A Forward-Secure Fuzzy Identity-Based Fully Homomorphic Signature over Lattices

Xiaopeng Yang Hejun Xuan and Jianping Tao

***Abstract*—A fuzzy identity-based signature (FIBS) allows a user with identity i to produce a signature that can be verified under identity j when and only when i and j are close to each other. Lattice-based cryptography is thus of high importance. Aiming to solve the unwanted disclosure of biometrics data in the biometrics applications and to enhance the computing efficiency and authentication security, adaptive security based on FIBS from lattices is proposed. On the basis of the definition and security model of the fuzzy identity fully homomorphic signature (FIFHS), the key homomorphism and partitioning technology can be used to assign values to any circuit of the signature message. The correctness and security of the scheme are derived and proved strictly, and the adaptive security existential unforgeability of the scheme under adaptive chosen message and identity attacks is reduced to the module short integer solution (MSIS) problem, which is as difficult as approximating the worst-case module-generalized independent vectors problem (Mod-GIVP).**

***Index Terms*—lattice-based cryptography; fuzzy identity fully homomorphic signature (FIFHS); forward security.**

I. Introduction

SHAMIR [1] proposed an identity-based cryptographic system. The main idea is to generate a public key from an arbitrary phone number, identity number, email, etc., and derive the corresponding private key from the key generation centre. Therefore, identity-based cryptography is a good alternative to public key infrastructure. Sahai and Waters [2] viewed each identity as a set of descriptive attributes to tolerate minor identity errors. Sahai and Waters proposed the concept of fuzzy identity-based encryption (FIBE), and an FIBS scheme was constructed from the decisional bilinear Diffie-Hellman (BDH) problem. Many FIBE schemes have emerged, such as [3], [4], [5]. Agrawal et al. [6] proposed a FIBE scheme based on learning with errors (LWE). Yang et al. [7] constructed a new cryptographic primitive called the fuzzy identity-based signature (FIBS), which is an analogue of FIBE, and constructed a FIBS scheme based on the computational Diffie-Hellman problem. Some FIBS schemes and ID-based biometric authentication schemes based on the traditional number theory assumptions, such as [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], are not immune to quantum computing attacks. In a FIBS scheme, a signer with identity i issues a signature that can be verified under identity i' when and only when identity i and identity i' are within a certain distance estimated by a certain measure. The private key associated with an identity is shared among signature generation servers rather than the master key of the public key generator. The FIBS schemes can naturally be applied to biometric identification applications.

Yang et al. [19] proposed the first FIBS scheme. A number of FIBS schemes were constructed under the assumptions of traditional number theory. However, according to Shor's work [20], traditional number theory problems can be solved using a quantum computer in polynomial time. As one of the most promising candidates for post-quantum cryptography, lattice-based cryptography has attracted significant interest in recent years due to several potential benefits: asymptotic efficiency, worst-case hardness assumptions and security against quantum computers. Inspired by the breakthrough results of Ajtai [21], lattice-based cryptography has been rapidly developing [22], [23], [24], [25]. Yao et al. [26] proposed a FIBS for the small integer solution (SIS) problem. Zhang et al. [27] constructed a FIBS scheme in which the lattice basis delegation technique is used to generate the private key, while the additive homomorphic hash function is used to obtain the homomorphic linear lattice-based signature. Zhang et al. [28] proposed a FIBS from lattices for identities in a large universe. In a homomorphic signature scheme, let f denote a Boolean circuit function. Given the public key and vector signatures $\sigma = (\sigma_1, \ldots, \sigma_l)$ for l messages $\mu = (\mu_1, \ldots, \mu_l)$, the homomorphic signature algorithm generates a signature σ' for $f(\mu)$. An arbitrary verifier can confirm the validity of the signature σ' given the tuple (σ', μ, f). Johnson et al. [29] proposed redactable signatures and set-homomorphic signatures that has the property that given a signature on a message, anyone can generate signatures on subsets of the message. Some homomorphic signature schemes are proposed, such as [30], [31], [32], [33]. The first homomorphic signature scheme can compute constant degree polynomials on signed messages [34]. A homomorphic signature scheme for a class of predicates was proposed in [35]. Inspired by [36], Wichs solved the difficulty of evaluating arbitrary circuits over signed data in homomorphic signature schemes [33]. Their scheme achieves adaptive security using chameleon hash functions. Another way to realize adaptively secure fully homomorphic signature schemes is using a normal signature plus a non-interactive zero-knowledge proof. Boyen et al. [37] constructed the first adaptively secure homomorphic signature scheme based on the short integer solution (SIS) problem that can evaluate any circuit over signed data. Zhang et al. [38] constructed a post-quantum forward-secure identity-based signature scheme from lattices and used the basis delegation technique to provide flexible key update. Wang et al. [46] constructed

Manuscript received August 18, 2020; revised February 16, 2021. This research is supported by the National Natural Science Foundation of China (Grant No.61801527, and 61802241) and the Fundamental Research Funds for the China Coast Guard Academy (Grant No. 2018FZJJA06).

Xiaopeng Yang is a Professor of Intelligence and Reconnaissance Department, China Coast Guard Academy, Ningbo 315801, China. His research interests include cryptography. Email: y_xp163@163.com.

Jianping Tao is a Professor of Intelligence and Reconnaissance Department, China Coast Guard Academy, Ningbo 315801, China. His research interests include cryptography. Email: taojianping163@163.com.

Hejun Xuan is a Professor of School of Computer and Information Technology, Xinyang Normal University, Xinyang 464000, China. His research interests include cloud/grid/cluster computing and scheduling in parallel and distributed systems. Email: xuanhejun0896@126.com

a leveled adaptively strong-unforgeable identity-based fully homomorphic signature. Ramadan et al. [47] constructed an identity-based signature with server-aided verification scheme for 5G mobile systems.

In this paper, we focus on four properties of identity-based signatures: forward security, strong unforgeability, full homomorphism, and post-quantum security. We present a forward-secure identity-based fully homomorphic signature scheme with flexible key update using the basis delegation technique from lattices. The proposed scheme is proved to be strongly unforgeable under the MSIS problem.

The rest of this paper is organized as follows. Some preliminaries are presented in Section II. The syntax and the security model of FIFHS are proposed in Section III. The proposed scheme and its security proof are presented in Section IV. Finally, the conclusion is given in Section V.

II. Preliminaries

A. Notation

Z denotes the set of integers. R denotes the set of real numbers. Random variables are denoted by upper-case italic letters (e.g., *X*). Vectors are column vectors denoted by bold lower-case letters (e.g., $\mathbf{v}$), and $\mathbf{v}^T$ denotes the transpose of $\mathbf{v}$. Matrices are sets of column vectors denoted by bold capital letters (e.g., $\mathbf{X}$). $\mathbf{I}_m$ denotes an m-order identity matrix. For a matrix $\mathbf{A} \in R^{n\times n}$, $s_1(\mathbf{A})$ denotes its spectral norm, and $\|\mathbf{A}\|_{GS}$ denotes the longest column vector of its Gram-Schmidt orthogonalization. Define a polynomial ring $R = Z[x]/\langle\Phi_m(x)\rangle$, where $\Phi_m(x) = x^{m/2}+1$ is an m-degree cyclotomic polynomial. The statistical distance between two distributions X and Y on a countable set D is defined as follows: $\Delta(X,Y) = \frac{1}{2}\sum_{d\in D}|X(d)-Y(d)|$. We say that a function $f(n)$ is $poly(n)$ if it is bounded by a polynomial in n. The notation $\omega(f(n))$ refers to the set of functions (or an arbitrary function in that set) growing faster than $c\cdot f(n)$ for any constant $c > 0$.

B. Lattices and Gaussian Distribution

Let q be prime, $\mathbf{A} \in Z_q^{n\times m}$, $\mathbf{u} \in Z_q^n$, and define the following three lattices

$$\Lambda_q(\mathbf{A}) = \{\mathbf{e} \in Z^m : \exists\ \mathbf{s} \in Z_q^n, \mathbf{e} = \mathbf{A}^T\mathbf{s}(mod\ q)\};$$

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{e} \in Z^m : \mathbf{A}\mathbf{e} = 0(mod\ q)\};$$

$$\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \{\mathbf{e} \in Z^m : \mathbf{A}\mathbf{e} = \mathbf{u}(mod\ q)\}.$$

$\rho_s(x) = \exp(\frac{-\pi\|x\|^2}{s^2})$ is the probability density function of the n-dimensional standard Gaussian distribution with centre 0 and variance s. For a lattice $\mathcal{L}$, $s > 0$, $D_{\mathcal{L},s}(x) = \frac{\rho_s(x)}{\sum_{x\in\mathcal{L}}\rho_s(x)}$ denotes the discrete Gaussian distribution over the lattice $\mathcal{L}$. For a polynomial ring R on the variable x over R, $D_{\mathcal{L},s}^{coeff}$ denotes the distribution of $a(x) = \sum_{i=0}^{n-1}a_ix^i$, of which coefficient vector $(a_0, a_1, \ldots, a_{n-1})$ follows a discrete Gaussian distribution $D_{\mathcal{L},s}$.

C. Rings

Let n be a power of 2. Let $m = 2n$. Define a polynomial ring $R = Z[x]/(x^{m/2}+1)$. For prime q, define $R_q = Z_q[x]/(x^{m/2}+1)$. The coefficient embedding is defined as follows:

$$\phi : \begin{cases} R & \to Z^n \\ \mathbf{a}(x) = \sum_{i=1}^{n} a_ix^i & \mapsto (a_0, \ldots, a_{n-1}) \end{cases}$$

The ring homomorphism $\mathbf{rot}_{\Phi_m,n} : R \to Z^{n\times n}$ maps $\mathbf{a}(x) \in R$ to a matrix over $Z^{n\times n}$, in which the i-th row vector is $\phi(x^i\cdot\mathbf{a}(x)mod\ \Phi_m(x)) \in Z^n$. An element of the R-model R^m is denoted as $\bar{\mathbf{x}} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)^T \in R^m$. Define two multiplication operations as follows: for $\bar{\mathbf{x}}, \bar{\mathbf{y}} \in R^m$, $\bar{\mathbf{x}}\otimes\bar{\mathbf{y}} = \sum_{i=1}^{n}\mathbf{x}_i\mathbf{y}_i$; For $\bar{\mathbf{x}} \in R^m$, $\mathbf{y} \in R$, $\bar{\mathbf{x}}\mathbf{y} = (\mathbf{x}_1\mathbf{y}, \mathbf{x}_2\mathbf{y}, \ldots, \mathbf{x}_n\mathbf{y})$.

lemma 1 ([39]) Let q be a prime such that $q \equiv 3(mod\ \ 8)$, and let n be a power of 2. We have the following two conclusions:

1) $\Phi_{2n}(x) = x^n+1$ splits as $x^n+1 \equiv t_1t_2(mod\ \ q)$ for two irreducible polynomials $t_1 = x^{n/2}+ux^{n/4}-1 \in Z_q[x]$ and $t_2 = x^{n/2}-ux^{n/4}-1 \in Z_q[x]$, where $u^2 \equiv -2(mod\ \ q)$. For each $\mathbf{a} \in R_q$ satisfying $\mathbf{a} \in R_q^{\times}$, are invertible and $\|\phi(\mathbf{a})\|_2 < \sqrt{q}$.
2) Let n be a power of 2, q be a prime larger than $4n$ such that $q \equiv 3(mod\ \ 8)$, and $k, k', \ell, \rho \in Z_+$ be positive integers satisfying $k', \ell \geq 1$, $k \geq 2$, and $\rho < \frac{1}{2}\sqrt{q/n}$. Define the family of hash functions $H = \{h_{\mathbf{a}}(\mathbf{x})|[-\rho,\rho]_R^k \to R_q^{k'}\}$, where $h_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}$ for $\mathbf{A} \in R_q^{k'\times k}$, $\mathbf{x} \in R_q^{k\times 1}$. Then, H is a universal hash function family. For $\mathbf{A} \in_R R_q^{k'\times k}$, $\mathbf{X} \in_R R_q^{k\times\ell}$, we have $\triangle\Big((\mathbf{A},\mathbf{A}\mathbf{X}),(\mathbf{A},U(R_q^{k'}\times\ell))\Big) \leq \frac{\ell}{2}\sqrt{\Big(\frac{q^{k'}}{(1+2\rho)^k}\Big)^n}$.

D. Important Algorithms

Definition 1 ([40]) A function $\epsilon(x)$ is negligible if, for every $m > 0$, there exists x_0 such that $\epsilon(x) \leq \frac{1}{x^m}$ for each $x \geq x_0$.

Lemma 2 ([41]) The randomized algorithm **TrapGen** outputs a vector $\mathbf{a} \in R_q^k$ and a matrix $\mathbf{T_a} \in R^{k\times k}$, where $\mathbf{rot}(\mathbf{a}^T)^T \in Z_q^{n\times nk}$ is a full-rank matrix and $\mathbf{rot}(\mathbf{T_a}) \in Z^{nk\times nk}$ is a basis for $\Lambda_q^{\perp}(\mathbf{rot}(\mathbf{a}^T)^T)$ such that $\mathbf{a}$ is $negl(n)$-close to uniform.

Lemma 3 ([42]) Let n be a power of 2 and q be a prime such that $q \equiv 3(mod\ \ 8)$. The randomized algorithm $\mathbf{e} \leftarrow \mathbf{SampleLeft}(\mathbf{a},\mathbf{b},\mathbf{u},\mathbf{T_a},\sigma)$ is defined such that given vectors $\mathbf{a},\mathbf{b} \in R_q^k$, where $\mathbf{rot}(\mathbf{a}^T)^T$ and $\mathbf{rot}(\mathbf{b}^T)^T \in Z_q^{n\times nk}$ are full-rank, an element $\mathbf{u} \in R_q$, a matrix $\mathbf{T_a} \in R^{k\times k}$ such that $\mathbf{rot}(\mathbf{T_a}) \in Z^{nk\times nk}$ is the trapdoor basis of the lattice $\Lambda^{\perp}(\mathbf{rot}(\mathbf{a}^T)^T)$, and a Gaussian parameter $\sigma \geq \|\mathbf{rot}(\mathbf{T_a})\|_{GS}\cdot\omega(\sqrt{\log nk})$, the algorithm outputs a vector $\mathbf{e} \in R^{2k}$ sampled from a distribution that is $negl(n)$-close to $D^{coeff}_{\Lambda^{\perp}_{\phi(\mathbf{u})}\left(\left[\mathbf{rot}(\mathbf{a}^T)^T|\mathbf{rot}(\mathbf{b}^T)^T\right]\right),\sigma}$, i.e., $\left[\mathbf{a}|\mathbf{b}\right]\mathbf{e}^T = \mathbf{u}$, $\phi(\mathbf{e}) \in Z^{2nk}$ is distributed according to $D_{\Lambda^{\perp}_{\phi(\mathbf{u})}\left(\left[\mathbf{rot}(\mathbf{a}^T)^T|\mathbf{rot}(\mathbf{b}^T)^T\right]\right),\sigma}$.

Lemma 4 ([39]) The randomized algorithm $\mathbf{e} \leftarrow \mathbf{Sampleright}(\mathbf{a},\mathbf{g_b},\mathbf{R},\mathbf{y},\mathbf{u},\mathbf{T_{g_b}},s)$ is defined such that given vectors $\mathbf{a},\mathbf{g_b} \in R_q^m$, where $\mathbf{b} = \mathbf{a}\mathbf{R}+\mathbf{y}\mathbf{g_b}$ such that $\mathbf{rot}(\mathbf{a}^T)^T$ and $\mathbf{rot}(\mathbf{g_b}) \in Z_q^{n\times nm}$ are full-rank matrices, elements $\mathbf{y} \in R_q^*$ and $\mathbf{u} \in R_q$, a matrix $\mathbf{R} \in R^{m\times m}$, a matrix $\mathbf{T_{G_b}} \in R^{m\times m}$ such that $\mathbf{rot}(\mathbf{T_{g_b}}) \in Z^{nm\times nm}$

is the basis of $\Lambda^{\perp}(\mathbf{rot}(\mathbf{g_b}))$, and a Gaussian parameter $s > s_1(\mathbf{R}) \cdot \|\mathbf{rot}(\mathbf{T_{g_b}})\|_{GS} \cdot \omega(\sqrt{\log nm})$, the algorithm outputs a vector $\mathbf{e} \in R^{2m}$ sampled from a distribution that is $negl(n)$-close to $D^{coeff}_{\Lambda^{\perp}_{\phi(\mathbf{u})}\left(\left[\mathbf{rot}(\mathbf{a}^T)^T|\mathbf{rot}(\mathbf{b}^T)^T\right]\right),s}$, i.e., $[\mathbf{a}|\mathbf{b}]\mathbf{e}^T = \mathbf{u}$, $\phi(\mathbf{e}) \in Z^{2nm}$ is distributed according to $D_{\Lambda^{\perp}_{\phi(\mathbf{u})}\left(\left[\mathbf{rot}(\mathbf{a}^T)^T|\mathbf{rot}(\mathbf{b}^T)^T\right]\right),s}$.

Lemma 5 ([42]) Let n be a power of 2 and q be a prime such that $q \equiv 3(mod \quad 8)$. The deterministic PPT algorithm $\mathbf{ExtBasis}(\mathbf{T_a}, \mathbf{c} = [\mathbf{a}|\mathbf{b}])$ is defined such that given vectors $\overline{\mathbf{a}} \in R_q^m$ and $\overline{\mathbf{b}} \in R_q^{\overline{m}}$, where $\mathbf{rot}(\mathbf{a}^T)^T \in Z_q^{n \times nm}$ and $\mathbf{rot}(\mathbf{b}^T)^T \in Z_q^{n \times n\overline{m}}$ are full-rank matrices, and a matrix $\mathbf{T_a} \in R^{m \times m}$ such that $\mathbf{rot}(\mathbf{T_a}) \in Z^{nm \times nm}$ is the trapdoor basis of $\Lambda^{\perp}(\mathbf{rot}(\mathbf{a}^T)^T)$, the algorithm outputs $\mathbf{T_c} \in Z_q^{(m+\overline{m}) \times (m+\overline{m})}$ such that $\mathbf{rot}(\mathbf{T_c}) \in Z_q^{n(m+\overline{m}) \times n(m+\overline{m})}$ is the trapdoor basis of $\Lambda^{\perp}\left(\left[\mathbf{rot}(\mathbf{a}^T)^T, \mathbf{rot}(\mathbf{b}^T)^T\right]\right)$.

Lemma 6 ([39]) Let the public matrix $\mathbf{g}_b = [1, b, \cdots, b^{k'-1}] \in R_q^k$ satisfying $rot(\mathbf{g}_b) \in Z^{n \times n}$ and $\|\mathbf{g}_b\|_{GS} \leq \sqrt{1+b^2}$, $k' \geq k$. There exists a deterministic polynomial time (PT) algorithm $\mathbf{g}_b^{-1}$ that inputs $\mathbf{u} \in R_q$ and outputs $\mathbf{P} = \mathbf{g}_b^{-1}(\mathbf{u})$ such that $\mathbf{g}_b\mathbf{P} = \mathbf{u}$.

Lemma 7 ([43]) The preimage sampling algorithm **PreSample** involves the input of a vector $\mathbf{a} \in R_q^k$, a short basis $\mathbf{T_a} \in R^{k \times k}$ as a trapdoor, where $\mathbf{rot}(\mathbf{a}^T)^T \in Z_q^{n \times nk}$ is a full-rank matrix and $\mathbf{rot}(\mathbf{T_a}) \in Z^{nk \times nk}$ is a basis for $\Lambda_q^{\perp}(\mathbf{rot}(\mathbf{a}^T)^T)$, a Gaussian parameter $\sigma \geq \|\mathbf{rot}(\mathbf{T_a})\|_{GS} \cdot \omega(\sqrt{\log nk})$, and a vector $\mathbf{u} \in R_q$. This algorithm works as follows: First, it chooses an arbitrary $\mathbf{t} \in R_q^k$ via the linear algebra equation $\mathbf{a} * \mathbf{t} = \mathbf{u}(mod \quad q)$ (except for a negligible fraction of $\mathbf{rot}(\mathbf{a}^T)^T$ such that $\mathbf{t}$ always exists). Then, the algorithm outputs $\mathbf{e} \leftarrow (D^{coeff}_{\Lambda^{\perp}_{\phi(\mathbf{t})}(\mathbf{rot}(\mathbf{a}^T)^T),\sigma})^k$.

Lemma 8 ([44]) Let $q > 2$, $\mathbf{A} \in Z_q^{n \times m}$, $\mathbf{R} \in Z_q^{n \times m}$. Let $\mathbf{T_A}$ be a basis of $\Lambda_q^{\perp}(\mathbf{A})$. There exists a PPT algorithm $\mathbf{NewBasis}(\mathbf{A}, \mathbf{R}, \mathbf{T_A}, \delta)$ that outputs a random basis $\mathbf{T_B}$ for $\Lambda_q^{\perp}(\mathbf{AR}^{-1})$ such that $\|\widetilde{\mathbf{T_B}}\| \leq O(\sqrt{\log_2 m})$ and $\delta \geq \|\widetilde{\mathbf{T_A}}\|\sigma_{\mathbf{R}}\sqrt{m} \cdot O(\sqrt{\log_2 m}) \cdot O(\log_2 m)$. There exists an algorithm $\mathbf{SampleRwithBasis}(\mathbf{A})$ that generates a matrix $\mathbf{R}$ sampled from $D_{m \times m}$ along with a short basis for $\Lambda_q^{\perp}(\mathbf{AR}^{-1})$ without any short basis for $\Lambda_q^{\perp}(\mathbf{A})$. This algorithm proceeds as follows:

1) Run the algorithm **TrapGen** to generate a random rank n matrix $\mathbf{B} \in Z_q^{n \times m}$ and a basis $\mathbf{T_B}$ for $\Lambda_q^{\perp}(\mathbf{B})$.
2) Sample $r_i \in Z^m$ via $\mathbf{PreSample}(\mathbf{B}, \mathbf{T_B}, a_i, \sigma_{\mathbf{R}})$ for $i \in \{1, \ldots, m\}$.
3) Output $\mathbf{R} \in Z^{m \times m}$ and the basis $\mathbf{T_B}$ for $\Lambda_q^{\perp}(\mathbf{B})$.

E. Module Short Integer Solution Problem

A module is an algebraic structure generalizing rings and vector spaces, whereas module lattices generalize both arbitrary lattices and ideal lattices. In [45], Langlois and Stehlé bridged the reduction from Mod-GIVP to MSIS.

Definition 2 ($MSIS_{q,m,\beta}$ assumption [44]) Given $\mathbf{a}_1, \cdots, \mathbf{a}_m \in R_q^k$ chosen independently from a uniform distribution, find $z_1, \cdots, z_m \in R$ such that $\sum_{i=1}^{m} z_i\mathbf{a}_i = 0(mod \quad q)$ and $0 \leq \|z\| \leq \beta$, where $\mathbf{z} = (z_1, \cdots, z_m)^t \in R_q^m$.

Theorem 1 (A reduction from Mod-GIVP to MSIS [45]) For any $d \geq 1$, $\varepsilon(N) = N^{-\omega(1)}$, there is a probabilistic polynomial time reduction from solving $Mod-GIVP_{\gamma}^{\eta_\varepsilon}$ in polynomial time (in the worst case, with high probability) to solving $MSIS_{q,m,\beta}$ in polynomial time with non-negligible probability, for any $m(N)$, $q(N)$, $\beta(N)$, $\gamma(N)$ such that $\gamma \geq \beta\sqrt{N} \cdot \omega(\sqrt{\log N})$, $q \geq \beta\sqrt{N} \cdot \omega(\log N)$ and $m, \log q \leq poly(N)$.

III. FIFHS and the Security Model

$\mathcal{M}$ denotes the plaintext space. $C : \mathcal{M}^l \rightarrow \mathcal{M}$ denotes a circuit that inputs l plaintexts and outputs a plaintext. The forward-secure FIFHS consists of the following five algorithms:

- $Setup(1^{\kappa}, 1^l, parameter)$ takes the security parameter 1^{κ}, the maximum size l for the message set, and the public parameter as inputs and outputs the master public key mpk and public key pk.
- $Extract(pk, mpk, \omega)$ takes pk, mpk and the identity $\omega = \{\omega_i\}_{i=1}^{\ell}$ as inputs and outputs the private key $sk_{\omega,1}$.
- $Update(pk, sk_{\omega,j}, \omega)$ Given pk, the current secret key $sk_{\omega,j}$ of a user ω at the current time period $j \leq d-1$, the algorithm computes an updated secret key $sk_{\omega,i}$ for user ω at update time period i $(j \leq i \leq d)$.
- $Sign(\tau, i, sk_{\omega,i}, \mu)$ takes the index $\tau \in \{0,1\}^{\kappa}$, a private key $sk_{\omega,i}$ associated with an identity ω at the current time period $i \leq d$, a message μ and its corresponding index i as inputs and outputs the signature $\sigma_{\omega,\mu}$.
- $Eval(pk, \tau, \mu, \sigma, C)$ takes the public key pk, index τ, message sequence μ, signature sequence σ and circuit C as inputs and outputs the signature $\sigma'_{\omega,\mu'}$ for the evaluation message $\mu' = C(\mu)$.
- $Verify(pk, \eta, \tau, \mu, \sigma_{\omega,\mu}, C)$ takes pk, identity $\eta = \{\eta_i\}_{i=1}^{\ell}$ $(|\eta \cap \omega| \geq t)$, index τ, message μ, signature $\sigma_{\omega,\mu}$, and circuit C as inputs outputs 1 if the verification is successful.

For any index $\tau \in \{0,1\}^{\lambda}$, any circuit C, any message μ, any index $i \in [l]$, identities $\omega = \{\omega_i\}_{i=1}^{\ell}$ and $\eta = \{\eta_i\}_{i=1}^{\ell}$ satisfying $|\eta \cap \omega| \geq t$, FIFHS satisfies consistency if the following two equations hold

$$Pr[Verify(pk, \eta, \mu, Sign(\tau, i, sk_{\omega,i}, \mu))] = 1;$$

$$Pr[Verify(pk, \tau, \mu', \sigma'_{\omega,\mu'}, C)] = 1.$$

For $i \in [l]$, σ_i is the signature generated by $Sign(sk_{\omega,i}, \tau, i, \mu_i)$, and σ' is the signature for evaluation circuit $\mu' = C(\mu)$ obtained by $Eval(pk, \tau, \mu, \sigma, C)$.

Let ε denote a FIFHS scheme, $\mathcal{F}$ denote a PPT adversary, and $\mathcal{D}$ denote a challenger. The notion of existentially unforgeable homomorphic signatures against adaptively full chosen message and identity attacks (EU-FH-ACMIA) is defined as follows:

- $Setup$: $\mathcal{D}$ runs the $Setup$ algorithm and provides the adversary $\mathcal{F}$ the public parameters.
- $Stage$ 1 : $\mathcal{F}$ declares the target identity $\omega^* = \{\omega_i^*\}_{i=1}^{\ell}$.
- $Stage$ 2 : $\mathcal{F}$ adaptively issues private key queries and signature queries for any identity $\omega = \{\omega_i\}_{i=1}^{\ell}$ satisfying $|\omega \cap \omega^*| < t$.
- $Stage$ 3 : $\mathcal{F}$ makes a number of different queries to the challenger $\mathcal{C}$.
  - $Extract\ Query$: $\mathcal{F}$ issues an extract query for any identity $\omega = \{\omega_i\}_{i=1}^{\ell}$ satisfying $|\omega \cap \omega^*| < t$;

$\mathcal{C}$ then runs the $Extract$ algorithm to obtain the private key sk_ω and sends it to $\mathcal{F}$.

- $Sign\ Query$: $\mathcal{F}$ can query for a dataset index $i \in 2^\kappa$, for a message index $j \in [l]$, a message $\mu_{ij} \in \mathcal{M}$, and any identity $\eta^{(j)} = \{\eta_i^{(j)}\}_{i=1}^{\ell}$ satisfying $|\eta^{(j)} \cap \omega^*| < t$. $\mathcal{F}$ assigns a random tag $\tau_i \in \{0,1\}^\kappa$ to the dataset i, then runs $Extract$ to obtain the private key $sk_{\eta^{(j)}}$, and finally runs $Sign(\tau_i, j, sk_{\eta^{(j)}}, \mu_{ij})$ to obtain the signature $\sigma_{\eta^{(j)},\mu_{ij}}$.

- $Output$: $\mathcal{F}$ outputs $(\omega^*, \mu^*, \sigma^*_{\omega^*,\mu^*})$. If the set in $\omega^* \cap \eta^{(j)}$ was not submitted to the $Extract\ Query$ and the $Sign\ Query$, respectively, and $Verify(pp, \omega^*, \mu^*, \sigma^*_{\omega^*,\mu^*}) = 1$.

$\mathcal{F}$ wins if $Verify(pp, \omega^*, \mu^*, \sigma^*_{\omega^*,\mu^*}) = 1$, and either

1) $\tau^* \neq \tau_i$ for all i or
2) $\tau^* = \tau_i$ for some i, but $\mu^* \neq C^*(\mu_i)$, where $\mu_i = (\mu_{i1}, \ldots, \mu_{il})$ is the vector of messages queried under a common tag τ_i but differing indices $j \in [l]$.

$\mathcal{F}$'s probability of success $Adv^{FIFH}_{EU-FH-ACMIA}(\mathcal{F}, \varepsilon)$ is defined as follows:

$$Pr[Verify(pp, \omega^*, \mu^*, \sigma^*_{\omega^*,\mu^*}) = 1].$$

If $Adv^{FIFH}_{EU-FH-ACMIA}(\mathcal{F}, \varepsilon)$ is negligible in the security parameter κ, we say the signature scheme satisfies EU-FH-ACMIA security.

IV. Forward-Secure FIBFHS over Lattices

Each dataset should be associated with a unique random tag τ that is used for signing and verification. τ consists of two components: $\mathbf{t} \in \{0,1\}^\lambda$ and $\mathbf{b} \in \{0,1\}^l$. The first bit is fixed to $\mathbf{t}[0] = 0$. We use the lattice mixing technique for $\mathbf{t} \in \{0,1\}^\lambda$ to realize adaptive security. $\mathbf{b} \in \{0,1\}^l$ is used to prove adaptive security. Let $H : \{0,1\}^* \to R_q^m$ be a hash function.

A. Construction

- $Setup$: Input security parameter 1^λ, the maximum number ℓ of inputs for the circuit family C, the number of bits $|\tau|$ ($|\tau| = |\mathbf{t}| + |\mathbf{b}| = \lambda + \ell$) for the tag, and the maximum depth $d_{\max}$ of the circuit family C.
  1) Set $n = n(\lambda, d_{\max})$, $q = q(n, d_{\max})$, and $m = m(n, d_{\max})$. Let the Gaussian parameters be $s_1 = s_1(n)$ and $s_2 = s_2(n)$.
  2) Run the algorithm $(\mathbf{a}, \mathbf{T_a}) \leftarrow$ **TrapGen** to generate one random matrix $\mathbf{a} \in R_q^m$ with its associated trapdoor $\mathbf{T_a} \in R_q^{m\times m}$.
  3) Sample $1 + 2\ell$ random matrices $\mathbf{f} \in R_q^m$ and $\mathbf{d}_{i\in[\ell],\tau\in\{0,1\}} \in R_q$ and $|\mathbf{t}|$ random matrices $\{\mathbf{w}_i\}_{i\in[\mathbf{t}]} \in R_q^m$.
  4) Output the master secret key $msk = \mathbf{T_a}$ and the public parameters $(\mathbf{a}, \mathbf{f}, \mathbf{g}_b, \mathbf{d}_{i\in[\ell],\tau\in\{0,1\}}, \{\mathbf{w}_i\}_{i\in[\mathbf{t}]})$.
- $Extract$: Given inputs pk, mpk, the identity $\omega = \{\omega_i\}_{i=1}^{\ell}$ and an initial time period $i = 1$, the key generation centre generates the private key as follows:
  1) Define $\mathbf{w} = \sum_{i=1}^{|\mathbf{t}|}(-1)^{\mathbf{t}[i]}\mathbf{w}_i$ and set $\mathbf{a_t} = (\mathbf{a}|\mathbf{b} + \mathbf{w}) \in R_q^{2m}$ to denote the dataset matrix.
  2) Run **ExBasis**$(\mathbf{a}, \mathbf{T_a}, \mathbf{b}+\mathbf{w})$ to generate the trapdoor $\mathbf{T_{a_t}}$ for the lattice $\Lambda^\perp(\mathbf{a}|\mathbf{b} + \mathbf{w})$.
  3) Let $R_{\omega\|1} = H(\omega\|1)$, and run $\mathbf{T}'_{\mathbf{a_t},\omega\|1} \leftarrow$ **NewBasisDel**$(\mathbf{a_t}, R_{\omega\|1}, \mathbf{T_{a_t}}, s_1)$.
  4) Output the private key $\{\mathbf{T}'_{\mathbf{a_t},\omega\|1}\}$.
- $Update$: Upon input of the public parameter, the current time period $i \leq d$, and $\mathbf{T}'_{\mathbf{a_t},\omega\|j}$, which denotes the signing secret key associated with the previous time period $j < i$, the user with identity ω performs the following steps to update his signing secret key:
  1) Compute $R_{\omega\|j} = H(\omega\|j) \cdots H(\omega\|1)$ and compute $\mathbf{a}_{\omega\|j} = \mathbf{a_t} \cdot R^{-1}_{\omega\|j}$ as the public key in time period j with respect to signing secret key $\mathbf{T}'_{\mathbf{a_t},\omega\|1}$.
  2) Let $R_{j\to i} = H(\omega\|i) \cdots H(\omega\|j+1)$, and compute $\mathbf{T}'_{\mathbf{a_t},\omega\|i} \leftarrow$ **NewBasisDel**$(\mathbf{a}_{\omega\|j}, R_{j\to i}, \mathbf{T}_{\mathbf{a}_{\omega\|i}}, s_i)$. Note that $\mathbf{T}'_{\mathbf{a_t},\omega\|i}$ is a short basis of $\Lambda^\perp(\mathbf{a}_{\omega\|j})$, where $\mathbf{a}_{\omega\|i} = \mathbf{a}_{\omega\|j} \cdot R^{-1}_{j\to i}$, and $R_{\omega\|i} = H(\omega\|i) \cdots H(\omega\|1)$.
- $Sign$: Upon input of the public parameter, an identity ω, and a message $\mathbf{u} = (u_1, \ldots, u_n) \in Z_q^n$, the signer generates the fuzzy identity-based fully homomorphic signature as follows:
  1) For each $i \in [\ell]$, choose a uniform random polynomial $f_i(x) \in Z_q[x]$ of degree t such that $f_i(0) = u_i$.
  2) Let $\widehat{u_i} = (f_1(i), \ldots, f_\ell(i)) \in R_q$ such that $\mathbf{u} = \sum_{i=1}^{\ell} l_i \cdot \widehat{u_i}$, where $l_i = \prod_{j\neq i} \frac{-i}{j-i}$.
  3) Let $\mathbf{u}' = C(\mathbf{u})$, run

     $$\textbf{SampleLeft}(\mathbf{a}, \mathbf{T}'_{\mathbf{a_t},\omega\|i}, \mathbf{a}_{\omega\|i}, \mathbf{d}_{i,\tau} + \mathbf{g}_b(\mathbf{u}' + \widehat{u_i}), s_2)$$

     to generate a vector $(\mathbf{r}_{i,1}|\mathbf{r}_{i,2}) \in R_q^{2m}$. That is, $(\mathbf{r}_{i,1}|\mathbf{r}_{i,2})$ satisfies the following equation:

     $$\mathbf{a}_{\omega\|i} \otimes (\mathbf{r}_{i,1}|\mathbf{r}_{i,2})^T = \mathbf{d}_{i,\tau} + \mathbf{g}_b(\mathbf{u}' + \widehat{u_i})(mod\ q).$$
  4) Output the signature $\{\mathbf{u}', (\mathbf{r}_{i,1}|\mathbf{r}_{i,2})_{i\in[\ell]}, \omega\}$.
- $Verify$: To verify the signature $\{\mathbf{u}', (\mathbf{r}_{i,1}|\mathbf{r}_{i,2})_{i\in[\ell]}, \omega\}$ with respect to the identity $\omega = \{\omega_1, \ldots, \omega_\ell\}$ against an identity $\eta = \{\eta_1, \ldots, \eta_\ell\}$, let $I \subseteq [\ell]$ denote the set of matching bits in ω and η. If $|I| = |\omega \cap \eta| < t$, the receiver outputs 0; otherwise, the receiver executes the following steps:
  1) Parse the index $\tau = (\mathbf{t}|\mathbf{b}) \in \{0,1\}^{\lambda+\ell}$, and parse the signature $\sigma_i = (\mathbf{r}_{i,1}|\mathbf{r}_{i,2})$.
  2) Compute $\mathbf{w} = \sum_{i=1}^{|\mathbf{t}|}(-1)^{\mathbf{t}[i]}\mathbf{w}_i$, set $\mathbf{a_t} = (\mathbf{a}|\mathbf{b} + \mathbf{w}) \in R_q^{2m}$.
  3) Compute $\mathbf{e}_i = \mathbf{g}_b^{-1}[\mathbf{a}_{\omega\|i}(\mathbf{r}_{i,1}|\mathbf{r}_{i,2})^T - \mathbf{d}_{i,\tau} - \mathbf{g}_b\mathbf{u}']$.
  4) Verify $\mathbf{u} = \sum_{j\neq i} l_i \cdot \mathbf{a}_{\omega\|i} \otimes \mathbf{e}_i^T$, where $l_i = \prod_{j\neq i} \frac{-i}{j-i}$.
- $Eval$: Upon input of the public key pk, index τ, message sequence μ, signature sequence σ and circuit C, the evaluation algorithm executes the following steps:
  1) Suppose the gate $g = (u, v, w)$ is a $NAND$ gate. For each wire in the gate, let $\mathbf{d}_i$ denote the public matrix associated with that wire. Construct the dataset matrix $\mathbf{w} = \sum_{i=1}^{|\mathbf{t}|}(-1)^{\mathbf{t}[i]}\mathbf{w}_i$, let $\mathbf{a_t} = (\mathbf{a}|\mathbf{b} + \mathbf{w}) \in R_q^{2m}$.
  2) Let (x, y) be the values carried by wires (u, v). Compute $\mathbf{a}_{\omega\|i} \otimes \mathbf{r}_u = \mathbf{d}_u + \mathbf{g}_b x$, $\mathbf{a}_{\omega\|i} \otimes \mathbf{r}_v = \mathbf{d}_u + \mathbf{g}_b y$.

3) Define $\mathbf{d}_w = \mathbf{d}_v\widetilde{\mathbf{d}_u} + (y\widetilde{\mathbf{d}_u} + \widehat{u_i}\widetilde{\mathbf{d}_u} - y\mathbf{d}_u - y\widehat{u_i})\mathbf{g}_b$, where $\widetilde{\mathbf{d}_u} = \mathbf{g}_b^{-1}(\mathbf{d}_u)$.
4) Output $\mathbf{r}_w = \mathbf{r}_v\widetilde{\mathbf{d}_u} - y\mathbf{r}_u$.

B. Correction

Let $\sigma_i = (\mathbf{r}_{i,1}|\mathbf{r}_{i,2})$ be the signature for message $\mathbf{u}'$ under the tag $\tau = (\mathbf{t}|\mathbf{b})$. By the construction of algorithm $Sign$, we have

$$\mathbf{a}_{\omega\|i} \otimes (\mathbf{r}_{i,1}|\mathbf{r}_{i,2})^T = \mathbf{d}_{i,\tau} + \mathbf{g}_b(\mathbf{u}' + \widehat{u_i})(mod\ q).$$

Let $\mathbf{r}_u$ and $\mathbf{r}_v$ be signatures for messages x and y, respectively, under public keys $\mathbf{d}_u$ and $\mathbf{d}_v$, such that

$$\mathbf{a}_{\omega\|i} \otimes \mathbf{r}_u = \mathbf{d}_u + (x + \widehat{u_i})\mathbf{g}_b,$$

$$\mathbf{a}_{\omega\|i} \otimes \mathbf{r}_v = \mathbf{d}_v + (y + \widehat{u_i})\mathbf{g}_b.$$

Compute

$$\begin{aligned} \mathbf{a}_{\omega\|i} \otimes \mathbf{r}_w &= \mathbf{a}_{\omega\|i} \otimes (\mathbf{r}_v \cdot \widetilde{\mathbf{d}_u} - y\mathbf{r}_u) \\ &= \mathbf{a}_{\omega\|i} \otimes \mathbf{r}_v\widetilde{\mathbf{d}_u} - \mathbf{a}_{\mathbf{t}} \otimes y\mathbf{r}_u \\ &= \mathbf{d}_v + (y + \widehat{u_i})\mathbf{g}_b\widetilde{\mathbf{d}_u} - y\mathbf{d}_u + (x + \widehat{u_i})\mathbf{g}_b \\ &= \mathbf{d}_w + (1 - xy)\mathbf{g}_b\widehat{u_i} \\ &= \mathbf{d}_w + (x\ NAND\ y)\mathbf{g}_b\widehat{u_i} \end{aligned} \tag{1}$$

C. Security

Theorem 2 For a prime modulus $q = poly(n)$, if there is a PPT forger $\mathcal{F}$ that outputs an EU-FH-ACMIA forgery with probability ε in time t, then there is a PPT algorithm $\mathcal{B}$ that solves the $MSIS_{q,n,m}$ assumption in time $t' \approx t$ and with probability $\varepsilon' \geq \varepsilon \cdot \frac{1-3^{-k}}{Q_{id}} \cdot (1 - \frac{Q_e}{Q_{id}}) \cdot (1 - \frac{Q_s}{Q_{id}})$, where Q_{id}, Q_e, and Q_s are the maximal numbers of hash queries, extract queries and sign queries made by $\mathcal{F}$, respectively.

Proof: Assume there exists a PPT adversary $\mathcal{F}$ who wins the unforgeability security game defined above; we construct a reduction $\mathcal{B}$ that can leverage the adversary $\mathcal{F}$ to break the $MSIS_{q,n,m}$ assumption.

$Setup$. $\mathcal{D}$ sends the public key and the public parameters to $\mathcal{F}$. $\mathcal{D}$ randomly chooses $|\mathbf{t}|$ vectors $\{\mathbf{s}_i\}_{i\in[|\mathbf{t}|]} \in R_q^m$. Select $|\mathbf{t}|$ uniformly random scalars $h_0, \ldots, h_{|\mathbf{t}|} \in Z_q$, and randomly select $(1+2\ell)$ vectors $\mathbf{x}, \mathbf{x}_{i,b} \in R_2^m$. Set $\mathbf{a} = \mathbf{a}^*\mathbf{x}$. Set the public key $pk = (\mathbf{a}, \mathbf{a}^*, \mathbf{g}_b, \{\mathbf{d}_{i,\tau} = \mathbf{a}^* \otimes \mathbf{x}_{i,b}\}_{i\in[\ell],b\in\{0,1\}}, \{\mathbf{t}_i = \mathbf{a}^* \otimes \mathbf{s}_i + h_i\mathbf{g}_b\}_{i\in[|\mathbf{t}|]})$.

$Stage\ 1$: $\mathcal{F}$ declares the target identity $\omega^* = \{\omega_i^*\}_{i=1}^{\ell}$.

$Stage\ 2$: For any identity $\omega = \{\omega_i\}_{i=1}^{\ell}$ such that $|\omega \cap \omega^*| < t$, $\mathcal{F}$ sends the private key query and signature query.

$Extract\ Query$. Although $\mathcal{C}$ does not know the master private key, $\mathcal{C}$ can construct a private key for ω. Given $\omega = \{\omega_1, \ldots, \omega_\ell\}$, $\mathcal{C}$ returns $\{\mathbf{T}'_{\mathbf{a_t},j}\}_{j\in[\ell]}$ to $\mathcal{F}$. $\mathcal{C}$ samples $\mathbf{r}_{j,\omega_j} \leftarrow Z^{n\times n}$ and runs **SampleRwithBasis** to obtain the short basis $\mathbf{T}'_{\mathbf{a_t},j}$ for the lattice $\Lambda_q^{\perp}(\mathbf{a} \cdot \mathbf{r}_{j,\omega_j}^{-1})$.

$Hash\ Query$. $\mathcal{F}$ may adaptively query the random oracle H on any identity, any time period i and any message of its choice. To respond consistently to these queries, $\mathcal{D}$ maintains a list $\mathcal{L}$ that is initially empty, and the simulator simply returns the same output on the same input without incrementing the query counter Q_{id}. $\mathcal{D}$ answers the Q-th query as follows.

1) For $Q = Q^*$, set $H(\omega\|i) = R_i^*$, store $(\omega, i, R_i^*, *, *)$ in $\mathcal{L}$, and return R_i^* as the oracle $H(\omega\|i)$'s value.
2) For $Q \neq Q^*$, compute $\mathbf{a}_i = \mathbf{a} \cdot (\overset{*}{R}_{i-1} \cdots \overset{*}{R}_2 \overset{*}{R}_1)^{-1}$, run $(R_i, \mathbf{T_b}) \leftarrow$ **SampleRwithBasis**$(\mathbf{a}_i)$, save the tuple $(\omega, i, R_i, \mathbf{b}, \mathbf{T_b})$ in $\mathcal{L}$, and return R_i as the value of $H(\omega\|i)$.

$Sign\ Query$. Reduction $\mathcal{B}$ answers adaptive message queries from $\mathcal{F}$ on any message as follows. $\mathcal{C}$ answers all the queries from $\mathcal{F}$ and executes the following operations:

1) Select a random index $\tau = (\mathbf{t}|\mathbf{b}) \in \{0,1\}^{\lambda+\ell}$, and restrict $\mathbf{t}[0] = 0$.
2) Compute $\mathbf{t_t} = \sum_i(-1)^{\mathbf{t}_i[i]}\mathbf{t}_i$, $\mathbf{h}_i = \sum_i(-1)^{\mathbf{t}_i[i]}\mathbf{h}_i$.
3) Compute $\mathbf{a_t} = (\mathbf{a}|\mathbf{b} + \mathbf{t_t})$. For each $i \in [\ell]$, run **SampleRight**$(\mathbf{a}^*, \mathbf{g}_b, \mathbf{u} + \sum_i(-1)^{\mathbf{t}[i]}\mathbf{s}_i, \mathbf{t}_{\mathbf{g}_b}, \mathbf{d}_{i,\mathbf{b}[i]} + \mathbf{u}_i\mathbf{g}_b, s_3)$ to generate $(\mathbf{r}_{i,1}|\mathbf{r}_{i,2})$.
4) Output the index $\tau = (\mathbf{t}|\mathbf{b}) \in \{0,1\}^{\lambda+\ell}$ and the signature $\sigma = \{\sigma_i\}_{i\in[\ell]}$.
5) Increment the counter.

$Output$. Reduction $\mathcal{B}$ receives a forgery tuple from $\mathcal{F}$.

1) If the type of forgery submitted by adversary $\mathcal{F}$ is different than the type initially guessed by the reduction, then abort the simulation.
2) Otherwise, construct a solution to the $MSIS_{q,n,m}$ challenge as follows: $\mathcal{F}$ computes the index vector and the scale $\mathbf{t}^* = \sum_i(-1)^{\mathbf{t}_i[i]}\mathbf{t}_i$ and $\mathbf{h}^* = \sum_i(-1)^{\mathbf{t}_i[i]}\mathbf{h}_i$.

We have $[\mathbf{a}^*|\mathbf{a}^*(\mathbf{x} + \sum_i(-1)^{\mathbf{t}^*[i]}\mathbf{s}_i)] \otimes (\mathbf{r}_{i,2}|\mathbf{r}_{i,1})^T = \mathbf{d}_C + \mathbf{g}_b(\mathbf{u}^* + \widehat{u_i})$. There exists a vector $\mathbf{k} \in R_q$, such that $\mathbf{d}_C = \mathbf{a}^* \otimes \mathbf{u}_C + \mathbf{k} \cdot \mathbf{g}_b$ and the following equation holds with an overwhelming advantage $\mathbf{a}^*(\mathbf{r}_{i,2}^* + (\mathbf{u} + \sum_i(-1)^{\mathbf{t}^*[i]}\mathbf{s}_i)\mathbf{r}_{i,1}^* - \mathbf{u}_C) = (\mathbf{k} + \mathbf{u}^*)\mathbf{g}_b = 0$. Since the proof is exactly the same as that of Lemma 4.4 of [37], we omit it here. Since there are exponentially many choices of $\mathbf{s}_i$ values that would result in the same view of the adversary. Therefore, the probability that the term on the right-hand side vanishes is negligible. If $\mathbf{k}+\mathbf{u}^* = 0$, $(\mathbf{r}_{i,2}^* + (\mathbf{u} + \sum_i(-1)^{\mathbf{t}^*[i]}\mathbf{s}_i)\mathbf{r}_{i,1}^* - \mathbf{u}_C)$ is the solution for the $MSIS_{q,n,m}$ assumption; otherwise, output $(\mathbf{r}_{i,2}^* + (\mathbf{u} + \sum_i(-1)^{\mathbf{t}^*[i]}\mathbf{s}_i)\mathbf{r}_{i,1}^* - \mathbf{u}_C)\mathbf{T}_{\mathbf{g}_b}$ as the solution. Furthermore, $\mathcal{B}$ completes $Extract\ Query$ and $Sign\ Query$ without aborting with probability at least $(1 - \frac{Q_e}{Q_{id}})(1 - \frac{Q_s}{Q_{id}})$. Therefore, we can deduce that $(\mathbf{r}_{i,2}^* + (\mathbf{u} + \sum_i(-1)^{\mathbf{t}^*[i]}\mathbf{s}_i)\mathbf{r}_{i,1}^* - \mathbf{u}_C)$ is a short non-zero preimage of $\mathbf{0}$ under $\mathbf{a}^*$ with probability $\varepsilon' \geq \varepsilon \cdot \frac{1-3^{-k}}{Q_{id}} \cdot (1 - \frac{Q_e}{Q_{id}}) \cdot (1 - \frac{Q_s}{Q_{id}})$.

D. Application to Biometric Authentication

- Enrolment Phase
  1) User A uses his biometric data in an enrolment phase. The properties of his biometric data are measured with specialized equipment and modelled as a feature vector.
  2) Run **NewBasisDel** to generate the private key s_ω.
  3) User name A is used as the signed message. Run $Sign(PP, s_\omega, A, \omega)$ to generate the reference data $(\mathbf{r}_{i,2}|\mathbf{r}_{i,1})_{i\in[\ell]}$. The certification authority stores $\mathbf{d}_{i,\tau}$, the reference data $(\mathbf{r}_{i,2}|\mathbf{r}_{i,1})_{i\in[\ell]}$ and the biometric measurement data $\omega = \{\omega_1, \ldots, \omega_\ell\}$.
  4) The certification authority erases the private key s_ω and the user name.
- Authentication/Verification Phase

1) Each user sends his biometric measurement data to the certification authority.
2) User B computes his biometric measurement data and his biometric measurement data η, randomly chooses $\varepsilon_i \in R_q^2$, and sends them to the certification authority.
3) The certification authority finds $(\mathbf{r}_{i,2}|\mathbf{r}_{i,1})_{i\in[\ell]}$ and the biometric measurement data ω by searching user name A.
4) The certification authority computes the set $I = \omega \cap \eta$, returns $\{\xi_i = (\mathbf{r}_{i,2}|\mathbf{r}_{i,1}) \otimes \varepsilon_i\}_{i\in[\ell]}$, his own biometric measurement data η, and his own user name to B.
5) User B computes $\{(\mathbf{r}_{i,2}|\mathbf{r}) = \xi_i \otimes \varepsilon_i^{-1}\}_{i\in[\ell]}$, computes $\mathbf{e}_i = \mathbf{g}_b^{-1}[\mathbf{a_t}(\mathbf{r}_{i,1}|\mathbf{r}_{i,2})^T - \mathbf{d}_{i,\tau} - \mathbf{g}_b\mathbf{u}']$, and verifies whether the following equation holds: $\mathbf{u} = \sum_{j\neq i} l_i \cdot \mathbf{a_t} \otimes \mathbf{e}_i^T$, where $l_i = \prod_{j\neq i} \frac{-i}{j-i}$.

E. Performance Analysis

It is assumed that the output of the hash algorithm is 128 bits and that the random number is 128 bits according to the NIST security parameter. Let n denote the lattice dimension, t_h denote the operation time of the hash function, t_p denote polynomial multiplication, t_g denote the Gaussian sampling algorithm, t_d denote dot multiplication, ℓ denote the length of the identity (attribute), and $|\omega|$ denote the length of the fuzzy identity. Table 1 compares the running times. We implemented these cryptography operations using the C/C++ PBC library on a 64-bit Windows 10 Thinkpad X1 notebook and a 64-bit Ubuntu 14.4 LTS Think Center desktop, as shown in Table 2, with $t_h = 0.3$ ms, $t_d = 0.28$ ms, $t_p = 0.45$ ms, $t_g = 0.52$ ms, $t_d = 0.27$ ms, $n = 128$, $m = 256$, and $\ell = 50$. Table 3 compares the communication overhead and computation overhead. In addition, Table 4 shows the concrete sizes of the related schemes when $n = 256$, $q = 12289$, $\ell = 50$, and $|\omega| = 25$. Table 5 gives the security comparison. Figure 1 shows the sizes of PK for $\ell = 10$, $q = 12289$. Figure 2 shows the sizes of SK for $\ell = 10$, $q = 12289$. Figure 3 shows the sizes of communication overhead for $\ell = 10$, $q = 12289$.

Table 1. Time Comparison

Scheme	Enrolment Phase	Authentication Phase
Ours	$2\ell m t_g$	$2\ell m t_p$
[26]	$nt_h + \ell n t_p + 2\ell m t_g$	$nt_h + 2\ell m t_p$
[27]	$nt_h + \ell n t_p + 2\ell m t_g$	$nt_h + 2\ell m t_p$
[28]	$nt_h + \ell n t_p + 2\ell m t_g$	$nt_h + 2\ell m t_p$

Table 2. Concrete Time Comparison

Scheme	Enrolment Phase	Authentication Phase
Ours	13312 ms	11520 ms
[26]	16230 ms	11558 ms
[27]	16230 ms	11558 ms
[28]	16230 ms	11558 ms

Table 3. Overhead Comparison

Scheme	PK	SK	Communication Overhead
Ours	$2n^2 \log q$	$2\ell n^2 \log q$	$\|\omega\| + (4\ell n^2 + n) \log q$
[26]	$8\ell n^2 \log^2 q$	$4\ell n\sqrt{n} \log^2 q$	$\|\omega\| + 4\ell n\sqrt{n} \log^2 q$
[27]	$5n^2 \log^2 q$	$5\ell n^2 \log^2 q$	$\|\omega\| + 5n^2(\ell+1) \log^2 q$
[28]	$6\ell n^2 \log^2 q$	$16\ell n^2 \log^2 q$	$\|\omega\| + 4\ell n^2 \log^2 q$

Table 4. Concrete Overhead Comparison

Scheme	PK	SK	Communication Overhead
Ours	217 KB	1359 KB	2718 KB
[26]	591000 KB	18469 KB	18468 KB
[27]	7388 KB	369376 KB	376764 KB
[28]	443251 KB	1182003 KB	295501 KB

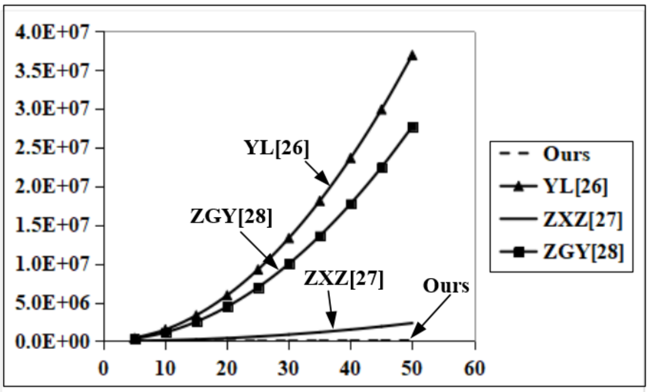

Fig. 1. Comparison for PK Sizes

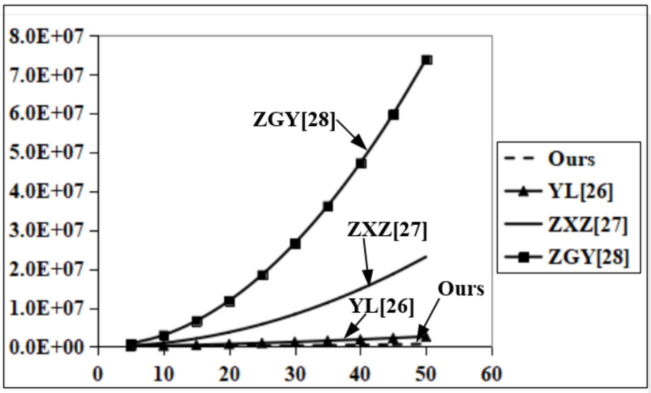

Fig. 2. Comparison for SK Sizes

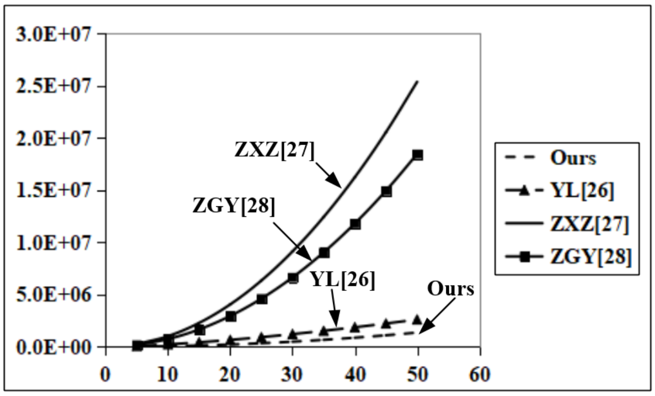

Fig. 3. Comparison for Communication Overhead

Table 5. Security Comparison

Scheme	Adaptive Security	Homomorphism	Forward Security
Ours	√	√	√
[26]	×	×	×
[27]	×	×	×
[28]	×	×	×
[46]	√	√	×

V. Conclusion

In this paper, we proposed a new construction for lattice-based fuzzy identity-based signatures with flexible key update that is fully homomorphic. The proposed scheme is proved to be existentially unforgeable under an adaptively full chosen message and identity attacks based on the MSIS problem, which is as difficult as approximating the Mod-GIVP assumption in the worst case. Compared with the previous lattice-based FIFHS schemes, our proposed FIFHS scheme is efficient, especially in terms of the communication overhead. The proposed scheme can be applied to biometric authentication in the post-quantum environment. The extension to an efficient fuzzy attribute-based fully homomorphic signature scheme in the standard model will be considered in our future work.

REFERENCES

[1] Shamir A, "Identity-based cryptosystems and signature schemes". in *Proc. of Advances in Cryptology. CRYPTO 1984*, Santa Barbara, CA, USA: Springer, vol 196, pp. 47–53, 1984. doi: 10.1007/3-540-39568-7_5.

[2] Sahai A, Waters B, "Fuzzy identity-based encryption". in *Proc. of Advances in cryptology-In Eurocrypt 2005*, Aarhus, Denmark: Springer, vol. 3494, 2005. pp. 457–473. doi: 10.1007/11426639_27.

[3] J. Baek, S. Willy, J. Zhou, "New constructions of fuzzy identity-based encryption". in *Proc. of the 2nd ACM symposium on Information, computer and communications security-ASIACCS'07* pp. 368–370. doi: 10.1145/1229285.1229330.

[4] A. Lewko, B. Waters, "Unbounded HIBE and attribute-based encryption". in *Proc. Advances in Cryptology-EUROCRYPT 2011*, Tallinn, Estoniapp: Springer, vol 6632, 2011. pp. 547–567. doi: 10.1007/978-3-642-20465-4_30.

[5] V. Goya, O. Pande, A. Sahai, "Attribute-based encryption for fine-grained access control of encrypted data". in *Proc. of the 13th ACM Conference on Computer and Communication Security 2006*, New York, USA: ACM, pp.89–98. doi: 10.1145/1180405.1180418.

[6] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, H. Wee, "Functional encryption for threshold functions (or Fuzzy IBE) from lattices". in *Proc. Public Key Cryptography-PKC 2012*, Darmstadt, Germany: Springer, vol 7293, 2012. pp. 280–297. doi: 10.1007/978-3-642-30057-8_17.

[7] P. Yang, Z. Cao, X. Dong, "Fuzzy identity based signature". Cryptology ePrint Archive, Report 2008/002, 2008. [Online]. Available: https://eprint.iacr.org/2008/002.

[8] C. Wang, J. Kim, "Two constructions of fuzzy identity based signature". in *Proc. of International conference on biomedical engineering and informatics*, 2009. pp. 1–5. doi: 10.1109/BMEI.2009.5305820.

[9] C. Wan, W. Che, Y. Liu, "A fuzzy identity based signature scheme". in *Proc. of International conference on E-business and information system security*, 2009. pp. 1–5. doi: 10.1109/EBISS.2009.5137871.

[10] C. Wang, "A provable secure fuzzy identity based signature scheme". in *Science China Information Sciences*, 2012. vol. 55, no. 9, pp. 2139–2148. doi: 10.1007/s11432-011-4454-x.

[11] L. Zhang, Q. Wu, Y. Hu, "Fuzzy Biometric Identity-Based Signature in the Standard Model". in *Applied Mechanics and Materials*, 2011. vol. 26, no. 5, pp. 3350–3354. doi: 10.4028/www.scientific.net/AMM.44-47.3350.

[12] C.Wang, H.Huang, Y. Yuan, "A Provably Secure Scalable Revocable Identity-Based Signature Scheme Without Bilinear Pairings". in *Proc. of the Second International Conference on Security with Intelligent Computing and Big Data Services*,2018. Springer. vol 895, pp. 588–597. doi: 10.1007/978-3-030-16946-6_47.

[13] F. Li, Y. Liao, Z. Qin, "Further improvement of an identity-based signcryption scheme in the standard model". in *Computers and Electrical Engineering*, 2012. vol. 38, no. 2, pp. 413–421. doi: 10.1016/j.compeleceng.2011.11.001.

[14] K. Takahashi, T. Matsuda, "Signature schemes with a fuzzy private key". in *International Journal of Information Security*, 2019. vol. 18, pp. 581–617. doi: 10.1007/s10207-019-00428-z.

[15] X. Li, J.W. Niu, J. Ma, ei al., "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart card". in *Journal of Network and Computer Applications*, 2011. vol. 34, no. 1, pp. 73–79. doi: 10.1016/j.jnca.2010.09.003.

[16] X. Li, J. Ma, W.D. Wang, ei al., "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environment". in *Mathematical and Computer Modelling*, 2013. vol. 58, no. 1, pp. 85–95. doi: 10.1016/j.mcm.2012.06.033.

[17] X. Li, J.W Niu, M.K. Khan, ei al., "An enhanced smart card based remote user password authentication scheme". in *Journal of Network and Computer Applications*, 2013. vol. 36, no. 5, pp. 1365–1371. doi: 10.1016/j.jnca.2013.02.034.

[18] X. Li, Y.P. Xiong, J. Ma, ei al., "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards". in *Journal of Network and Computer Applications*, 2012. vol. 35, no. 2, pp. 763–769. doi: 10.1016/j.jnca.2011.11.009.

[19] P. Yang, Z. Cao, X. Dong, "Fuzzy identity based signature with applications to biometric authentication". in *Computers and Electrical Engineering*, 2019. vol. 37, no. 4, pp. 532–540. doi: 10.1016/j.compeleceng.2011.04.013.

[20] P. Shor, "Polynomial-time algorithm for prime factorizeation and discrete logarithm on a quantum computer", *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1999. doi: 10.1137/S0097539795293172.

[21] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)". in *Proc. of STOC*, 1996. Springer. pp. 99–108. doi: 10.1145/237814.237838.

[22] Alwen, Joel, and C. Peikert, "Generating Shorter Bases for Hard Random Lattice". in *Proc. of International Symposium on Theoretical Aspects of Computer Science*, 2011. Springer. pp. 535–553. doi: 10.1007/s00224-010-9278-3.

[23] C. Gentry, C. Peikert, V. Vaikuntanathan, "How to use a short basis: trapdoors for hard lattices and new cryptographic constructions". in *Proc. of STOC*, 2008. Springer. pp. 197–206. doi: 10.1145/1374376.1374407.

[24] D. Micciancio, C. Peikert, "Trapdoors for lattices: simpler, tighter, faster, smaller", in *Proc. of EUROCRYPT 2012*, Cambridge, UK: Springer, 2012, pp. 700–718. doi: 10.1007/978-3-642-29011-4_41.

[25] D. Micciancio, O. Regev, " Worst-case to average-case reductions based on Gaussian measures". in *SIAM Journal on Computing*, 2007. vol. 37, no. 1, pp. 267–302. doi: 10.1137/S0097539705447360.

[26] Y. Yao, Z. Li, "A novel fuzzy identity based signature scheme based on the short integer solution problem". in *Computers and Electronical Engineering*, 2019. vol. 40, no. 6, pp. 1930–1939. doi: 10.1016/j.compeleceng.2013.09.005.

[27] X. Zhang, C. Xu, Y. Zhang, "Fuzzy identity-based signature scheme from lattice and its application in biometric authentication". in *KSII Transactions on Internet and Information Systems*, 2017. vol. 11, no. 5, pp. 2762–2777. doi: 10.3837/tiis.2017.05.025.

[28] Y.H. Zhang, Y. Gan, Y.F. Yin et al., "Efficient fuzzy identity-based signature from lattices for identities in a small (or large) universe". in *Journal of Information Security and Applications*, 2019. vol. 47, pp. 86–93. doi: 10.1007/978-981-13-3095-7_7.

[29] R. Johnson, D. Molnar, X. Song, and D. Wagner, "Homomorphic signature schemes". in *Proc. of CT-RSA 2002*, 2002. Springer. vol 2271, pp. 244–262. doi: 10.1007/3-540-45760-7_17.

[30] D. Catalano, D. Fiore, and B. Warinschi, "Efficient network coding signatures in the standard model". in *Proc. of PKC 2012*, 2012. Springer. vol 7293, pp. 680–696. doi: 10.1007/978-3-642-30057-8_40.

[31] D. Catalano, D. Fiore, and B. Warinschi, "Homomorphic signatures with efficient verification for polynomial functions". in *Proc. of CRYPTO 2014*, 2014. Springer. vol 8616, pp. 371–389. doi: 10.1007/978-3-662-44371-2_21.

[32] S. Gorbunov and V. Vaikuntanathan, "(leveled) fully homomorphic signatures from lattices". Cryptology ePrint Archive, Report 2014/463, 2014. [Online]. Available: http://eprint.iacr.org/2014/463.

[33] D. Wichs, "Leveled fully homomorphic signatures from standard lattices". Cryptology ePrint Archive, Report Report 2014/451, 2014. [Online]. Available: http://eprint.iacr.org/2014/451.

[34] D. Boneh and D. M. Freeman, "Homomorphic signatures for polynomial functions". in *Proc. of EUROCRYPT 2011*, 2011. Springer. vol 6632, pp. 149–168. doi: 10.1007/978-3-642-20465-4_10.

[35] J.H. Ahn, D. Boneh, J. Camenisch, et al, "Computing on authenticated data". in *Proc. of TCC 2012*, 2012. Springer. vol 7194, pp. 1–20. doi: 10.1007/978-3-642-28914-9_1.

[36] D. Boneh, C. Gentry, S. Gorbunov, "Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits," in *Proc. of EUROCRYPT 2014*, 2014. Springer. vol 8441, pp. 533–556. doi: 10.1007/978-3-642-55220-5_30.

[37] X. Boyen, X. Fan and E. Shi, "Adaptively secure fully homomorphic signatures based on lattices", Cryptology ePrint Archive, Report 2014/916, 2014. [Online]. Available: http://eprint.iacr.org/2014/916.

[38] X. Zhang, Z. Liu, "Lattice-based strongly-unforgeable forward-secure identity-based signature scheme with flexible key update", *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS*, vol. 11, no. 5, pp. 2792–2810, 2017. doi: 10.3837/tiis.2017.05.027 .

[39] S. Katsuamta, S. Yamada, "Partitioning via non-Linear polynomial functions: more compact IBEs from ideal lattices and bilinear maps", in *Proc. of ASIACRYPT 2016*, Hanoi, Vietnam: Springer, 2016, pp. 682–712. doi: 10.1007/978-3-662-53890-6_23.

[40] S.H. Islam, A. Das, 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, 2019. doi: 10.1002/sec.1528.

[41] D. Stehlé, R. Steinfeld, K. Tanaka, K. Xagawa, "Efficient public key encryption based on ideal lattices," in *Proc. of ASIACRYPT 2009*, Tokyo, Japan: Springer, 2009, pp. 617–635. doi: 10.1007/978-3-642-10366-7_36.

[42] D. Cash, D. Hofheinz, E. Kiltz, C. Peikert, ”Bonsai trees, or how to delegate a lattice basis”, *Journal of Cryptology*, vol. 25, no. 4, pp. 601–639, 2012. doi: 10.1007/s00145-011-9105-2.

[43] C. Gentry, C. Peikert, V. Vaikuntanathan, ”Trapdoors for hard lattices and new cryptographic constructions”, in *Proc. of 40th Annual ACM Symposium on Theory of Computing 2008*, New York, NY, USA: ACM, 2008, pp. 197–206, 2008. doi: 10.1145/1374376.1374407.

[44] S. Agrawal, D. Boneh, X. Boyen, ”Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE”, in *Proc. of Advances in cryptology-CRYPTO 2010*, Springer, vol. 6223, pp. 98–115, 2010. doi: 10.1007/978-3-642-14623-7_6.

[45] A. Langlois, D. Stehle, ”Worst case to average case reductions for module lattices”, *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015. doi: 10.1007/s10623-014-9938-4.

[46] C. Wang, B. Wu and H. Yao, ”Leveled Adaptively Strong-Unforgeable Identity-Based Fully Homomorphic Signatures”, *IEEE Access*, vol. 8, pp. 119431–119447, 2020. doi: 10.1109/ACCESS.2020.3003685.

[47] M. Ramadan, Y. Liao, F. Li and S. Zhou, ”Identity-Based Signature With Server-Aided Verification Scheme for 5G Mobile Systems”, *IEEE Access*, vol. 8, pp. 51810-51820, 2020. doi: 10.1109/ACCESS.2020.2980213.