbf{D}_\mu = \sum_{j=0}^k (-1)^{\mu[j]} \mathbf{D}_j = \mathbf{F}_{i,\text{id}_i} \mathbf{R}_\mu + h_\mu \mathbf{E}_i$. If $h_\mu = 0 \pmod{q}$, abort the simulation. Otherwise, compute the matrix $\mathbf{F}_{i,\text{id}_i,\mu} = \mathbf{F}_{i,\text{id}_i} \|\mathbf{F}_{i,\text{id}_i} \mathbf{R}_\mu + h_\mu \mathbf{E}_i$ and run the algorithm $\sigma_i \leftarrow \text{SampleRight}(\mathbf{F}_{i,\text{id}_i}, h_\mu \mathbf{E}_i, \mathbf{R}_\mu, \mathbf{S}_{\mathbf{E}_i}, \hat{\mathbf{y}}_i, s_2)$. Finally, respond to the adversary $\mathcal{A}$ with the signature $(\mu, (\sigma_1, \sigma_2, \dots, \sigma_l), \text{ID})$.

Now, we prove that the signature is a valid signature and the distribution is identical to the real one. First, according to lemma 8, we have $(\mathbf{F}_{i,\text{id}_i} \|\mathbf{F}_{i,\text{id}_i} \mathbf{R}_\mu + h_\mu \mathbf{E}_i) \sigma_i = \hat{\mathbf{y}}_i$ for all $i \in [l]$ and σ_i is with negligible statistical distance from the distribution $\mathcal{D}_{\Lambda_q^{\hat{\mathbf{y}}_i}(\mathbf{Q}_{i,\text{id}_i}), s_2}$, where $\mathbf{Q}_{i,\text{id}_i} = \mathbf{F}_{i,\text{id}_i} \|\mathbf{F}_{i,\text{id}_i} \mathbf{R}_\mu + h_\mu \mathbf{E}_i$. Therefore, $(\mathbf{F}_{i,\text{id}_i} \|\mathbf{D}_\mu) \sigma_i = \hat{\mathbf{y}}_i$ due to the assumptions that $\mathbf{R}_\mu = \sum_{j=0}^k (-1)^{\mu[j]} \mathbf{R}'_j$ and $h_\mu = \sum_{j=0}^k (-1)^{\mu[j]} h_j$. In addition, $\|\sigma_i\| \leq s_2 \sqrt{3m}$ for all $i \in [l]$ from

Lemma 7(1). Therefore, $(\mu, (\sigma_1, \sigma_2, \dots, \sigma_l), \text{ID})$ is a valid signature.

- (b) If $|\text{ID} \cap \text{ID}^*| < d$, the challenger $\mathcal{C}$ uses the secret key from extract query for responding the signature query by the signature algorithm.
- (c) If $d \leq |\text{ID} \cap \text{ID}^*| < l$, the challenger $\mathcal{C}$ will firstly compute the secret key for identity ID like the extract query. Then, respond with the signature query as aforementioned.

(v) *Forgery*: the adversary $\mathcal{A}$ outputs a valid forgery signature $(\mu^*, (\sigma_1^*, \sigma_2^*, \dots, \sigma_l^*), \text{ID}^*)$ for the target identity ID^* . Then the challenger $\mathcal{C}$ computes the matrix $\mathbf{R}_{\mu^*} = \sum_{j=0}^k (-1)^{\mu^*[j]} \mathbf{R}_j'$, $h^* = \sum_{j=0}^k (-1)^{\mu^*[j]} h_j$. If $h^* \neq 0 \pmod{q}$, he aborts the simulation. According to whether the message μ^* is queried or not, there are two different cases that need to be considered.

- (a) The message μ^* is queried in the Sign queries. Assume that the challenger responded $(\mu^*, (\sigma_1', \sigma_2', \dots, \sigma_l'), \text{ID}^*)$ for message μ^* in the Sign queries. Then for all $i \in [l]$, parse $\sigma_i^* = \begin{bmatrix} \sigma_{i1}^* \\ \sigma_{i2}^* \\ \sigma_{i3}^* \end{bmatrix}$,

$$\sigma_i' = \begin{bmatrix} \sigma_{i1}' \\ \sigma_{i2}' \\ \sigma_{i3}' \end{bmatrix},$$

$$\mathbf{A}_{i, \text{id}^*} \left[(\sigma_{i1}^* - \sigma_{i1}') + \mathbf{R}_i (\sigma_{i2}^* - \sigma_{i2}') \right. \\ \left. + (\mathbf{R}_{\mu^*}^{(1)} + \mathbf{R}_i \mathbf{R}_{\mu^*}^{(2)}) (\sigma_{i3}^* - \sigma_{i3}') \right] = 0 \pmod{q}, \quad (9)$$

where $\mathbf{R}_{\mu^*}^{(1)}$ is the first m rows of matrix $\mathbf{R}_{\mu^*}$ and $\mathbf{R}_{\mu^*}^{(2)}$ is the last m rows of matrix $\mathbf{R}_{\mu^*}$. Let $\mathbf{e}_i^* = (\sigma_{i1}^* - \sigma_{i1}') + \mathbf{R}_i (\sigma_{i2}^* - \sigma_{i2}') + (\mathbf{R}_{\mu^*}^{(1)} + \mathbf{R}_i \mathbf{R}_{\mu^*}^{(2)}) (\sigma_{i3}^* - \sigma_{i3}')$; then $\|\mathbf{e}_i^*\| \leq 2s_2 \sqrt{m}(1 + 12\sqrt{2m})(1 + s_2 \sqrt{m(k+1)})$. The challenger $\mathcal{C}$ returns $\mathbf{e}_0 = \begin{bmatrix} \mathbf{e}_1^* \\ \mathbf{e}_2^* \\ \vdots \\ \mathbf{e}_l^* \end{bmatrix}$ as solution to $\mathbf{A}\mathbf{e}_0 = 0 \pmod{q}$ and $\|\mathbf{e}_0\| \leq 2s_2 l \sqrt{m}(1 + 12\sqrt{2m})(1 + s_2 \sqrt{m(k+1)}) = \beta$.

In addition, According to Lemma 26 of [16], $\Pr \{\mathbf{e}_i^* \neq 0\} \geq 2/3$; therefore, the probability of $\mathbf{e}_0 \neq 0$ is at least $1 - (1/3)^l$.

- (b) The message μ^* is not queried in the Sign queries. For every $i \in [l]$, separate σ_i^* into $\begin{bmatrix} \sigma_{i1}^* \\ \sigma_{i2}^* \\ \sigma_{i3}^* \end{bmatrix}$; then

$$\mathbf{A}_{i, \text{id}^*} \left[\sigma_{i1}^* + \mathbf{R}_i \sigma_{i2}^* + (\mathbf{R}_{\mu^*}^{(1)} + \mathbf{R}_i \mathbf{R}_{\mu^*}^{(2)}) \sigma_{i3}^* - \mathbf{x}_i \right] = 0 \pmod{q} \quad (10)$$

and $\|\sigma_{i1}^* + \mathbf{R}_i \sigma_{i2}^* + (\mathbf{R}_{\mu^*}^{(1)} + \mathbf{R}_i \mathbf{R}_{\mu^*}^{(2)}) \sigma_{i3}^* - \mathbf{x}_i\| \leq s_2 \sqrt{m}(2 + 12\sqrt{2m} + s_2 \sqrt{m(k+1)}(1 + 12\sqrt{2m}))$, where $\mathbf{R}_{\mu^*}^{(1)}$ is the first m rows of matrix $\mathbf{R}_{\mu^*}$ and $\mathbf{R}_{\mu^*}^{(2)}$ is the last m rows of matrix $\mathbf{R}_{\mu^*}$. Let

$$\mathbf{e}_i^* = \sigma_{i1}^* + \mathbf{R}_i \sigma_{i2}^* + (\mathbf{R}_{\mu^*}^{(1)} + \mathbf{R}_i \mathbf{R}_{\mu^*}^{(2)}) \sigma_{i3}^* - \mathbf{x}_i,$$

$$\text{and the challenger } \mathcal{C} \text{ returns } \mathbf{e}_0 = \begin{bmatrix} \mathbf{e}_1^* \\ \mathbf{e}_2^* \\ \vdots \\ \mathbf{e}_l^* \end{bmatrix}$$

as solution to $\mathbf{A}\mathbf{e}_0 = 0 \pmod{q}$ and $\|\mathbf{e}_0\| \leq s_2 l \sqrt{m}(2 + 12\sqrt{2m} + s_2 \sqrt{m(k+1)}(1 + 12\sqrt{2m})) \leq 2s_2 l \sqrt{m}(1 + 12\sqrt{2m})(1 + s_2 \sqrt{m(k+1)}) = \beta$.

In addition, according to Lemma 2.9 of [15], $\mathbf{e}_i^* \neq 0$ with overwhelming probability; therefore, $\mathbf{e}_0 \neq 0$ with overwhelming probability.

Furthermore, according to Lemma 27 of [16], the simulation completes both the Queries and the Forgery phases without aborting with probability of at least $(1/q)(1 - ((q_e + q_s)/q))$. Therefore, the probability that the challenger $\mathcal{C}$ can return a SIS solution is $\epsilon' \geq [(1/2)(1 - (1/3)^l) + (1/2)] \cdot (1/q) \cdot (1 - ((q_e + q_s)/q))\epsilon$. $\square$

Remark 13. In fact, there is a weakness in the above security proof. Specifically, in the forge phase, the adversary outputs a signature signed by ID^* instead of ID' ($|\text{ID}' \cap \text{ID}^*| \geq d$). If we change it into ID' that satisfies $|\text{ID}' \cap \text{ID}^*| \geq d$ and the signature can be verified correctly, the SIS hardness problem could not be embedded and the SIS solution will not be found. In addition, there is a similar question in the security proof of [21]. We think this problem is the bottleneck of constructing fuzzy attribute-based signature from lattices, and we will solve this problem as a long-term research direction.

6. Performance Analysis and Simulations

6.1. Comparison with the Scheme of [21]. The efficiency and security of our scheme and the scheme of [21] are summarized in Table 1, where the efficiency includes the size of storage space, the communication cost, and computation cost.

Firstly, we consider the size of storage space and the communication cost. Specifically, we compare the length of public parameters PP, the master secret key MK, and the private key of identity ID, which affect the the size of storage space. We also compare the length of the signature, which affects the communication cost.

- (i) As for the size of the public parameters PP, the scheme of [21] needs $2l$ matrices in $\mathbb{Z}_{pq}^{n \times m}$; the size is about $2lnm \log(pq)$. Our scheme needs $(4l + k + 1)$ matrices in $\mathbb{Z}_q^{n \times m}$ and a vector in $\mathbb{Z}_q^n$; the size is about $(4l + k + 1)nm \log q + n \log q$.
- (ii) As for the size of the master secret key MK, the scheme of [21] needs $2l$ matrices in $\mathbb{Z}_{pq}^{m \times m}$; the size is about $2lm^2 \log(pq)$. Our scheme needs $2l$ matrices in $\mathbb{Z}_q^{m \times m}$; the size is about $2lm^2 \log q$.
- (iii) As for the size of the private key of identity ID, the scheme of [21] needs l matrices in $\mathbb{Z}_{pq}^{2m \times 2m}$; the size is about $4lm^2 \log(pq)$. Our scheme needs l matrices in $\mathbb{Z}_q^{2m \times 2m}$; the size is about $4lm^2 \log q$.
- (iv) As for the size of the signature σ , the signature of the scheme of [21] is made of l vectors in $\mathbb{Z}_{pq}^{2m}$; the size is

TABLE 1: Performance comparison with the scheme of [21].

	Length of PP	Length of MK	Length of sk_{ID}	Length of σ
[21]	$2lmn \log(pq)$	$2lm^2 \log(pq)$	$4lm^2 \log(pq)$	$2lm \log(pq)$
Ours	$(4l + k + 1)mn \log q + n \log q$	$2lm^2 \log q$	$4lm^2 \log q$	$3lm \log q$
	Sign cost	Verify cost	Unforgeability	Model
[21]	$n \text{ SSS}^\dagger$ + $l \text{ PS}^\ddagger(pq)$	$d \text{ MVP}^\S(pq)$ + $d \text{ SMP}^\S(pq)$	$\text{EU}^b <$	$\text{ROM}^\ddagger$
Ours	$n \text{ SSS}$ + $l \text{ DGS}^\S(q)$ + $l \text{ PS}^\ddagger(q)$	$d \text{ MVP}(q)$ + $d \text{ SMP}(q)$ + $k \text{ MMA}^\blacklozenge(q)$	$\text{SU}^\#$	$\text{SM}^\parallel$

Note. The units of public parameters size, master secret key size, private key of identity size, and signature size are bits. The base of the logarithm function is 2; $\text{SSS}^\dagger$ denotes Shamir secret sharing operation; $\text{PS}^\ddagger$ denotes preimage sampling algorithm; $\text{MVP}^\S$ denotes matrix and vector product (where the matrix form is $(n \times 2m)$ and the vector form is $2m$ -row); $\text{SMP}^\S$ denotes scalar multiplication; EU^b denotes existential unforgeability; $\text{ROM}^\ddagger$ denotes random oracle model; $\text{DGS}^\S$ DGS denotes discrete Gaussian sampling algorithm; $\text{MMA}^\blacklozenge$ denotes matrix and matrix addition; $\text{SU}^\#$ denotes strong unforgeability; $\text{SM}^\parallel$ denotes the standard model. The (pq) and (q) denote modules that are used in the corresponding operations.

TABLE 2: Parameters settings.

Number	1	2	3	4	5	6
n	128	136	192	214	256	320
q	2053	2003	4093	16381	4093	4093
m	8448	8976	13824	17976	18432	23040

about $2lm \log(pq)$. Our signature is made of l vectors in $\mathbb{Z}_q^{3m}$; the size is about $3lm \log q$.

Secondly, we compare sign cost and verify cost of our scheme and the scheme of [21], which affects the computation cost.

- (i) Sign cost: in the scheme of [21], the process of signing is made of n times of Shamir secret-sharing operations (SSS) and l times of preimage sampling algorithms (PS) with module pq . In our scheme, the process of signing is made of n times of Shamir secret-sharing operations (SSS), l times of discrete Gaussian sampling algorithms (DGS) with module q , and l times of preimage sampling algorithms (PS) with module q .
- (ii) Verify cost: in the scheme of [21], the process of verifying is made of d times of matrix and vector products in $\mathbb{Z}_{pq}$ (MVP) (where the matrix form is $(n \times 2m)$ and the vector form is $2m$ -row), d times of scalar multiplications in $\mathbb{Z}_{pq}^{2m}$ (SMP). In our scheme, the process of verifying is made of d times of matrix and vector products in $\mathbb{Z}_q$ (MVP) (where the matrix form is $(n \times 3m)$ and the vector form is $3m$ -row), d times of scalar multiplication in $\mathbb{Z}_q^{3m}$ (SMP), and k times of matrix and matrix additions (MMA) in $\mathbb{Z}_q^{n \times m}$.

Finally, we compare the security that these two schemes achieved. Improving the security of the scheme of [21] is our motivation of this paper. Specifically, our scheme can achieve strong unforgeability instead of existential unforgeability. Meanwhile, we prove the security proof in the standard model instead of in the random oracle model. Therefore, our scheme seems safer than the scheme of [21]. To the best of our

knowledge, our scheme is the first FIBS scheme from lattices without random oracles and achieves strong unforgeability.

6.2. Simulations. The scheme of [21] and our scheme are implemented in Visual Studio 2008 in Windows 7 Service Pack1 64-bit operating system. We use a desktop which has a 4-core Intel(R) Core (TM) i7-860 processor running at 2.79 GHz and 8 GB of RAM.

We carry out 6 simulations with different parameter settings that are given in Table 2 (it is suggested from [26, 29]). As for other parameters, we set the length of identity string $l = 80$, the error tolerance parameter $d = 40$, and the length of message $k = 80$. We use the same parameter settings and choose another module p in [21]. We let $p = q$ in the simulation, but in fact, the module p is larger than q . The average sign time and verify time are listed in Table 3 and illustrated in Figure 3. The length of public parameters and master secret key is illustrated in Figure 1. The length of private key of identity and signature is illustrated in Figure 2.

Remark 14. In fact, in the simulation of signing, we only count the time of l times preimage sampling algorithms (PS) with module pq in the scheme of [21], and we count the time of l times discrete Gaussian sampling algorithms (DGS) with module q and l times preimage sampling algorithms (PS) with module q in our scheme. The time of n times Shamir secret-sharing operations (SSS) is not included because it is the same in these two schemes.

Remark 15. In the simulation of verifying, we count the time of $(d + 1)$ times matrix and vector products in $\mathbb{Z}_{pq}$ (MVP) (where the matrix form is $(n \times 2m)$ and the vector form is $2m$ -row) in the scheme of [21]; the additional one time MVP

FIGURE 1: Length of public parameters/master secret key.

FIGURE 2: Length of private key of identity/signature.

in $\mathbb{Z}_{pq}$ is derived from d times scalar multiplications (SMP) in $\mathbb{Z}_{pq}^{2m}$. We count the time of $(d + 1)$ times matrix and vector products in $\mathbb{Z}_q$ (MVP) (where the matrix form is $(n \times 3m)$ and the vector form is $3m$ -row); the additional one time MVP in $\mathbb{Z}_q$ is derived from d times scalar multiplications in $\mathbb{Z}_q$ (SMP) and k times matrix and matrix additions (MMA).

From Figures 1, 2, and 3, we may draw the following conclusions. (1) In the aspect of storage space, the length of our scheme's public parameters is longer than the one of [21], while the length of the master secret key and the length of identity's private key are shorter than the ones of [21]. So,

the storage space of PKG and identities is broadly flat in these two schemes. (2) The sign time in these two schemes is approximately the same, while the verify time of our scheme is longer than the one of [21]. Therefore, the computation cost of our scheme is larger than the scheme of [21]. (3) The length of signature of our scheme is shorter than the one of [21], which leads to the result that the communication cost is smaller the scheme of [21]. In general, in the personal computer, the storage space is large and the computational ability is strong enough, while the bandwidth becomes a main factor of restricting the communication. The signature size of our scheme is shorter, which is good for communication.

FIGURE 3: Average sign/verify time.

TABLE 3: Average sign/verify time (s).

Number		1	2	3	4	5	6
[21]	Sign	705.408	734.72	1041.344	1411.392	1455.824	1992.768
	Verify	51.26	59.37	129.168	186.2	232.872	362.96
Ours	Sign	703.6	732.448	1040.336	1401.728	1449.056	2000.448
	Verify	34.41	39.21	85.104	125.04	150.256	240.44

7. Conclusions and Open Problems

In this paper, we present an FIBS scheme from lattices and prove the strong unforgeability of our scheme under selective chosen-identity and adaptive chosen-message attacks (SU-sID-CMA) in the standard model. In addition, complexity analysis and simulations are given in the end of the paper.

Attribute-based signature (ABS) scheme extends (fuzzy) identity-based signature in which a signer is defined by a set of attributes instead of a single string representing the signer's identity. For further research, we aim for constructing a fuzzy attribute-based signature scheme from lattices. In addition, we can also use other secret sharing schemes [30] to construct FIBS scheme.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors are grateful to the reviewers for their helpful advices. This work is partially supported by the National Natural Science Foundation of China (NSFC) (nos. 61121061, 61202082, and 61370194), the NSFC A3 Foresight Program (no. 61161140320), and the Fundamental Research Funds for the Central Universities (BUPT2012RC0219).

References

- [1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, vol. 196 of *Lecture Notes in Computer Science*, pp. 47–53, Springer, Berlin, Germany, 1985.
- [2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO*, pp. 213–229, Springer, Berlin, Germany, 2001.
- [3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT 2005*, pp. 457–473, Springer, Berlin, Germany, 2005.
- [4] J. Baek, W. Susilo, and J. Zhou, "New constructions of fuzzy identity-based encryption," in *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS '07)*, pp. 368–370, ACM, March 2007.
- [5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, ACM, November 2006.
- [6] P. Yang, Z. Cao, and X. Dong, "Fuzzy identity based signature," Report 2008/002, IACR Cryptology ePrint Archive, 2008.
- [7] P. Yang, Z. Cao, and X. Dong, "Fuzzy identity based signature with applications to biometric authentication," *Computers and Electrical Engineering*, vol. 37, no. 4, pp. 532–540, 2011.
- [8] L. Zhang, Q. Wu, and Y. Hu, "Fuzzy biometric identity-based signature in the standard model," *Applied Mechanics and Materials*, vol. 44–47, pp. 3350–3354, 2011.

- [9] C. Wang, "A provable secure fuzzy identity based signature scheme," *Science China: Information Sciences*, vol. 55, no. 9, pp. 2139–2148, 2012.
- [10] C. Wang and J. Kim, "Two constructions of fuzzy identity based signature," in *Proceedings of the 2nd International Conference on Biomedical Engineering and Informatics (BMEI '09)*, pp. 1–5, October 2009.
- [11] C. Wang, W. Chen, and Y. Liu, "A fuzzy identity based signature scheme," in *Proceedings of the International Conference on E-Business and Information System Security (EBISS '09)*, pp. 1–5, Wuhan, China, May 2009.
- [12] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.
- [13] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, article 34, 2009.
- [14] D. Micciancio and C. Peikert, "Trapdoors for lattices: Simpler, tighter, faster, smaller," in *Proceedings of the Advances in Cryptology (EUROCRYPT '12)*, pp. 700–718, Springer, Berlin, Germany, 2012.
- [15] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08)*, pp. 197–206, ACM, May 2008.
- [16] X. Boyen, "Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more," in *Public Key Cryptography—PKC 2010*, vol. 6056 of *Lecture Notes in Computer Science*, pp. 499–517, Springer, Berlin, Germany, 2010.
- [17] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," *Journal of Cryptology*, vol. 25, no. 4, pp. 601–639, 2012.
- [18] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H) IBE in the standard model," in *Advances in Cryptology—EUROCRYPT 2010*, pp. 553–572, Springer, Berlin, Germany, 2010.
- [19] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in *Proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS '11)*, pp. 97–106, 2011.
- [20] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," in *Proceeding of the 3rd Conference on Innovations in Theoretical Computer Science (ITCS '12)*, pp. 309–325, New York, NY, USA, January 2012.
- [21] Y. Yao and Z. Li, "A novel fuzzy identity based signature scheme based on the short integer solution problem," *Computers and Electrical Engineering*, 2013.
- [22] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *Journal of the ACM*, vol. 51, no. 4, pp. 557–594, 2004.
- [23] G. Leurent and P. Nguyen, "How risky is the random-oracle model?" in *Advances in Cryptology-CRYPTO 2009*, pp. 445–464, Springer, Berlin, Germany, 2009.
- [24] A. Shamir, "How to share a secret," *Communications of the Association for Computing Machinery*, vol. 22, no. 11, pp. 612–613, 1979.
- [25] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, Springer, New York, NY, USA, 2002.
- [26] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267–302, 2007.
- [27] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," *Theory of Computing Systems*, vol. 48, no. 3, pp. 535–553, 2011.
- [28] H. Krawczyk and T. Rabin, "Chameleon signatures," in *Proceedings of the Network and Distributed System Security Symposium (NDSS '00)*, pp. 143–154, San Diego, Calif, USA, 2000.
- [29] R. Lindner and C. Peikert, "Better key sizes (and attacks) for LWE-based encryption," in *Topics in Cryptology CCT-RSA*, pp. 319–339, Springer, Berlin, Germany, 2011.
- [30] D. Zhao, H. Peng, C. Wang, and Y. Yang, "A secret sharing scheme with a short share realizing the (t, n) threshold and the adversary structure," *Computers & Mathematics with Applications*, vol. 64, no. 4, pp. 611–615, 2012.