Hindawi
Security and Communication Networks
Volume 2021, Article ID 6692608, 9 pages
https://doi.org/10.1155/2021/6692608

Research Article

Fuzzy Identity-Based Ring Signature from Lattices

Chengtang Cao, Lin You, and Gengran Hu

School of Cyberspace Security, Hangzhou Dianzi University, Hangzhou 310018, China

Correspondence should be addressed to Lin You; mryoulin@gmail.com

Received 7 October 2020; Revised 17 February 2021; Accepted 6 March 2021; Published 16 March 2021

Academic Editor: Clemente Galdi

In this paper, a construction of a fuzzy identity-based ring signature scheme (LFIBRS) is proposed. Our LFIBRS combines the characteristics of both the fuzzy identity-based signature (FIBS) and the ring signature. On the one hand, a signature issued under an identity ID can be verified by any identity ID′ that is "close enough" to the identity ID. Since biometric identification is the well-known most popular and reliable identification method, our LFIBRS can be applied in such a situation whenever it is required for official audit or supervision that the signer's real identity is needed to be authenticated. On the other hand, LFIBRS provides anonymity under the random oracle model. In addition, LFIBRS provides unforgeability under the small integer solution (SIS) lattice hardness assumption which can resist large-scale quantum computer attacks in the future.

1. Introduction

Ring signatures, which were first suggested by Rivest, Shamir, and Tauman [1], allow signing a message on behalf of a spontaneous set of signers, without breaking the anonymity of the signatory. Recently, many versions of ring signature schemes based on this concept have been constructed.

Nevertheless, numerous ring signature schemes concern classical number theory or algebraic mathematical assumptions, such as large integer factoring problem [1, 2], discrete logarithm problem [3–5], and bilinear pairing problems [6–10]. None of the schemes are secure with the onset of powerful quantum computers. Among the current postquantum cryptographic candidates, lattice-based cryptography has attracted significant attention of cryptographers recently. In 2008, the first ring signature scheme on lattice was constructed by Gentry et al. [11] and then a lot of ring signature schemes have been constructed [12–14]. Shamir [15] introduced an identity-based cryptosystem. Later, Sahai and Waters [16] put forward the concept of fuzzy identity-based encryption (FIBE), and they regarded identities as a set of biometric attributes rather than any string. Since then, many kinds of fuzzy identity-based signature schemes have been constructed [17–21]. As one of the most promising research alternatives of postquantum cryptography, lattice-based cryptography has attracted great attention due to its several potential advantages: asymptotic efficiency, the worst-case hardness hypothesis, and the security against quantum computing.

How to design a secure and efficient lattice-based cryptosystem is a very interesting and challenging problem. In this manuscript, based on the work of [21, 22], a fuzzy identity ring signature scheme based on the computational difficulty problem on lattices is constructed by combining the characteristics of fuzzy identity signature and ring signature.

1.1. Related Work. Wang et al. [23] proposed a lattice-based ring signature scheme in the Bonsai tree model, which was based on the hard assumption of SIS problem; meanwhile, unforgeability had been proved in both the random oracle and standard model. Wang [24] and Jia et al. [22] proposed identity-based ring signature scheme from lattice which was based on the hard assumption of SIS problem. As we know, Yao and Li [19] constructed the first FIBS scheme based on the hard assumption of SIS problem. By using the Bonsai tree techniques, they proved that their scheme was secure in the random oracle model. Recently, Zhang et al. [21]

proposed an extended version of Yao and Li's FIBS scheme and claimed that it could capture more expressive attributes in a large universe. Besides, their version was proved to be strongly unforgeable against selective chosen-identity and adaptive chosen-message attacks (SU-sID-CMA) secure in the standard model.

1.2. Contributions. In this paper, we propose a fuzzy identity-based ring signature scheme (LFIBRS) based on the hard assumption of SIS problem and prove that it is unforgeable in the random oracle model. In this work, we focus on combining the characteristics of ring signature and the fuzzy identity-based signature from lattices, and it makes our scheme be able to provide biometric authentication and maintain anonymity at the same time.

1.3. Structure of the Paper. In Section 2, some mathematical symbols, integer lattices, and statistical distance are defined. Section 3 gives the framework of the signature scheme. The construction of our signature scheme is described in Section 4. The security of our LFIBRS is proved in Section 5. Finally, some comparisons with some other referred works and conclusion remarks are given.

2. Preliminaries

2.1. Notations. In this section, we make use of the following notations:

$[i]$: The set $\{1, 2, \ldots, i\}$

$x \leftarrow S$: x is sampled uniformly at random from the set S

$\|z\|$: The Euclidean norm of $\mathbf{z}$

$\|\mathbf{A}\|$: The norm of $\|\mathbf{A}\|$ as the norm of its longest column $\|\mathbf{A}\| = \max_i \|\mathbf{A}_i\|$

$\widetilde{\mathbf{A}}$: The matrix after Gram-Schmidt orthogonalization of matrix $\mathbf{A}$

$f(n) = \omega(g(n))$: If $\lim_{n\longrightarrow\infty} = g(n)/f(n) = 0$

$f(n) = \widetilde{O}(g(n))$: If $f(n) = g(n) \cdot \mathrm{poly}(\log n)$

2.2. Integer Lattices

Definition 1. Let $\mathbf{B} = [\mathbf{b}_1|\mathbf{b}_2|\cdots|\mathbf{b}_m] \in \mathbb{R}^{m\times m}$ be a matrix with m linearly independent vectors. The m-dimensional lattice Λ generated by $\mathbf{B}$ is as follows:

$$\Lambda = \mathscr{L}(\mathbf{B}) = \{\mathbf{y} \in \mathbb{R}^m : \exists \mathbf{s} \in \mathbb{Z}^m, \quad \mathbf{y} = \mathbf{Bs}\}. \tag{1}$$

Definition 2. For prime $q \geq 2$ and matrix $\mathbf{A} \in \mathbb{Z}^{n\times m}$, define

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{Ay} = \mathbf{O} \bmod q\}. \tag{2}$$

For $s > 0$, define the Gaussian function on $\mathbb{R}^m$ with center $\mathbf{c}$: $\forall \mathbf{e} \in \mathbb{R}^m$, $\rho_{s,\mathbf{c}}(\mathbf{e}) = \exp(-\pi\|\mathbf{e} - \mathbf{c}\|^2/s^2)$. For m-dimensional lattice Λ, define $\rho_{s,\mathbf{c}}(\Lambda) = \sum_{\mathbf{e}\in\Lambda}\rho_{s,\mathbf{c}}(\mathbf{e})$. For $\mathbf{c} \in \mathbb{R}^m$ and $s > 0$, define the discrete Gaussian distribution over Λ as follows: $\forall \mathbf{e} \in \Lambda, \mathscr{D}_{\Lambda,s,\mathbf{c}} = \rho_{s,\mathbf{c}}(\mathbf{e})/\rho_{s,\mathbf{c}}(\Lambda)$. For convenience, if $\mathbf{c} = \mathbf{O}$, we denote $\mathscr{D}_{\Lambda,s,\mathbf{c}}$ as $\mathscr{D}_{\Lambda,s}$.

2.3. Lattice-Related Algorithms. How to obtain a matrix $\mathbf{A}$ with a low Gram-Schmidt norm basis for $\Lambda_q^{\perp}(\mathbf{A})$ was introduced by Ajtai [25], and two improved algorithms were proposed by [26, 27], respectively.

Lemma 1 (see [26]). *Let integers $q \geq 3$ be odd, $n \geq 1$, and $m = 2n\lceil \log q \rceil$. There exists a PPT algorithm $\mathbf{TrapGen}(q, n, m)$ that outputs $\mathbf{A}$ and $\mathbf{T}_\mathbf{A}$ such that $\mathbf{A}$ is statistically close to a uniform matrix in $\mathbb{Z}_q^{n\times m}$ and $\mathbf{T}_\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ is a short basis for $\Lambda_q^{\perp}(\mathbf{A})$, satisfying $\|\widetilde{\mathbf{T}_\mathbf{A}}\| \leq O(\sqrt{n\log q})$ with all but a negligible probability in n.*

In this subsection, we recall several useful facts on lattices in the literatures [1, 28], in order to generate another short basis for a lattice which contains a sublattice isomorphic to the original.

Lemma 2 (Lemma 3.2 of [28]). *On input $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, whose columns generate the entire group $\mathbb{Z}_q^n$ and an arbitrary $\mathbf{B} \in \mathbb{Z}_q^{n\times m'}$, given a basis $\mathbf{T}_\mathbf{A}$ of $\Lambda_q^{\perp}(\mathbf{A})$, there is a deterministic polynomial-time algorithm $\mathbf{ExtBasis}(\mathbf{T}_\mathbf{A}, A' = [\mathbf{A}|\mathbf{B}])$ that outputs a basis $\mathbf{T}_{A'}$ for $\Lambda_q^{\perp}(A') \subseteq \mathbb{Z}^{m+m'}$ such that $\|\widetilde{\mathbf{T}_{A'}}\| = \|\widetilde{\mathbf{T}_\mathbf{A}}\|$. Moreover, this statement holds even for any given permutation of the columns of A'.*

Lemma 3 (Lemma 3.3 of [28]). *On input $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $s \geq \|\widetilde{\mathbf{T}_\mathbf{A}}\| \cdot \omega(\sqrt{\log n})$. Given a basis $\mathbf{T}_\mathbf{A}$ of $\Lambda_q^{\perp}(\mathbf{A})$, there is a PPT algorithm $\mathbf{RandBasis}(\mathbf{A}, \mathbf{T}_\mathbf{A}, s)$ that outputs a basis $\mathbf{T}_\mathbf{A}'$ for $\Lambda_q^{\perp}(\mathbf{A})$ such that $\|\widetilde{\mathbf{T}_\mathbf{A}'}\| \leq s\sqrt{m}$ and no information specific to $\mathbf{T}_\mathbf{A}$ is leaked.*

We adopt the preimage sampling lemma from the discrete Gaussian distribution over lattices, which is shown in [11].

Lemma 4 (see [11]). *Assume integer $q \geq 2, \mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and real $0 < \epsilon < 1$. Let $\mathbf{T}_\mathbf{A}$ be a short basis for $\Lambda_q^{\perp}(\mathbf{A})$; parameter $s \geq \|\widetilde{\mathbf{T}_\mathbf{A}}\| \cdot \omega(\sqrt{\log n})$. Then, for $\mathbf{c} \in \mathbb{R}^m, \mathbf{u} \in \mathbb{Z}_q^m$,*

(1) $\Pr[\mathbf{x} \leftarrow D_{\Lambda,s,\mathbf{c}} : \|\mathbf{x} - \mathbf{c}\| > s\sqrt{m}] < ((1+\epsilon)/(1-\epsilon)) \cdot 2^{-m}$

(2) A PPT algorithm $\mathbf{SampleGau}(\mathbf{A}, \mathbf{T}_A, s, \mathbf{c})$ returns $\mathbf{e} \in \Lambda_q^{\perp}(\mathbf{A})$ drawn from a distribution statistically close to $\mathscr{D}_{\Lambda_q^{\perp}(\mathbf{A}),s,\mathbf{c}}$

(3) A PPT algorithm $\mathbf{SamplePre}(\mathbf{A}, \mathbf{T}_A, s, \mathbf{c})$ returns $\mathbf{e} \in \Lambda_q^{\mathbf{u}}(\mathbf{A})$ sampled from a distribution statistically close to $\mathscr{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),s}$

In [22], Lemma 4 is extended to the matrix sampling algorithm, which is repeated as follows.

Lemma 5 (see [22]). *On input $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $s \geq \|\widetilde{\mathbf{T}}\| \cdot \omega(\sqrt{\log n})$. Given a short basis $\mathbf{T}$ for $\Lambda_q^{\perp}(\mathbf{A})$ and arbitrary matrix $\mathbf{V} \in \mathbb{Z}_q^{n\times k}$, there is a polynomial-time algorithm $\mathbf{SampleMatPre}(\mathbf{A}, \mathbf{T}, s, \mathbf{V})$, which outputs a matrix $\mathbf{S} \in \mathbb{Z}_q^{m\times k}$, so that $\mathbf{AS} = \mathbf{V}$, $\mathbf{V}$ and $D_{\Lambda^{\perp}(\mathbf{A})}$ are statistically close, and $\|\mathbf{V}\| \leq s\sqrt{m}$ holds with overwhelming probability.*

Rejection sampling is an important technology of lattice-based signature scheme, which is proposed by Lyubashevsky in [29]. In the signing process, we output the candidate

signature in a certain probability without using a preimage sampling algorithm; hence, the distribution of the output signature is independent of the private key of the signer. With regard to the technique of rejecting sampling, we use the two following results.

Lemma 6 (Lemma 4.4 of [29]). *For any $\sigma > 0$ and integer m, the following inequalities hold:*

(1) $\Pr[\mathbf{x} \leftarrow D_\sigma : \|\mathbf{x}\| > w(\sigma\sqrt{\log m})] < 2^{-\omega(\log m)}$

(2) For any $\mathbf{z} \in \mathbb{Z}^m$ *and* $\sigma > \sqrt{\log 3m}$, $D_\sigma^m < 2^{-m+1}$ *holds*

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

Theorem 1 (Theorem 4.6 of [29]). *Let* $\mathbf{V}$ *be a subset of* $\mathbb{Z}^m$ *in which all elements have norms less than* T, *let* σ *be some element in* $\mathbb{R}$ *such that* $\sigma = \omega(T\sqrt{\log m})$, *and let* h: $\mathbf{V} \longrightarrow \mathbb{R}$ *be a probability distribution. Then there exists a constant* $M = O(1)$ *such that the distribution of the following algorithm* $\mathcal{A}$,

(1) $\mathbf{v} \leftarrow h$

(2) $\mathbf{z} \leftarrow D_{\mathbf{v},\sigma}^m$

(3) output $(\mathbf{z}, \mathbf{v})$ *with probability* $\min((D_\sigma^m(\mathbf{z})/MD_{\mathbf{v},\sigma}^m(\mathbf{z})), 1)$

is within the statistical distance $2^{-\omega(\log m)}/M$ *of the distribution of the following algorithm* $\mathcal{F}$:

(1) $\mathbf{v} \leftarrow h$

(2) $\mathbf{z} \leftarrow D_\sigma^m$

(3) output $(\mathbf{z}, \mathbf{v})$ *with probability* $1/M$

Moreover, the probability that A outputs something is at least $(1 - 2^{-\omega(\log m)})/M$.

2.4. Statistical Distance. The statistical distance measures how different two probability distributions are. In order to be employed in the anonymity of our scheme, we recall it as follows.

Definition 3 (Definition 8.5 of [30]). Let X and X' be two random variables over a countable set S. The statistical distance between X and X' is defined by

$$\Delta(X, X') = \frac{1}{2}\sum_{x \in S}\left|\Pr[X = x] - \Pr[X' = x]\right|. \quad (3)$$

The following lemmas show that the statistical distance cannot be increased by a randomized algorithm.

Lemma 7 (Proposition 8.9 of [30]). *Let* $X_1, X_2, \ldots, X_k$ *and* $Y_1, Y_2, \ldots, Y_k$ *be two lists of totally independent random variables. Then,*

$$\Delta((X_1, X_2, \ldots, X_k), (Y_1, Y_2, \ldots, Y_k)) \le \sum_{i=1}^{k}\Delta(X_i, Y_i). \quad (4)$$

Lemma 8 (Proposition 8.10 of [30]). *Assume that* X *and* X' *are two random variables over set* S. *For any (possibly randomized) function* f *with domain* S, *the statistical distance between* $f(X)$ *and* $f(X')$ *is at most*

$$\Delta(f(X), f(X')) \le \Delta(X, X'). \quad (5)$$

2.5. The SIS Problem. The SIS problem is as hard as the worst-case lattice problem; it was proved by Ajtai [25] for the first time,and then by Micciancio and Regev [31] and Gentry et al. [11]. We recall it as follows.

Definition 4. The SIS problem in the Euclidean norm is that, given an integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and a positive real β, the goal is to find a nonzero vector $\mathbf{e} \in \mathbb{Z}^m$ satisfying $\mathbf{Ae} = \mathbf{O} \bmod q$, and $\|\mathbf{e}\| \le \beta$.

Lemma 9 (Theorem 5.16 of [31]). *For poly-bounded* m, $\beta = poly(n)$, *and prime* $q \ge \beta \cdot \omega(\sqrt{n \log n})$, *the average-case* $SIS_{q,n,m,\beta}$ *problem is as hard as approximating the shortest independent vector problem* $SIVP_\gamma$ *to within certain* $\gamma = \beta \cdot \widetilde{O}(\sqrt{n})$ *factor.*

3. System Framework and Security Model of LFIBRS Scheme

A fuzzy identity-based ring signature scheme consists of the following four probabilistic polynomial-time (PPT) algorithms:

SetUp(q, n, m): The Private Key Generator (PKG) runs a PPT algorithm that takes the security parameter n as input and generates the system parameters PP, an error tolerance parameter k, and master keys **MK**. The system parameters PP are made public and master keys **MK** are kept secret.

KeyExt(ID, **PP**, **MK**): It is a PPT algorithm that takes an identity ID, the public parameters PP, and the master keys **MK** as input and outputs secret keys SK and public key $\mathbf{A_{ID}}$ associated with the ID.

Sign$(\mu, \mathrm{sk}, \mathrm{PK}, \mathrm{PP})$: It is a PPT algorithm that takes the public parameters PP, the public keys $\mathrm{PK} = \{\mathbf{PK_{ID}}^{\langle i \rangle}\}_{i \in [l]}$ corresponding to the identities of l ring members, the secret keys SK associated with an identity ID, and a message μ as input and outputs a signature σ.

Verify$(\mu, \sigma, \mathrm{ID}', \mathrm{PP}, \mathrm{PK})$: It is a deterministic algorithm that takes the public parameters PP, an fuzzy identity ID$'$ s, the message μ, the public keys PK, and the corresponding signature σ as input and outputs "1" or "0."

The correctness of a ring signature scheme with fuzzy identity means that the verification algorithm always outputs "1" for a legal signature and "0" for an illegal signature.

3.1. Security Properties. A security ring signature must satisfy anonymity and unforgeability. The formal definition of the security model is given as follows.

Definition 6 (anonymity). If there is no polynomial-time adversary $\mathscr{A}$ to win the following games with an advantage that cannot be ignored, the LFIBRS scheme is signer-ambiguous.

(1) **Setup**: input system parameters n and $\mathscr{C}$ to generate and send public parameter PP and the maximum possible user set $U_N = \{\mathbf{ID}^{\langle 1\rangle}, \mathbf{ID}^{\langle 2\rangle}, \ldots, \mathbf{ID}^{\langle N\rangle}\}$ to $\mathscr{A}$.

(2) **Query**: $\mathscr{A}$ performs a polynomially bounded number of queries.

(3) **Challenge**: $\mathscr{C}$ selects the message μ, $U^* = \{\mathbf{ID}^{\langle i1^*\rangle}, \mathbf{ID}^{\langle i2^*\rangle}, \ldots, \mathbf{ID}^{\langle il^*\rangle}\} \subseteq U_N$, and uses the master key MK to generate the secret key SK_{i_0} and SK_{i_1} which corresponds to ID_{i_0} and ID_{i_1}. $\mathscr{C}$ randomly selects $b \in \{0,1\}$ and then calls the signature algorithm to generate the signature σ_{i_b}.

(4) **Guess**: $\mathscr{A}$ outputs bit b' as a guess of b. If $b' = b$, then $\mathscr{A}$ wins the game.

The advantage is defined as $\mathrm{Adv}_{\mathscr{A}} = |\Pr[b' = b] - (1/2)|$.

Definition 7 (unforgeability). If there is no polynomial time adversary $\mathscr{A}$ to win the following games with an advantage that cannot be ignored, then the LFIBRS scheme is said to be unforgeable.

(1) **Setup**: $\mathscr{C}$ exposes parameters PP and identity set U_N and sends them to $\mathscr{A}$.

(2) **Query**: adversary $\mathscr{A}$ can perform polynomial query:

Private key query: $\mathscr{C}$ calls the private key extraction algorithm, obtains the secret key SK corresponding to the identity ID, and returns it to $\mathscr{A}$

Signature query: $\mathscr{C}$ calls the signature algorithm to get the signature σ of the message μ and returns it to $\mathscr{A}$

(3) **Forgery**: the adversary $\mathscr{A}$ submits $(i^*, \mathrm{ID}'^*, \mathrm{PK}, \mu^*, \sigma^*)$, if the following conditions are true:

(1) σ^* is a legal signature
(2) $\mathscr{A}$ did not query the private key of ID'^*
(3) $\mathscr{A}$ did not query ID'^* and μ^*; then $\mathscr{A}$ won the game

The advantage is defined as $\mathrm{Adv}_{\mathscr{A}} = \Pr[\mathbf{LFIBRS} - \mathbf{Verify}(\mu, \sigma^*, \mathrm{ID}'^*, \mathrm{PP}, \mathrm{PK}) = 1]$.

4. Construction of LFIBRS

In this part, we present our construction of LFIBRS from lattice. The LFIBRS consists of four probability polynomial-time algorithms **Setup**, **KeyExt**, **Sign**, and **Verify**. We have incorporated different notations of the proposed LFIBRS scheme in the following.

4.1. LFIBRS Setup. This phase can be described as follows:

Step 1. For $i \in [l]$, run $\mathrm{Trapgen}(q, n, m)$ to generate a uniformly random matrix $\mathbf{E}_i \in \mathbb{Z}_q^{n\times m}$ together with a short basis $\mathbf{T}_{\mathbf{E}_i}$ for $\Lambda^{\perp}(\mathbf{E}_i)$, such that $\|\widetilde{\mathbf{T}_{\mathbf{E}_i}}\| \le O(\sqrt{n \log q})$.

Step 2. Run $\mathrm{Trapgen}(q, n, m)$ to generate a uniformly random matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$ together with a short basis $\mathbf{T}_{\mathbf{B}}$ for $\Lambda^{\perp}(\mathbf{B})$, such that $\|\widetilde{\mathbf{T}_{\mathbf{B}}}\| \le O(\sqrt{n \log q})$.

Step 3. For $i \in [l]$, randomly choose matrix $\mathbf{F}_i$ in $\mathbb{Z}_q^{n\times m}$.

Step 4. Randomly choose matrices $\mathbf{B}, \mathbf{C}$ in $\mathbb{Z}_q^{n\times m}$ and $\mathbf{D}$ in $\mathbb{Z}_q^{m\times m}$.

Step 5. Select hash functions $\mathbf{H}_1: \mathbb{Z}_q^m \longrightarrow \mathbb{Z}_q^{n\times n}$, $\mathbf{H}_2: (\mathbb{Z}_q^m)^l \times \mathbb{Z}_q^m \longrightarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{H}_3: \{0,1\}^* \longrightarrow \mathbb{Z}_q^n$, and $\mathbf{H}_4: \mathbb{Z}_q^{2m} \times \{0,1\}^* \longrightarrow \{v \in \mathbb{Z}_q^m: \|v\| \le t\}$.

Step 6. Select an error tolerance parameter k such that $k \le l - 1$.

Step 7. Output public parameters PP and master keys **MK**:

$$\mathrm{PP} = (\{\mathbf{E}_i, \mathbf{F}_i\}_{i\in[l]}, \mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{H}_1, \mathbf{H}_2, \mathbf{H}_3, \mathbf{H}_4, k) \text{ and } \mathbf{MK} = (\{\mathbf{T}_{\mathbf{E}_i}\}_{i\in[l]}, \mathbf{T}_{\mathbf{B}}).$$

Public parameters are made public and master keys are kept secret.

4.2. LFIBRS-KeyExt. Input a user whose identify $\mathbf{ID} = (\mathbf{ID}_1, \mathbf{ID}_2, \ldots, \mathbf{ID}_l)$; $\mathbf{ID}_i \in \mathbb{Z}_q^m$ and $i \in [l]$. Let us do the steps as follows:

Step 1. For $i \in [l]$, compute $\mathbf{G}_i = [\mathbf{E}_i | \mathbf{H}_1(\mathbf{ID}_i)\mathbf{F}_i]$, $\mathbf{G}_i \in \mathbb{Z}_q^{n\times 2m}$.

Step 2. For $i \in [l]$, compute matrix $\mathbf{T}_{\mathbf{G}_i}$ using algorithm $\mathrm{RandBasis}(\mathbf{G}_i, \mathrm{ExtBasis}(\mathbf{T}_{\mathbf{E}_i}, \mathbf{E}_i), s_0)$.

Step 3. Compute $\mathbf{PK}_{\mathbf{ID}} = [\mathbf{B} | \mathbf{H}_2(\mathbf{ID})\mathbf{D}]$, $\mathbf{PK}_{\mathbf{ID}} \in \mathbb{Z}_q^{n\times 2m}$. We remark that $\mathbf{PK}_{\mathbf{ID}} = [\mathbf{B} | \mathbf{H}_2(\mathbf{ID})\mathbf{D}]$ plays the role of the associated public key.

Step 4. Compute the matrix $\mathbf{T}_{\mathbf{PK}_{\mathbf{ID}}}$ using algorithm $\mathrm{RandBasis}(\mathbf{PK}_{\mathbf{ID}}, \mathrm{ExtBasis}(\mathbf{T}_{\mathbf{B}}, \mathbf{B}), s_0)$.

Step 5. Run $\mathrm{SampleMatpre}(\mathbf{PK}_{\mathbf{ID}}, \mathbf{T}_{\mathbf{PK}_{\mathbf{ID}}}, s, \mathbf{C})$ to generate $\mathbf{S}_{\mathbf{ID}} \in \mathbb{Z}_q^{2m\times m}$ and $\mathbf{PK}_{\mathbf{ID}}\mathbf{S}_{\mathbf{ID}} = \mathbf{C}$, such that $\|\mathbf{S}_{\mathbf{ID}}\| \le s\sqrt{2m}$.

Step 6. Output $\mathbf{PK}_{\mathbf{ID}}$ and $\mathrm{SK} = (\{\mathbf{T}_{\mathbf{G}_i}, \mathbf{G}_i\}_{i\in[l]}, \mathbf{S}_{\mathbf{ID}})$. $\mathbf{PK}_{\mathbf{ID}}$ is the $\mathbf{ID}$'s public key and $\mathrm{SK} = (\{\mathbf{T}_{\mathbf{G}_i}, \mathbf{G}_i\}_{i\in[l]}, \mathbf{S}_{\mathbf{ID}})$ are the corresponding secret keys.

4.3. LFIBRS-Sign. Input a message μ and the public keys $\mathrm{PK} = \{\mathbf{PK}_{\mathbf{ID}^{\langle i\rangle}}\}_{i\in[l]}$ corresponding to the identities of l ring members where the identity $\mathbf{ID}^{\langle\pi\rangle}$ ($\pi \in [l]$) of the real signer is related to the public key $\mathbf{PK}_{\mathbf{ID}^{\langle\pi\rangle}}$ and the secret keys $\mathrm{SK}_{\pi} = (\{\mathbf{T}_{\mathbf{G}_i}, \mathbf{G}_i\}_{i\in[l]}, \mathbf{S}_{\mathbf{ID}^{\langle\pi\rangle}})$. The signing process is as follows:

Step 1. Compute $\mathbf{v}_1 = \mathbf{H}_3(\mu, \mathrm{PK})$.

Step 2. $\mathbf{v}_1 = (\mathbf{v}_{11}, \mathbf{v}_{12}, \ldots, \mathbf{v}_{1m}) \in \mathbb{Z}_q^m$. The Shamir's secret sharing scheme is applied to every coordinate $\mathbf{v}_1^a$ of $\mathbf{v}_1$, that is, when $a \in [m]$, the polynomial with degree $k - 1$ is constructed in $\mathbb{Z}_q^m$, such that $p_a(0) = v_{1a}$.

Step 3. Construct the a-th share vector, $\widehat{\mathbf{v}_a} = (p_1(a), p_2(a), \ldots, p_m(a)) \in \mathbb{Z}_q^m$. Thus, for $J \subseteq [l]$ and

$k = |J| \le l - 1$, there are fractional Lagrangian coefficients L_a such that $\mathbf{v}_1 = \sum_{a\in[J]} L_a \widehat{\mathbf{v}}_a \bmod q$.

Step 4. For $i \in [l]$, call algorithm SamplePre$(\mathbf{G}_i, \mathbf{T}_{\mathbf{G}_i}, \widehat{\mathbf{v}}_a, s_2)$ to calculate $\mathbf{e}_i \in \mathbb{Z}_q^{2m}$.

Step 5. Compute $\mathbf{v} = \mathbf{H}_4(\sum_{i\in[l]} \mathbf{PK}_{\mathbf{ID}^{\langle i\rangle}} \mathbf{e}_i, \mu)$.

Step 6. Let $\mathbf{z}_\pi = \mathbf{S}_{\mathbf{ID}^{\langle\pi\rangle}} \cdot \mathbf{v} + \mathbf{e}_\pi$, and call algorithm $\mathscr{A}$ in Theorem 1; if there is output, output $\mathbf{z}_\pi$; otherwise, reselect the public key and go to the first step.

Step 7. For $i \in [l]\backslash\{\pi\}$, let $\mathbf{z}_i = \mathbf{e}_i$.

Step 8. Output $\sigma = (\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_l, \mathbf{v})$.

4.4. LFIBRS-Verify. Input the fuzzy identity $\mathbf{I}D' = (\mathbf{ID}'_1, \mathbf{ID}'_2, \ldots, \mathbf{ID}'_l)$, public parameters PP, message μ, the public keys PK $= \{\mathbf{PK}_{\mathbf{ID}^{\langle i\rangle}}\}_{i\in[l]}$, and the signature σ. The verification process is given as follows:

Step 1. For $i \in [l]$, verify $\|\mathbf{z}_i\| \le 2s_2\sqrt{2m}$. If it is true, continue to the next step. Otherwise, stop.

Step 2. For $i \in [l]$, calculate $\mathbf{G}'_i = [\mathbf{E}_i | \mathbf{H}_1(\mathbf{ID}'_i)\mathbf{F}_i]$.

Step 3. Let $E \subseteq \{\mathbf{G}'_1, \mathbf{G}'_2, \ldots, \mathbf{G}'_l\}$ and $|E| = k$; if there is E such that $\sum_{\mathbf{G}'_a\in E} L_a \mathbf{G}'_a \mathbf{z}_a = \mathbf{H}_3(\mu, \mathrm{PK})$, $(L_a = \prod_{a\in\{a:\, \mathbf{G}'_a\in E\}, i\ne a} (i/(i-a)))$, continue to the next step. Otherwise, stop.

Step 4. If $\mathbf{v} = \mathbf{H}_4(\sum_{i\in[l]} \mathbf{PK}_{\mathbf{ID}^{\langle i\rangle}} \mathbf{z}_i - \mathbf{cv}, \mu)$, output "1." Otherwise, output "0."

4.5. LFIBRS-Parameters. The safety parameter of scheme FIBRS is n, and other parameters are set as follows:

(1) Since TrapGen(q, n, m) is called, $m = 2n\lceil \log q \rceil$ is set by Lemma 1.

(2) To ensure the difficulty of SIS problem, set $q \ge \beta\omega(\sqrt{n\log n})$, $\beta = 2s_1\sqrt{2m}$, by Lemma 9

(3) Because RandBasis$(\mathbf{PK}_{\mathbf{ID}}, \mathrm{ExtBasis}(\mathbf{T}_\mathbf{B}, \mathbf{B}), s_0)$ is called, by Lemmas 2 and 3, set $s_0 \ge O(\log n) \cdot \omega(\sqrt{\log n})$

(4) Because SampleMatpre$(\mathbf{PK}_{\mathbf{ID}}, \mathbf{T}_{\mathbf{A}_{\mathbf{ID}}}, s, \mathbf{C})$ is called, by Lemma 5, set $s \ge s_0\sqrt{2m} \cdot \omega(\sqrt{\log n})$

(5) Because the signature algorithm needs Lemma 4 and Theorem 1, set $s_1 = \omega(T\sqrt{\log 2m})$

(6) Due to call SamplePre$(\mathbf{G}_i, \mathbf{T}_{\mathbf{G}_i}, \widehat{\mathbf{v}}_a, s_2)$, set $s_2 = s_1\sqrt{2m} \cdot \omega(\sqrt{\log 2m})$

4.6. LFIBRS-Correctness. The correctness analysis is briefly described as follows:

(1) According to Theorem 1 and Lemma 6, the signature will output $\mathbf{z}_j$ with overwhelming probability.

(2) According to Lemma 4, when the real identity can pass the verification in step 1 of the verification process, the next step can be continued.

(3) The following formula is established:

$$\begin{aligned}\sum_{i\in[l]} \mathbf{PK}_{\mathbf{ID}^{\langle i\rangle}} \mathbf{z}_i - \mathbf{Cv} &= \sum_{i\in[l]\backslash\{\pi\}} \mathbf{PK}_{\mathbf{ID}^{\langle i\rangle}} \mathbf{z}_i + \mathbf{PK}_{\mathbf{ID}^{\langle\pi\rangle}} \mathbf{z}_\pi - \mathbf{Cv} \\ &= \sum_{i\in[l]\backslash\{\pi\}} \mathbf{PK}_{\mathbf{ID}^{\langle i\rangle}} e_i + \mathbf{PK}_{\mathbf{ID}^{\langle\pi\rangle}} e_\pi \\ &= \sum_{i\in[l]} \mathbf{PK}_{\mathbf{ID}^{\langle i\rangle}} e_i.\end{aligned} \tag{6}$$

5. Security Analysis

Next, we will prove that the above LFIBRS scheme satisfies anonymity and unforgeability as required.

Theorem 2 (anonymity). *For prime $q \ge 3$, $m = 2n\lceil \log q \rceil$, and $b \in \{0, 1\}$, $\sigma_{b,PP,\mathbf{ID}_{i_b},PK,SK_{i_b},\mu}$ are the outputs of the algorithm* **LFIBRS-Sign**$(PP, \mathbf{ID}, PK, SK_{i_b}, \mu)$*, where PP is the public parameter, $\mathbf{ID}_{i_b}$ is the identity, SK_{i_b} is the secret key of the corresponding signature, and μ is the message of the corresponding signature. For any polynomial-time adversary, when SK_{i_0} and SK_{i_1} are unknown, the following formula holds:*

$$\Delta\left(\sigma_{0,\mathrm{PP},\mathbf{ID}_{i_0},\mathrm{SK}_{i_0},\mu}, \sigma_{1,\mathrm{PP},\mathbf{ID}_{i_1},\mathrm{SK}_{i_1},\mu}\right) \le n^{-\omega(1)}. \tag{7}$$

Therefore, the proposed LFIBRS scheme is computationally anonymous under the random oracle model.

Proof. The adversary $\mathscr{A}$ is a probabilistic polynomial-time Turing machine, which is allowed to make queries to the following oracles:

Setup: $\mathscr{C}$ performs the following operations to generate the public parameter PP and all user identities U_N and sends them to $\mathscr{A}$.

(1) Determine the maximum possible user set $U_N = \{\mathbf{ID}^{\langle 1\rangle}, \mathbf{ID}^{\langle 2\rangle}, \ldots, \mathbf{ID}^{\langle N\rangle}\}$

(2) Randomly select matrices $\mathbf{B}, \mathbf{C}$ in $\mathbb{Z}_q^{n\times m}$ and $\mathbf{D}$ in $\mathbb{Z}_q^{m\times m}$

(3) Output public parameters PP $= (\mathbf{B}, \mathbf{C}, \mathbf{D})$ and $U_N = \{\mathbf{ID}^{\langle 1\rangle}, \mathbf{ID}^{\langle 2\rangle}, \ldots, \mathbf{ID}^{\langle N\rangle}\}$

Query: adversary $\mathscr{A}$ can send the following query to $\mathscr{C}$, and $\mathscr{C}$ will return the query result to $\mathscr{A}$. Without losing generality, let $\mathscr{A}$ not repeat the query. $\mathscr{C}$ performs the following operations:

Hash query:

(1) $\mathscr{A}$ submits a user $\mathbf{ID}^{\langle i\rangle} = (\mathbf{ID}_1^{\langle i\rangle}, \mathbf{ID}_2^{\langle i\rangle}, \ldots, \mathbf{ID}_l^{\langle i\rangle})$ to $\mathscr{C}$, and, for $j \in [l]$, $\mathscr{C}$ selects $\mathbf{H}_1(\mathbf{ID}_j^{\langle i\rangle}) \in \mathbb{Z}_q^{n\times n}$ to return it to $\mathscr{A}$

(2) $\mathscr{A}$ submits the user $\mathbf{ID}^{\langle i\rangle}$ to $\mathscr{C}$, and $\mathscr{C}$ selects $\mathbf{H}_2(\mathbf{ID}^{\langle i\rangle}) \in \mathbb{Z}_q^{n\times m}$ to return it to $\mathscr{A}$

(3) $\mathscr{A}$ submits a message μ and the public keys PK $= \{\mathbf{PK}_{\mathbf{ID}^{\langle i\rangle}}\}_{i\in[l]}$ corresponding to the identities of l ring members, where the identity $\mathbf{ID}^{\langle\pi\rangle}$ $(\pi \in [l])$ to $\mathscr{C}$ and $\mathscr{C}$ selects $\mathbf{v}_1 \in\in \mathbb{Z}_q^n$ to return it to $\mathscr{A}$

(4) $\mathcal{A}$ submits a message μ and the public keys $\mathrm{PK} = \{\mathbf{PK}_{\mathbf{ID}^{\langle i\rangle}}\}_{i\in[l]}$ corresponding to the identities of l ring members, and $\mathcal{C}$ selects $\mathbf{v} \in \{\mathbf{v} \in \mathbb{Z}_q^m : \|\mathbf{v}\| \le t\}$ to return it to $\mathcal{A}$

Extract query: $\mathcal{A}$ adaptively selects a user $\mathbf{ID}^{\langle i\rangle}$ ($i \in [N]$) to $\mathcal{C}$. $\mathcal{C}$ returns the secret key $\mathrm{SK}_{\mathbf{ID}^{\langle i\rangle}}$ of the corresponding user $\mathbf{ID}^{\langle i\rangle}$.

Sign query: $\mathcal{A}$ submits message μ, the identity subset $U = \{\mathbf{ID}^{\langle i1\rangle}, \mathbf{ID}^{\langle i2\rangle}, \ldots, \mathbf{ID}^{\langle il\rangle}\} \subseteq U_N$, and the user $\mathbf{ID}^{\langle it\rangle} \in U$ to $\mathcal{B}$. $\mathcal{B}$ operates as follows:

(1) $\mathcal{C}$ runs the algorithm **LFIBRS** − **KeyExt** to get the corresponding public keys subring $\mathrm{PK} = \{\mathbf{PK}_{\mathbf{ID}^{\langle it\rangle}}\}_{t\in[l]}$ corresponding to the identities of l ring members, where the identity $\mathbf{ID}^{\langle it\rangle}$ ($\pi \in [l]$)

(2) Input the message μ, public keys subring $\mathrm{PK} = \{\mathbf{PK}_{\mathbf{ID}^{\langle it\rangle}}\}_{t\in[l]}$, and secret key $\mathrm{SK}_{\mathrm{ID}^{\langle it\rangle}}$; $\mathcal{C}$ runs the algorithm **LFIBRS** − **Sign** and returns the signature $(\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_l, \mathbf{v})$ of the user $\mathbf{ID}^{\langle it\rangle}$

Challenge: $\mathcal{C}$ selects μ^* and the identity subset $U^* = \{\mathbf{ID}^{\langle i1^*\rangle}, \mathbf{ID}^{\langle i2^*\rangle}, \ldots, \mathbf{ID}^{\langle il^*\rangle}\} \subseteq U_N$ and uses the master key **MK** to generate the secret keys SK_{i_0} and SK_{i_1} corresponding to ID_{i_0}, where $\mathrm{ID}_{i_1}, \mathrm{ID}_{i_0} \in U^*$. $\mathcal{C}$ randomly selects $b \in \{0, 1\}$ and then calls the signature algorithm to generate the signature σ_{i_b}.

Guess: $\mathcal{A}$ outputs bit b'.

Suppose that the signature with secret key SK_{i_0} outputs $\sigma_0 = (\sigma_{10}, \mathbf{z}_{20}, \ldots, \mathbf{z}_{l0}, \mathbf{v}_0)$ and the signature with secret key SK_{i_1} outputs $\sigma_1 = (\mathbf{z}_{11}, \mathbf{z}_{21}, \ldots, \mathbf{z}_{l1}, \mathbf{v}_1)$. $\sigma_{0,\mathrm{PP},\mathbf{ID}_{i_0},\mathrm{PK},\mathrm{SK}_{i_0}}$ is abbreviated as σ_0. $\sigma_{1,\mathbf{PP},\mathbf{ID}_{i_1},\mathrm{PK},\mathrm{SK}_{i_1}}$ is abbreviated as σ_1.

To get anonymity, we just need to prove that the signatures σ_0 and σ_1 are statistically indistinguishable. From Lemmas 7 and 8 and trigonometric inequality, we can get

$$\begin{aligned}\Delta(\sigma_0, \sigma_1) &= \Delta((\mathbf{z}_{10}, \mathbf{z}_{20}, \ldots, \mathbf{z}_{l0}, \mathbf{v}_0), (\mathbf{z}_{11}, \mathbf{z}_{21}, \ldots, \mathbf{z}_{l1}, \mathbf{v}_1))\\ &\le \Delta((\mathbf{z}_{10}, \mathbf{z}_{20}, \ldots, \mathbf{z}_{l0}), (\mathbf{z}_{11}, \mathbf{z}_{21}, \ldots, \mathbf{z}_{l1}))\\ &\le \Delta\left((\mathbf{z}_{10}, \mathbf{z}_{20}, \ldots, \mathbf{z}_{l0}), \left(D_{s_1}^{2m}\right)^l\right) + \Delta\left((\mathbf{z}_{11}, \mathbf{z}_{21}, \ldots, \mathbf{z}_{l1}), \left(D_{s_1}^{2m}\right)^l\right)\\ &\le l\Delta\left(\mathbf{z}_{i0}, D_{s_1}^{2m}\right) + l\Delta\left(\mathbf{z}_{i1}, D_{s_1}^{2m}\right).\end{aligned} \tag{8}$$

From Theorem 1, we can get $\Delta(\mathbf{z}_{i0}, D_{s_1}^{2m}) \le (2^{-\omega(\log 2m)}/M)$ and $\Delta(\mathbf{z}_{i1}, D_{s_1}^{2m}) \le (2^{-\omega(\log 2m)}/M)$, so

$$l\Delta\left(\mathbf{z}_{i0}, D_{s_1}^{2m}\right) + l\Delta\left(\mathbf{z}_{i1}, D_{s_1}^{2m}\right) \le 2l\frac{2^{-\omega(\log 2m)}}{M} = n^{-\omega(1)}. \tag{9}$$

Therefore, the proposed LFIBRS scheme is computationally anonymous under the random oracle model. □

Theorem 3 (Unforgeability). *For prime $q \ge 3$ and $m = 2n\lceil \log q \rceil$, in time $\mathcal{T}$, if there is a polynomial-time adversary $\mathcal{A}$ that can forge the effective signature of LFIBRS scheme with the probability of ϵ, then there is a polynomial-time algorithm $\mathcal{B}$ that can solve the $\mathrm{SIS}_{q,n,m,\beta}$ problem with the probability of ϵ' in time $\mathcal{T}' \approx \mathcal{T}$, where $\epsilon' \ge \epsilon - n^{-\omega(1)}$ and $\beta = 2s_1\sqrt{2m}$.*

Proof. The proof process is similar to literature [21, 22]. The analysis is as follows.

Suppose that there is a polynomial-time adversary $\mathcal{A}$ that forges the signature of LFIBRS scheme with the probability of ϵ. Next, the polynomial-time algorithm $\mathcal{B}$ is constructed to solve the $\mathrm{SIS}_{q,n,m,\beta}$ problem by using the ability of adversary $\mathcal{A}$ to forge signature.

$\mathcal{B}$ gives an example of $\mathrm{SIS}_{q,n,m,\beta}$ problem and uses the ability of $\mathcal{A}$ to give a solution.

(1) $\mathcal{B}$ selects randomly matrix $\mathbf{B}$ in $\mathbb{Z}_q^{n\times m}$

(2) $\mathcal{B}$ finds a nonzero vector $\mathbf{e} \in \mathbb{Z}_q^m$ to make $\mathbf{Be} = \mathbf{O} \bmod q$ and $\|\mathbf{e}\| \le \beta$

First of all, $\mathcal{B}$ creates three empty lists L_1, L_2, L_3 to store the queries of adversary $\mathcal{A}$, $\mathbf{H}_2$ and $\mathbf{H}_4$, and secret key. The interaction between $\mathcal{B}$ and $\mathcal{A}$ is as follows:

Setup: $\mathcal{B}$ performs the following operations to generate the public parameter **PP** and all user identities U_N and sends them to $\mathcal{A}$.

(1) Determine the maximum possible user set $U_N = \{\mathbf{ID}^{\langle 1\rangle}, \mathbf{ID}^{\langle 2\rangle}, \ldots, \mathbf{ID}^{\langle N\rangle}\}$ and a challenge user $\mathbf{ID}^{\langle i^*\rangle}$, $i^* \in [N]$

(2) For $i \in [N]$, run $\mathrm{Trapgen}(q, n, m)$ to output a matrix $\mathbf{H}_2(\mathbf{ID}^{\langle i\rangle}) = \mathbf{B}_i \in \mathbb{Z}_q^{n\times m}$ together with a short basis $\mathbf{T}_{\mathbf{B}_i}$ for $\Lambda^{\perp}(\mathbf{B}_i)$

(3) $\mathcal{B}$ calls $\mathrm{SampleMatpre}(\mathbf{B}_{i^*}, \mathbf{T}_{\mathbf{B}_{i^*}}, s, \mathbf{O})$ and outputs $\mathbf{D} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{B}_{i^*}\mathbf{D} = \mathbf{O}$

(4) Randomly select matrices $\mathbf{B}, \mathbf{C}$ in $\mathbb{Z}_q^{n\times m}$. The user's secret key is $\mathbf{T}_{\mathbf{B}_{i^*}}$ and his corresponding public key is $\mathbf{PK}_{i^*} = [\mathbf{B}|\mathbf{B}_{i^*}\mathbf{D}] \in \mathbb{Z}_q^{n\times 2m}$

(5) Output public parameters $\mathbf{PP} = (\mathbf{B}, \mathbf{C}, \mathbf{D})$ and $U_N = \{\mathbf{ID}^{\langle 1\rangle}, \mathbf{ID}^{\langle 2\rangle}, \ldots, \mathbf{ID}^{\langle N\rangle}\}$

Query: Adversary $\mathcal{A}$ can send the following query to $\mathcal{B}$, and $\mathcal{B}$ will return the query result to $\mathcal{A}$. For the identity subset $U = \{\mathbf{ID}^{\langle i1\rangle}, \mathbf{ID}^{\langle i2\rangle}, \ldots, \mathbf{ID}^{\langle il\rangle}\} \subseteq U_N$, $\mathcal{B}$ performs the following operations:

Hash query 1:

(1) $\mathcal{B}$ queries the list L_1 first. If $\mathbf{ID}^{\langle i\rangle}$ has already been queried, $\mathcal{B}$ returns $\mathbf{H}_2(\mathbf{ID}^{\langle i\rangle})$

(2) Otherwise, let $\mathbf{H}_2(\mathbf{ID}^{\langle i\rangle}) = \mathbf{B}_i$ and $\mathbf{B}_i$ is sent to $\mathcal{A}$. $\mathcal{B}$ computes $\mathbf{PK}_i = [\mathbf{B}|\mathbf{B}_i\mathbf{D}]$, and add $(\mathbf{ID}^{\langle i\rangle}, \mathbf{PK}_i, \mathbf{T}_{\mathbf{B}_i})$ to the list L_1

Hash query 2:

(1) $\mathcal{A}$ submits message μ to $\mathcal{B}$. For $i \in [l]$, $\mathcal{B}$ randomly selects $y_i \in D_{s_1}^{2m}$. $\mathcal{B}$ queries the list L_2 and returns the same result if they already have been checked

(2) Otherwise, $\mathcal{B}$ randomly selects $\mathbf{v} \in \{\mathbf{v} \in \mathbb{Z}_q^m : \|\mathbf{v}\| \le t\}$ and sends $\mathbf{v}$ to $\mathcal{A}$ and $\mathcal{B}$ adds $(\mu, U, (\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_l), \mathbf{v})$ to the list L_2

Extract query: $\mathcal{A}$ adaptively selects a user $\mathbf{ID}^{\langle i\rangle}$ ($i \in [N]$) to $\mathcal{B}$. $\mathcal{B}$ checks list L_1 to find $(\mathbf{ID}^{\langle i\rangle}, \mathbf{PK}_i, \mathbf{T}_{\mathbf{B}_i})$ and then uses $(\mathbf{ID}^{\langle i\rangle}, \mathbf{PK}_i, \mathbf{T}_{\mathbf{B}_i})$ to run $\mathrm{SampleMatpre}(\mathbf{PK}_i, \mathbf{T}_{\mathbf{B}_i}, s, \mathbf{C})$. Output $\mathbf{S}_i \in \mathbb{Z}_q^{2m\times m}$,

Table 1: Comparison of communication costs.

Scheme	Reference [21], work-1	Reference [21], work-2	[22]	This work
$\lvert\mathbf{PP}\rvert$	$(5lm + k')n\log q$	$2lmn\log q$	$2mn\log q$	$(2l+3)mn\log q$
$\lvert\mathbf{MK}\rvert$	$2lm^2\log q$	$lm^2\log q$	$m^2\log q$	$(l+1)m^2\log q$
$\lvert\mathrm{sk}\rvert$	$4lm^2\log q$	$4lm^2\log q$	$m^2\log q$	$2(l+1)m^2\log q$
$\lvert\sigma\rvert$	$2lm\log q$	$2lm\log q$	$(lm+1)\log q$	$(2lm+1)\log q$

Table 2: Comparison of time costs.

Scheme	Reference [21], work-1	Reference [21], work-2	[22]	This work
Ext – Cost	lT_1	lT_1	$T_3 + T_5 + T_8$	$(l+1)T_1 + T_7$
Sig – Cost	$nT_2 + lT_4$	$nT_2 + lT_4$	$m(l+1)T_6$	$mT_1 + lT_3$
Ver – Cost	$k(nT_5 + T_6)$	$k(nT_5 + T_6)$	$(l+1)T_5$	$(C_l^k + l + 1)T_5$

satisfying $\mathbf{PK}_i\mathbf{S}_i = \mathbf{C}$, and $\|\mathbf{S}_i\| \le s\sqrt{2m}$. Add $(\mathbf{ID}^{\langle i\rangle}, \mathbf{S}_i)$ to the list L_3.

Sign query: $\mathscr{A}$ submits message μ, the identity subset $U = \{\mathbf{ID}^{\langle i1\rangle}, \mathbf{ID}^{\langle i2\rangle}, \ldots, \mathbf{ID}^{\langle il\rangle}\} \subseteq U_N$, and the user $\mathbf{ID}^{\langle it\rangle} \in U$ to $\mathscr{B}$. $\mathscr{B}$ operates as follows:

(1) $\mathscr{B}$ checks the list L_2. If $(\mu, U, (\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_l), \mathbf{v})$ was not recorded, go to hash query 2 and record $(\mu, U, (\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_l), \mathbf{v})$ in the list L_2

(2) $\mathscr{B}$ checks the list L_3. If $(\mathbf{ID}^{\langle i\rangle}, \mathbf{S}_i)$ was not recorded, go to extract query and record $(\mathbf{ID}^{\langle i\rangle}, \mathbf{S}_i)$ in the list L_3

(3) $\mathscr{B}$ checks the lists L_2 and L_3. $\mathscr{B}$ looks for the corresponding record $(\mu, U, (\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_l), \mathbf{v})$ in L_2 and the record $(\mathbf{ID}^{\langle i\rangle}, \mathbf{S}_i)$ in L_3

(4) Let $\mathbf{z}_j = \mathbf{y}_j$ $(j \ne t)$ and $\mathbf{z}_j = \mathbf{S}_i\mathbf{v} + \mathbf{y}_j$ $(j = t)$; $\mathscr{B}$ returns the signature $(\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_l, \mathbf{v})$ of the user $\mathbf{ID}^{\langle it\rangle}$

Forgery: $\mathscr{A}$ submits message μ^*, the identity subset $U^* = \{\mathbf{ID}^{\langle i1^*\rangle}, \mathbf{ID}^{\langle i2^*\rangle}, \ldots, \mathbf{ID}^{\langle il^*\rangle}\} \subseteq U_N$, and forged signature $(\mathbf{z}_1^*, \mathbf{z}_2^*, \ldots, \mathbf{z}_l^*, \mathbf{v}^*)$ by the user $\mathbf{ID}^{\langle it^*\rangle} \in U^*$ to $\mathscr{B}$, meeting the following conditions:

(1) $\mathscr{A}$ has not asked for the private key of the user $\mathbf{ID}^{\langle it^*\rangle}$

(2) $\mathscr{A}$ did not ask for (U^*, μ^*)'s signature

The signature $(\mathbf{z}_1^*, \mathbf{z}_2^*, \ldots, \mathbf{z}_l^*, \mathbf{v}^*)$ is used in the following, which is an example of the identity subset U^*'s legal signature of message μ^* to solve the $\mathrm{SIS}_{q,n,m,\beta}$ problem given at the beginning. $\mathscr{B}$ first queries L_2 to find $(\mu^*, U^*, (\mathbf{y}_1^*, \mathbf{y}_2^*, \ldots, \mathbf{y}_l^*), \mathbf{v}^*)$. If $(\mu^*, U^*, (\mathbf{y}_1^*, \mathbf{y}_2^*, \ldots, \mathbf{y}_l^*), \mathbf{v}^*)$ does not exist, then the game is terminated immediately. Otherwise, since $(\mathbf{z}_1^*, \mathbf{z}_2^*, \ldots, \mathbf{z}_l^*, \mathbf{v}^*)$ is a legal signature, we obtain

$$\mathbf{PK}_{it^*}\mathbf{z}_{it}^* - \mathbf{C}\mathbf{v}^* = \mathbf{PK}_{it^*}\mathbf{y}_t^*. \tag{10}$$

$\mathscr{B}$ extracts the key $\mathbf{S}_{it^*}$ of $\mathbf{ID}^{\langle it^*\rangle}$ in Table L_3, and let $\mathbf{z}_i' = \mathbf{y}_i^*$ (if $i \ne t$) and $\mathbf{z}_{it}' = \mathbf{S}_{it^*}\mathbf{v}^* + \mathbf{y}_{it}^*$ (if $i = t$). It is easy to see that $(\mathbf{z}_1', \mathbf{z}_2', \ldots, \mathbf{z}_l', \mathbf{v}^*)$ is also a legal signature, so

$$\mathbf{PK}_{it^*}\mathbf{z}_{it}' - \mathbf{C}\mathbf{v}^* = \mathbf{PK}_{it^*}\mathbf{y}_t^*. \tag{11}$$

From (10) and (11), we obtain $\mathbf{PK}_{it^*}(\mathbf{z}_{it}^* - \mathbf{z}_{it}') = \mathbf{O}$.

If $\mathbf{z}_{it}^* - \mathbf{z}_{it}' = \mathbf{O}$, then the game is terminated immediately.

If $\mathbf{z}_{it}^* - \mathbf{z}_{it}' \ne \mathbf{O}$, let $\mathbf{z}_{it}^* - \mathbf{z}_{it}' = (\mathbf{e}, e')^\top$, where $\mathbf{e}, e' \in \mathbb{Z}^m$. If $\mathbf{e} = \mathbf{O}$, then the game is terminated immediately. Otherwise, $\mathbf{Be} = \mathbf{O}$. Because $\mathbf{PK}_{it^*} = [\mathbf{B}|\mathbf{H}_1(\mathbf{ID}^{\langle it^*\rangle})\mathbf{D}]$ and $\mathbf{H}_1(\mathbf{ID}^{\langle it^*\rangle})\mathbf{D} = \mathbf{O}$, it follows that $\mathbf{PK}_{it^*}(\mathbf{z}_{it}^* - \mathbf{z}_{it}') = [\mathbf{Be}|\mathbf{O}] = \mathbf{O}$; namely, $\mathbf{Be} = \mathbf{O}$. Because $\|\mathbf{e}\| \le \|\mathbf{z}_{it}^* - \mathbf{z}_{it}'\| \le \|\mathbf{z}_{it}^*\| + \|\mathbf{z}_{it}'\| \le 2s_1\sqrt{2m}$, let $\beta = 2s_1\sqrt{2m}$; it is easy to check that $\mathbf{e}$ is the solution of the $\mathrm{SIS}_{q,n,m,\beta}$ problem that is put forward at the beginning.

In the following analysis, $\mathscr{B}$ can successfully find the probability ϵ' of $\mathbf{e}$. $\mathscr{B}$ will give up the game in the three following situations, which implies that the game fails.

(1) When $(\mu^*, U^*, (\mathbf{y}_1^*, \mathbf{y}_2^*, \ldots, \mathbf{y}_l^*), \mathbf{v}^*)$ is not in L_2, the probability that $\mathbf{v}^* = \mathbf{H}_2(\sum_{i\in[l]}\mathbf{PK}_i\mathbf{z}_i - \mathbf{C}\mathbf{v}^*, \mu^*)$ passing the signature verification is $1/(2t)^{2m}$

(2) When $\mathbf{z}_{it}^* - \mathbf{z}_{it}' = \mathbf{O}$, due to $\Delta(\mathbf{z}_{it}^*, D_{s_1}^{2m}) \le (2^{-\omega(\log 2m)}/M)$ and $\Delta(\mathbf{z}_{it}', D_{s_1}^{2m}) \le (2^{-\omega(\log 2m)}/M)$, $\Delta(\mathbf{z}_{it}^*, \mathbf{z}_{it}') \le \Delta(\mathbf{z}_{it}^*, D_{s_1}^{2m}) + \Delta(\mathbf{z}_{it}', D_{s_1}^{2m}) \le 2(2^{-\omega(\log 2m)}/M)$

(3) When $\mathbf{e} = \mathbf{O}$, namely, $\mathbf{z}_{it}^* - \mathbf{z}_{it}' = [\mathbf{O}, e']^\top$ and $e' \ne \mathbf{O}$, the statistical distance between $\mathbf{z}_{it}^*$ and $\mathbf{z}_{it}'$ satisfying $\Delta(\mathbf{z}_{it}^*, \mathbf{z}_{it}') \le 8(2^{-\omega(\log 2m)}/M)$

From the above analysis, we can see that $\epsilon' \ge \epsilon - (1/(2t)^{2m}) - 10(2^{-\omega(\log 2m)}/M) = \epsilon - n^{-\omega(1)}$. □

6. Efficiency Analysis

In Table 1, we set the following:

$\lvert\mathbf{PP}\rvert$: public parameters size

$\lvert\mathbf{MK}\rvert$: master key size

$\lvert\mathrm{sk}\rvert$: secret key size

$\lvert\sigma\rvert$: signature size

From Table 1, we may conclude that the communication and time cost of our scheme are larger than those of the

scheme in [22], and only the size of private key is smaller than that of [21].

In Table 2, we set the following:

Ext – Cost: secret key extraction cost

Sig – Cost: signing cost

Ver – Cost: verification cost

T_1: the cost of RandBasis(ExtBasis)

T_2: the cost of Shamir's secret sharing operation

T_3: the cost of SampleMatpre

T_4: the cost of SamplePre

T_5: the cost of matrix product

T_6: the cost of scalar multiplication

T_7: the cost of BasisDel

T_8: the cost of matrix inversion

From Table 2, we may conclude that our scheme has higher verification cost than those in [21, 22].

7. Conclusions

In this paper, we construct a fuzzy identity ring signature scheme based on SIS problem and prove its unforgeability in random oracle model. In particular, this scheme requires that the number of ring members be equal to the number of fuzzy identity coordinates. When the number of the components of the identity vector is greater than the number of the ring members, a certain number of temporary identities can be added as the ring members, so that the number of the ring members is equal to the number of the components of the identity vector. When the number of the ring members is more than the number of the components of the identity vector, a certain number of vector components will be randomly selected from $\mathbb{Z}_q^m$ to expand the number of components of the identity vector. A signature issued under an identity ID can be verified by any identity ID$'$ that is "close enough" to the identity ID. This property allows our signature scheme to have an application in biometric authentication. Compared with the existing signature scheme of fuzzy identity, the scheme has the anonymity of ring signature which fuzzy identity signature does not have, so the efficiency of verification operation is lower. As the third step in the verification process, the worst case is to calculate C_l^k times, so when the signature scheme is used and C_l^k is too large in this paper, the verification efficiency will be very low. In the future, we hope to improve the algorithm of FIBRS to improve the efficiency of verification signature algorithm.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This research was partially supported by the Key Program of the Natural Science Foundation of Zhejiang Province of China (no. LZ17F020002) and the National Natural Science Foundation of China (no. 61772166).

References

[1] R. L. Rivest, Adi Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology*vol. 565, p. 552, Springer, Berlin, Germany, 2001.

[2] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous identification in ad hoc groups," in *Advances in Cryptology*vol. 626, p. 609, Springer, Berlin, Germany, 2004.

[3] J. Liu, K. Victor, and S. W. Duncan, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Information Security and Privacy*, pp. 325–335, Springer, Berlin, Germany, 2004.

[4] J. Herranz and G. Sáez, "Forking lemmas for ring signature schemes," in *Progress in Cryptology*, pp. 266–279, Springer, Berlin, Germany, 2003.

[5] J. Cha Choon and J. Hee Cheon, "An identity-based signature from gap diffie-hellman groups," in *Public Key*, pp. 18–30, Springer, Berlin, Germany, 2002.

[6] H. Shacham and B. Waters, "Efficient ring signatures without random oracles," in *Public Key Cryptography*, pp. 166–180, Springer, Berlin, Germany, 2007.

[7] F. Zhang, R. Safavinaini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Public Key Cryptography*, pp. 277–290, Springer, Berlin, Germany, 2004.

[8] S. H. Islam, A. K. Das, and M. K. Khan, "Design of a provably secure identity-based digital multi-signature scheme using biometrics and fuzzy extractor," *Security and Communication Networks*, vol. 9, no. 16, pp. 3229–3238, 2016.

[9] L. Deng and J. Zeng, "Two new identity-based threshold ring signature schemes," *Theoretical Computer Science*, vol. 535, pp. 38–45, 2014.

[10] L. Deng, Y. Jiang, and B. Ning, "Identity-based linkable ring signature scheme," *IEEE Access*, vol. 7, pp. 153969–153976, 2019.

[11] G. Craig, 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*, pp. 197–206, Cambridge MA USA, 2008.

[12] F. Xu and X. Lv, "A new identity-based threshold ring signature scheme," in *Proceedings of the 2011 IEEE International Conference on Systems, Man, and Cybernetics*, pp. 2646–2651, IEEE, Anchorage, AK, USA, 2011.

[13] P. L. Cayrel, R. Lindner, M. Rückert, and R. Silva, "A lattice-based threshold ring signature scheme," in *Progress in Cryptology*, pp. 255–272, Springer, Berlin, Germany, 2010.

[14] C. Aguilar Melchor, S. Bettaieb, X. Boyen, L. Fousse, and P. Gaborit, "Adapting lyubashevsky's signature schemes to the ring signature setting," in *Progress in Cryptology*, pp. 1–25, Springer, Berlin, Germany, 2013.

[15] Adi Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, pp. 47–53, Springer, Berlin, Germany, 1985.

[16] S. Amit and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*, pp. 457–473, Springer, Berlin, Germany, 2005.

[17] C. Wang and J. Kim, "Two constructions of fuzzy identity based signature," in *Proceedings of the 2009 2nd International*

Conference on Biomedical Engineering and Informatics, pp. 1–5, IEEE, Tianjin, China, 2009.

[18] P. Yang, Z. Cao, and X. Dong, "Fuzzy identity based signature with applications to biometric authentication," *Computers & Electrical Engineering*, vol. 37, no. 4, pp. 532–540, 2011.

[19] Y. Yao and Z. Li, "A novel fuzzy identity based signature scheme based on the short integer solution problem," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1930–1939, 2014.

[20] X. Zhang, C. Xu, and Y. Zhang, "Fuzzy identity-based signature scheme from lattice and its application in biometric authentication," *Ksii Transactions on Internet and Information Systems*, vol. 11, no. 5, pp. 2762–2777, 2017.

[21] Y. Zhang, Y. Hu, Y. Gan, Y. Yin, and H. Jia, "Efficient fuzzy identity-based signature from lattices for identities in a small (or large) universe," *Journal of Information Security and Applications*, vol. 47, pp. 86–93, 2019.

[22] X. Jia, D. He, Z. Xu, and Q. Liu, "An efficient identity-based ring signature over a lattice (in Chinese)," *Journal of Cryptologic Research*, vol. 4, no. 4, pp. 392–404, 2017.

[23] F.-h. Wang, Y.-p. Hu, and C.-x. Wang, "A lattice-based ring signature scheme from bonsai trees," *Journal of Electronics & Information Technology*, vol. 32, no. 10, pp. 2400–2403, 2010.

[24] J. Wang and B. Sun, "Ring signature schemes from lattice basis delegation," in *Proceedings of the international conference on information and communications security (ICICS 2011)*, pp. 15–28, Beijing, China, 2011.

[25] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the twenty-eighth annual ACM symposium on the theory of computing*, pp. 99–108, New York, NY, USA, 1996.

[26] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," *Theory of Computing Systems*, vol. 48, no. 3, pp. 535–553, 2011.

[27] D. Micciancio and C. Peikert, "Trapdoors for lattices: simpler, tighter, faster, smaller," in *Advances in Cryptology*, pp. 700–718, Springer, Berlin, Germany, 2012.

[28] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Advances in Cryptology*, pp. 523–552, Springer, Berlin, Germany, 2010.

[29] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology*, pp. 738–755, Springer, Berlin, Germany, 2011.

[30] D. Micciancio and S. Goldwasser, "Complexity of lattice problems: a cryptographic perspective," *Kluwer International Series in Engineering and Computer Science*, vol. 671, 2002.

[31] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," in *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pp. 267–302, IEEE, Rome, Italy, 2007.