Fuzzy identity-based signature scheme from lattice and its application in biometric authentication

Xiaojun Zhang[1,2*], Chunxiang Xu[2], Yuan Zhang[2]
[1]School of Computer Science, Southwest Petroleum University, Xindu Avenue, No.8, Xindu Zone, Chengdu 610500, China
[e-mail: zhangxjdzkd2012@163.com]
[2]School of Computer Science and Engineering, University of Electronic Science and Technology of China, 2006 Xi Yuan Avenue, West High-tech Zone, Chengdu 611731, China
*Corresponding author: Xiaojun Zhang

Received September 16, 2016; revised November 26, 2016; accepted March 16, 2017; published May 31, 2017

Abstract

A fuzzy identity based signature (FIBS) scheme allows a signer with identity ω to generate a signature which could be verified under identity ω' if and only if ω and ω' are within a certain distance of each other as judged by some metric. In this paper, we propose an efficient FIBS scheme from lattice assumption, which can resist quantum-computer attacks. Without using the Bonsai Tree technique, we utilize the lattice basis delegation technique to generate the private key, which has the advantage of keeping the lattice dimension invariant. We also prove that our proposed scheme is existentially unforgeable under an adaptive chosen message and identity attack in the random oracle model. Compared with existing scheme, our proposed scheme is much more efficient, especially in terms of communication overhead. Since our FIBS scheme possesses similar error-tolerance property, it can be well applied in post-quantum communication biometric authentication environments, where biometric identifiers such as fingerprints, voice, iris and gait are used in human identification.

Keywords: Fuzzy identity based signature, lattice assumption, existentially unforgeable, post-quantum communication, biometric authentication

1. Introduction

Shamir [1] first introduced the concept of identity based cryptography, in which the public key of an entity can be easily computed from his arbitrary string, e.g. telephone number, an e-mail address, IP address, and so on. While the corresponding private key can be generated by the trusted Private Key Generator (PKG). Thus identity-based cryptography provides a more convenient alternative to the traditional Public Key Infrastructure (PKI).

To tolerate small errors of the identity, in 2005, Sahai and Waters [2] first introduced fuzzy identity based encryption (FIBE), in which identities are regarded as a set of descriptive attributes instead of a string of characters in previous IBE system. They also showed that FIBE can be used for a kind of application considered as attribute based encryption [3, 4]. In an FIBE scheme, a user with the private key for identity ω is able to decrypt a ciphertext with identity ω' if and only if ω and ω' are within a certain distance of each other as judged by some metric. Thus, an FIBE scheme allows for a certain amount of error tolerance in the identities.

A novel cryptographic primitive that is the signature analog of an FIBE scheme, we call it fuzzy identity based signature (FIBS). An FIBS scheme allows a signer with the identity ω to issue a signature which could be verified under the identity ω' if and only if ω and ω' are within a certain distance of each other as judged by some metric. An important feature of FIBS is that a private key associated with an identity rather than a master secret key of the PKG is shared among signature generation servers, which is more desirable in practice. FIBS scheme can be directly applied to IBS system which uses biometric identities. Consider the following situation: for a verifier, how to confirm the signer is the very one who has signed the contract if he had never known the signer? The signer should come to see the verifier with the contract he signed, and the verifier would use a biometric reading and ask the signer to provide his biometric information on the spot, the verifier can then construct the signer's public key from the collected biometric information and verify the signature of contract successfully.

Yang et al. [5] first proposed the FIBS scheme based on Sahai and Waters's FIBE scheme [2]. Subsequently, some FIBS schemes [6, 7, 8, 9] were proposed based on the traditional cryptographic hardness assumptions. However, according to the proof in Shor [10], these traditional hardness assumptions can be solved by a quantum computer in polynomial time. Consequently, it is urgent to engage in researching cryptographic algorithms which can resist quantum computer attacks, namely post-quantum cryptography. During the post-quantum cryptography, the lattice-based cryptography has been regarded as the most important option for resisting quantum computer attacks due to its attractive advantages. Firstly, lattice-based cryptographic systems are based on worst-case hardness assumption while other known cryptographic constructions are based on average-case hardness assumption. It means that breaking the lattice-based cryptographic algorithm implies an efficient algorithm for solving any instance of some underlying lattice problem [11]. Secondly, the main operations in lattice-based cryptography are additions and multiplications over a moderate modulus, thus it is suitable for low power devices. Recently, Agrawal et al. [12] constructed an FIBE scheme from the hardness of the learning with errors (LWE). Inspired by this, Yao [13] constructed a fuzzy identity based signature based on the small integer solution (SIS) assumption. Particularly, with the Bonsai Tree technique in [14], the private key of each identity bit is enerated by the fuzzy extract algorithm. As a result, the dimension of private key and signature is expanded twice as much, thus the size of private key of each identity bit and the length of fuzzy identity-based signature are also expanded twice as much.

1.1 Our contributions

As far as we are concerned, before our proposed scheme, there is only one FIBS scheme from lattice assumption [13]. Considering the needs to have more efficient fuzzy identity-based signature which can be applied even in the presence of quantum-computer, in this paper, we propose a new efficient fuzzy identity-based signature from lattice assumption. Without using the Bonsai Tree technique, we utilize the lattice basis delegation technique to generate the private key, which has the advantage of keeping the lattice dimension invariant. Meanwhile, we employ additive homomorphic hash function [15] to realize our homomorphic linearly lattice-based signature. We utilize the lattice basis delegation technique to construct fuzzy extract algorithms for each identity bit, the original related short basis of which is different from each other, while all the identities have a common short basis as the master secret key. Due to this property, we can further use Shamir secret-sharing technique to construct fuzzy identity-based signature. Moreover, we also prove that our scheme is existentially unforgeable under an adaptive chosen message attack and identity attack (EU-ACMIA) in the random oracle. Compared with existing lattice-based FIBS scheme, our proposed scheme is much more efficient, especially in terms of the communication overhead.

2. Preliminaries

2.1 Background on lattices

Notation. Throughout this paper we say that a function ϵ is negligible if it is smaller than all polynomial fractions for sufficiently large n. We say that an event happens with overwhelming probability if it happens with probability at least $1-\epsilon(n)$ for some negligible function ϵ. We say that integer vectors $v_1,\cdots,v_n \in Z_q^n$ are Z_q-linearly independent if they are linearly independent reduced modulo q. Let B be a set of vectors as $B=[b_1,\cdots,b_m]\subseteq R^{m\times m}$, $\| B\| = max_i \| b_i\|$ $(1\le i\le m)$ denotes the L_2 length of the longest vector in B. While $\tilde{B}=[\widetilde{b_1},\cdots,\widetilde{b_m}]\subseteq R^{m\times m}$ denotes the Gram-Schmidt orthogonalization of the vectors $b_1,\cdots,b_m$ taken in that order. We refer to $\tilde{B}$ as the Gram-Schmidt norm of B. We denote $f(n)=\tilde{O}(g(n))$ if $f(n)=O(g(n)\log^c n)$ for some fixed constant.

In this section, we describe the basic definitions and properties of lattices that will be used later. Throughout the paper, we let the parameters $q=q(\lambda)$, $m=m(\lambda)$, $n=n(\lambda)$ are polynomial functions of the security parameter λ.

Definition 1. Let $B=[b_1,\cdots,b_m]\subseteq R^{m\times m}$ be an $m\times m$ matrix whose columns are linearly independent vectors $b_1,\cdots,b_m\in R^m$. The m-dimensional full-rank lattice Λ generated by B is the set: $\Lambda=\mathcal{L}(B)=\{y\in R^m : \exists s=(s_1,\cdots,s_m)\in Z^m, y=Bs=\sum_{i=1}^{i=m} s_i b_i\}$.

Here, we introduce the integer lattices in [16].

Definition 2. For q prime, $A\in Z_q^{n\times m}$ and $u\in Z_q^n$, define:

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

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

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

Observe that if $t \in \Lambda_q^u(A)$ then $\Lambda_q^u(A) = \Lambda_q^\perp(A) + t$ and hence $\Lambda_q^u(A)$ is a shift of $\Lambda_q^\perp(A)$.

Lemma 1. Let $q \geq 3$ be odd and $m \geq 5n\log q$. There exists a probabilistic polynomial time algorithm **TrapGen** in [17] that outputs a pair $(A \in Z_q^{n\times m},\ T_A \in Z_q^{m\times m})$ such that A is statistically close to a uniform rank n matrix in $Z_q^{n\times m}$ and T_A is a basis for $\Lambda_q^\perp(A)$ with length $\|\widetilde{T_A}\| \leq O(n\log q)$ and $\|T_A\| \leq O(n\log q)$ with all but negligible probability in n.

Discrete Gaussian on lattices. Here we briefly review the discrete Gaussian distribution which is a useful tool in lattice-based cryptography. The discrete Gaussian function on R^m centered at vector c with parameter $\delta > 0$ is defined as $\varphi_{\delta,c}(x) = exp(-\pi\| x-c\|^2) / \delta^2$ and $\varphi_{\delta,c}(\Lambda) = \sum_{x\in\Lambda} \varphi_{\delta,c}(x)$. The discrete Gaussian distribution over Λ with center c and parameter δ is $\forall y \in \Lambda$, $\mathcal{D}_{\Lambda,\delta,c}(y) = \varphi_{\delta,c}(y) / \varphi_{\delta,c}(\Lambda)$.

Hardness of ISIS assumption. The security of our fuzzy identity-based signature scheme is based on the hardness assumption of the inhomogeneous small integer solution (ISIS) [18]. The ISIS assumption is given an integer q, a matrix $A \in Z_q^{n\times m}$, a syndrome $y \in Z_q^n$ and a real number ζ, find a nonzero integer vector $e \in Z^m$ such that $0 < \| e\| \leq \zeta$, $Ae = y\ mod\ q$.

As described in [18], for any poly-bounded $m, \zeta = poly(n)$ and for any prime $q > \zeta O(\sqrt{n\log n})$, the average-case $ISIS_{q,m,\zeta}$ assumption is as hard as approximating the $SIVP$ assumption in the worst case to within certain factors $\gamma(n) = \zeta\tilde{O}(\sqrt{n})$.

Now we introduce a collection of one-way preimage sampleble functions [18], including **TrapGen**, **SampleD**, **SampleDom**, **SamplePre**. Set the Gaussian smoothing parameter $\delta_1 \geq \|\tilde{T}\| O(\sqrt{\log m})$. The function f_A is defined as $f_A(e) = Ae\ \ mod\ \ q$, with domain $D_n = \{e \in Z^m : 0 < \|e\| \leq \delta_1\sqrt{m}\}$ and range $R_n = Z_q^n$.

TrapGen $(1^n, 1^m, q)$: The probabilistic polynomial time (PPT) algorithm **TrapGen** $(1^n, 1^m, q)$ has been described in Lemma 1.

SampleD (T, δ_1, c): On input a basis T of a lattice Λ, the PPT algorithm **SampleD** samples from a discrete Gaussian distribution over the lattice Λ around the center $c \in R^m$ with the standard deviation δ_1.

SampleDom (A, δ_1): Sample an x from D_n for which the distribution of $f_A(x)$ is uniform over R_n.

SamplePre (A, T, y, δ_1): The PPT algorithm executes as follows: First, via linear algebra choose an arbitrary $z \in Z^m$ such that $Az = y\ \ mod\ q$. Then sample v from the discrete Gaussian distribution $\mathcal{D}_{\Lambda_q^\perp(A),\delta_1,-z}$ using SampleD$(T, \delta_1, -z)$ and output $e \in D_n$ such that $e = z + v$.

Now, we describe Agrawal et al. [19] lattice basis delegation technique, we first describe

the distribution $\mathcal{D}_{m\times m}$ as follows:

$\mathcal{D}_{m\times m}$ denotes the distribution on matrics in $Z_q^{m\times m}$ which is defined as $(\mathcal{D}_{Z^m,\sigma_R})^m$ conditioned on the resulting matrix being Z_q -invertible. Here the parameter $\sigma_R=\sqrt{n\log q}O(\sqrt{\log m})$, and Z_q -invertible means that the matrix $R \ mod \ q$ is invertible as a matrix in $Z_q^{m\times m}$.

Lemma 2. Let $q>2, A\in Z_q^{n\times m}$ and $R\in Z^{m\times m}$. Suppose R is sampled from $\mathcal{D}_{m\times m}$. Let T_A be a basis of $\Lambda_q^{\perp}(A)$, there exists a PPT algorithm **NewBasisDel**(A,R,T_A,δ_2) that outputs a random basis T_B for $\Lambda_q^{\perp}(AR^{-1})$ such that $\left\|\widetilde{T_B}\right\|\le O(\sqrt{\log m})$, where $\delta_2\ge\left\|\widetilde{T_A}\right\|\sigma_R\sqrt{m}O(\log^{1/2}m)O(\log m)$.

Now we describe the algorithm **SampleRwithBasis(A)** which generates a matrix R sampled from $\mathcal{D}_{m\times m}$ along with a short basis of $\Lambda_q^{\perp}(AR^{-1})$ without any short basis of $\Lambda_q^{\perp}(A)$. The algorithm proceeds as follows:

(1) It runs the algorithm **TrapGen**($1^n,1^m,q$) to generate a random rank n matrix $B\in Z_q^{n\times m}$ and a basis T_B of $\Lambda_q^{\perp}(B)$.

(2) It samples $r_i\in Z^m$ using the algorithm **SamplePre**(B,T_B,a_i,σ_R) for $i\in\{1,\cdots,m\}$. Note that $Br_i=a_i \ mod \ q$, and r_i is sampled from a distribution statistically close to $\mathcal{D}_{\Lambda_q^{a_i}(B),\sigma_R}$. The algorithm **SamplePre** repeats until r_i is Z_q -linearly independent of $r_1,\cdots,r_{i-1}$.

(3) It outputs $R\in Z^{m\times m}=\{r_1,\cdots,r_m\}$ and the basis T_B of $\Lambda_q^{\perp}(B)$.

By construction, $BR=A \ mod \ q$ and thus $B=AR^{-1} \ mod \ q$. Therefore, the basis T_B is a short basis of $\Lambda_q^{\perp}(AR^{-1})$.

3. Fuzzy identity-based signature and the security model

The FIBS scheme consists of the following four algorithms.

FIBS.Setup($\mathbf{1}^{\kappa}$,**params**): The PPT algorithm takes as input a security parameter 1^k and public parameters **params** that contain an error tolerance parameter t, and outputs the master secret key mk and public key PP.

FIBS.Extract($\mathbf{PP},\mathbf{mk},\omega$): The PPT algorithm takes as input PP, the master secret key mk and an identity $\omega=\{\omega_i\}_{i=1}^{\ell}$, and outputs a private key associated with ω, denoted by sk_{ω}.

FIBS.Sign($\mathbf{PP},\mathbf{sk}_{\omega},\mathbf{M}$): The PPT algorithm takes as input PP, a private key sk_{ω} associated with an identity ω and a message M, and outputs the signature $\theta_{\omega,M}$.

FIBS.Verify($\mathbf{PP},\eta,\mathbf{M},\theta_{\omega,\mathbf{M}}$): This deterministic polynomial time algorithm takes as input PP, an identity $\eta=\{\eta_i\}_{i=1}^{\ell}$, such that $|\eta\cap\omega|\ge t$ (where $|\eta\cap\omega|\ge t$ means the

cardinality of the overlapped set $|\eta \cap \omega|$), the message M and the corresponding signature $\theta_{\omega,M}$, and returns a bit τ, where $\tau = 1$ means that the signature is valid.

These algorithms must satisfy the standard consistency requirement. That is the FIBS scheme demands that for any fixed $\omega = \{\omega_i\}_{i=1}^{\ell}$, and $\eta = \{\eta_i\}_{i=1}^{\ell}$ such that $|\eta \cap \omega| \geq t$, it holds that $Pr(FIBS.Verify(PP, \eta, M, FIBS.Sign(PP, sk_{\omega}, M))) = 1 - negl(\kappa)$.

3.1 Security model

Definition 3(EU-ACMIA). Let $\mathcal{E}$ be a fuzzy identity based signature (FIBS) scheme. Let $\mathcal{F}$ be a probabilistic polynomial-time adversary, and $\mathcal{C}$ be a challenger. The definition of existentially unforgeable against adaptively chosen message and identity attacks (EU-ACMIA) is described in the following game in which $\mathcal{F}$ interacts with the challenger $\mathcal{C}$.

FIBS.Setup : The challenger $\mathcal{C}$ runs the Setup algorithm and provides the adversary $\mathcal{F}$ the public parameters.

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

Phase 2: $\mathcal{F}$ adaptively issues private key queries and signature queries for any identity $\omega = \{\omega_i\}_{i=1}^{\ell}$ such that $|\omega \cap \omega^*| < t$.

Phase 3: The adversary $\mathcal{F}$ makes a number of different queries to the challenger $\mathcal{C}$. Each query can be described as follows:

Extract query: $\mathcal{F}$ issues private key query for any identity $\omega = \{\omega_i\}_{i=1}^{\ell}$ such that $|\omega \cap \omega^*| < t$, the challenger $\mathcal{C}$ then runs the **FIBS.Extract** algorithm to obtain the private key sk_{ω} and sends it to $\mathcal{F}$.

Sign query: The adversary $\mathcal{F}$ can query for any identity $\eta^{(j)} = \{\eta_i^{(j)}\}_{i=1}^{\ell}$ such that $|\eta^{(j)} \cap \omega^*| < t$ on any message M. To answer the Sign query, the challenger $\mathcal{C}$ runs the algorithm **FIBS.Extract** to obtain the private key $sk_{\eta^{(j)}}$, then runs the algorithm $\mathbf{FIBS.Sign(PP, sk}_{\eta^{(j)}}\mathbf{, M)}$ to obtain the signature $\theta_{\eta^{(j)},M}$, and sends it to $\mathcal{F}$.

Output: Finally the adversary $\mathcal{F}$ outputs $(\omega^*, M^*, \theta^*_{\omega^*,M^*})$. $\mathcal{F}$ succeeds if it satisfies $\mathbf{FIBS.Verify}(PP, \omega^*, M^*, \theta^*_{\omega^*,M^*}) = 1$ and the set in $\omega^* \cap \eta^{(j)}$ (where $|\omega^* \cap \eta^{(j)}| \geq t$) were not submitted to the private key Extract query and the Sign query, respectively.

We define $\mathcal{F}'s$ successful probability as follows:

$$FIBS - Adv_{EU-ACMIA}[\mathcal{F}, \mathcal{E}] = Pr[FIBS.Verify(PP, \omega^*, M^*, \theta^*_{\omega^*,M^*}) = 1].$$

The fuzzy identity-based scheme $\mathcal{E}$ is existentially unforgeable against adaptively chosen message and identity attacks, if $FIBS - Adv_{EU-ACMIA}[\mathcal{F}, \mathcal{E}]$ is negligible in the security parameter κ.

4. Fuzzy identity-based signature scheme from lattice assumption

In this section, we begin to describe our fuzzy identity-based scheme from lattice assumption. Our construction is motivated by lattice-based linearly homomorphic signature scheme [20, 21]

and the FIBS scheme in [13]. Moreover, we employ the lattice basis delegation technique in [19] to extract the private key for each identity bit, and we make use of the GPV signature scheme [18] and Shamir secret share technique to realize the construction of fuzzy identity-based signature scheme. Additionally, to make sure the two algorithms **SamplePre** and **NewBasisDel** run correctly, we need to set two secure Gaussian parameters δ_1, δ_2, which have been described as before. Our FIBS scheme consists of the following four algorithms:

FIBS.Setup$(\mathbf{1^n}, \mathbf{params})$: On input a secure parameter n and $\mathbf{params} = (q, m, t, \ell, \tilde{L}, D_n)$, where $q = poly(n)$, $m \geq 5n\log q$, ℓ is the length of every identity string, $t < \ell$ is the error tolerance parameter, $\tilde{L} = O(n\log q)$, $D_n = \{e \in Z^m : 0 < \|e\| \leq \delta_1\sqrt{m}\}$. The PKG performs as follows:

(1) Run the algorithm $TrapGen(1^n, 1^m, q)$ to generate 2ℓ uniform random matrices $P_{j,\tau} \in Z_q^{n\times m}$ for all $j \in \{1, 2, \cdots, \ell\}$ and $\tau \in \{0,1\}$ together with a full-rank set of vectors $S_{j,\tau} \subseteq \Lambda_q^{\perp}(P_{j,\tau})$ such that $\|\widetilde{S_{j,\tau}}\| \leq \tilde{L}$.

(2) Let $H_1 : \{0,1\}^* \to Z^{m\times m}$ be a secure hash function, and the output value of H_1 is distributed as $\mathcal{D}_{m\times m}$. Let $H_2 : Z_q^m \times \{0,1\}^* \to Z_q^m$ also be a secure collision-resistant hash function.

(3) Output the public parameters $PP = (\{P_{j,\tau}\}_{j\in[\ell],\tau\in\{0,1\}}, H_1, H_2)$ and the master secret key $mk = \{S_{j,\tau}\}_{j\in[\ell],\tau\in\{0,1\}}$.

FIBS.Extract$(\mathbf{PP}, \mathbf{mk}, \omega)$: The PKG takes the public parameters PP, an identity $\omega = \{\omega_1, \cdots, \omega_\ell\} \in \{0,1\}^\ell$, and the master secret key mk as input, and generates the private key for $\omega = \{\omega_1, \cdots, \omega_\ell\} \in \{0,1\}^\ell$ as follows:

(1) Evaluate $S'_{j,\omega_j} \leftarrow NewBasisDel(P_{j,\omega_j}, H_1(\omega_j \| \omega \| j), S_{j,\omega_j}, \delta_2)$ for all $j \in \{1, 2, \cdots, \ell\}$.

(2) Output the private key $S_\omega = \{\omega, (S'_{1,\omega_1}, \cdots, S'_{\ell,\omega_\ell})\}$ for $\omega = \{\omega_1, \cdots, \omega_\ell\}$.

FIBS.Sign$(\mathbf{PP}, \mathbf{S}_\omega, \mathbf{v}, \omega)$: On input PP, an identity $\omega = \{\omega_1, \cdots, \omega_\ell\} \in \{0,1\}^\ell$, and a message $\mathbf{v} = (v_1, v_2, \cdots, v_m) \in Z_q^m$. The signer generates the fuzzy identity-based signature as follows:

(1) Construct ℓ shares of $\mathbf{v} = (v_1, v_2, \cdots, v_m)$ with a Shamir secret-sharing technique applied to each coordinate of $\mathbf{v}$ independently. That is, for each $l \in \{1, 2, \cdots, m\}$, choose a uniform random polynomial $p_l \in Z_q[x]$ of degree $t-1$ such that $p_l(0) = v_l$. Construct the k-th share vector $\overline{\mathbf{v_k}} = (p_1(k), p_2(k), \cdots, p_m(k)) \in Z_q^m$. Thus for all $\mathcal{I} \subseteq \{1, 2, \cdots, \ell\}$ such that $|\mathcal{I}| \geq t$, we can compute fractional lagrangian coefficients ξ_k satisfying $\mathbf{v} = \sum_{k\in\mathcal{I}} \xi_k \overline{\mathbf{v_k}} \pmod q$. That is, we interpret ξ_k as a fraction of integers, which we can also evaluate $(\bmod q)$.

(2) Compute n vectors $\rho_i = H_2(\mathbf{v} \| i) \in Z_q^m$ for $i \in \{1, 2, \cdots, n\}$.

(3) Compute the inner products $f_{j,i} = \langle \overline{v_j}, \rho_i \rangle$, where $1 \le j \le \ell$ and $1 \le i \le n$, and parse $f_j = (f_{j1}, \cdots, f_{jn})^\top$.

(4) Evaluate $\theta_j \leftarrow SamplePre(P_{j,\omega_j}(H_1(\omega_j \| \omega \| j))^{-1}, S'_{j,\omega_j}, f_j, \delta_1)$ for $j \in \{1, 2, \cdots, \ell\}$.

(5) Output the signature $\theta_{\omega,\mathbf{v}} = \{\mathbf{v}, (\theta_1, \theta_2, \cdots, \theta_\ell), \omega)\}$.

FIBS.Verify$(\mathbf{PP}, \eta, \theta_{\omega,\mathbf{v}})$: To verify the signature $\theta_{\omega,\mathbf{v}} = \{\mathbf{v}, (\theta_1, \theta_2, \cdots, \theta_\ell), \omega\}$ with respect to the identity $\omega = \{\omega_1, \cdots, \omega_\ell\}$ against an identity $\eta = \{\eta_1, \cdots, \eta_\ell\}$. Let $\mathcal{I} \subseteq [\ell]$ denote the set of matching bits in ω and η, that is $\mathcal{I} = \omega \cap \eta$. If $|\mathcal{I}| = |\omega \cap \eta| < t$, the receiver outputs *false*. Otherwise, the receiver computes n vectors $\rho_i = H_2(\mathbf{v} \| i) \in Z_q^m$ for each $i \in \{1, 2, \cdots, n\}$ and $f = (\langle \mathbf{v}, \rho_1 \rangle, \langle \mathbf{v}, \rho_2 \rangle, \cdots, \langle \mathbf{v}, \rho_n \rangle)^\top$. The receiver accepts the fuzzy identity-based signature if and only if both the following conditions are satisfied:

(1) $\theta_j \in D_n$ such that $0 < \|\theta_j\| \le \delta_1 \sqrt{m}$ for all $j \in \{1, 2, \cdots, \ell\}$.

(2) $\sum_{j \in \mathcal{I}} \xi_j P_{j,\omega_j}(H_1(\omega_j \| \omega \| j))^{-1} \theta_j = f$, where $\xi_j = \prod_{i \ne j, i \in \mathcal{I}} \frac{0-i}{j-i}$ is the corresponding fractional lagrangian coefficient.

Otherwise, the receiver rejects.

4.1 Correctness

The correctness of our proposed FIBS scheme is elaborated as follows. Here we just consider the case $|\mathcal{I}| \ge t$. For each $j \in \{1, 2, \cdots, \ell\}$, the vector θ_j output by the algorithm **FIBS.Sign** satisfying $P_{j,\omega_j}(H_1(\omega_j \| \omega \| j))^{-1} \theta_j = f_j$ and is drawn from a distribution statistically close to $\mathcal{D}_{\Lambda_q^{f_j}(P_{j,\omega_j}(H_1(\omega_j \| \omega \| j))^{-1}), \delta_1}$. Thus for all $j \in \{1, 2, \cdots, \ell\}$, each θ_j satisfies $0 < \|\theta_j\| \le \delta_1 \sqrt{m}$ with overwhelming probability. Since:

$$
\begin{aligned}
&\sum_{j \in \mathcal{I}} \xi_j P_{j,\omega_j}(H_1(\omega_j \| \omega \| j))^{-1} \theta_j = \sum_{j \in \mathcal{I}} \xi_j f_j \\
&= \sum_{j \in \mathcal{I}} \xi_j (\langle \rho_1, \overline{\mathbf{v_j}} \rangle, \langle \rho_2, \overline{\mathbf{v_j}} \rangle, \cdots, \langle \rho_n, \overline{\mathbf{v_j}} \rangle)^\top \\
&= \sum_{j \in \mathcal{I}} (\langle \rho_1, \xi_j \overline{\mathbf{v_j}} \rangle, \langle \rho_2, \xi_j \overline{\mathbf{v_j}} \rangle, \cdots, \langle \rho_n, \xi_j \overline{\mathbf{v_j}} \rangle)^\top \\
&= (\langle \rho_1, \sum_{j \in \mathcal{I}} \xi_j \overline{\mathbf{v_j}} \rangle, \langle \rho_2, \sum_{j \in \mathcal{I}} \xi_j \overline{\mathbf{v_j}} \rangle, \cdots, \langle \xi_n, \sum_{j \in \mathcal{I}} \xi_j \overline{\mathbf{v_j}} \rangle)^\top \\
&= (\langle \rho_1, \mathbf{v} \rangle, \langle \rho_2, \mathbf{v} \rangle, \cdots, \langle \rho_n, \mathbf{v} \rangle)^\top \\
&= f
\end{aligned}
$$

Thus, the verification equation $\sum_{j \in \mathcal{I}} \xi_j P_{j,\omega_j}(H_1(\omega_j \| \omega \| j))^{-1} \theta_j = f$ holds.

Therefore, if the fuzzy identity-based signature $\theta_{\omega,\mathbf{v}} = \{\mathbf{v}, (\theta_1, \theta_2, \cdots, \theta_\ell), \omega\}$ is generated

by the signer, and the condition $|\mathcal{I}|=|\omega \cap \eta| \geq t$ holds, the receiver will accept the signature. Otherwise, he rejects.

4.2 Performance comparison

Until now, as far as we are concerned, there is only one fuzzy identity based signature based on lattice [13], whose advantages have been shown in the details of the performance comparison with previous schemes [5, 6, 7, 8]. For simplicity, we give the following notations in **Table 1**.

Table 1. Notation

ℓ	the length of identity(attribute)
t	the error tolerance parameter
l_q, l_{pq}	the bit-length of an element in Z_q, Z_{pq}
PP, mk， UPK, USK	the size of master public key, master secret key, user public key, user secret key
$T_{Rand(Ext)}$	the time of the algorithm $RandBasis(ExtBasis)$
$T_{BasisDel}$	the time of the algorithm $NewBasisDel$
T_{Sampre}	the time of the algorithm $Sample\,\mathrm{Pr}\,e$
I, I'	inner product in Z_q^m, Z_{pq}^{2m}
Mu, Mu'	scalar multiplication in Z_q^n, Z_{pq}^n
LS	the length of fuzzy identity-based signature
CE, CS, CV	the computation cost of FIBS.Extrct, FIBS.Sign, FIBS.Very
ROM, SM	random oracle model, standard model
HP	hardness problem assumption

Now we only focus on giving the details of the performance comparison between our scheme and the scheme in [13] in **Table 2**.The performance comparison includes the communication overhead (PP, mk, UPK, USK, LS), the computation cost (CE, CS, CV), hardness assumption, and the security model. From **Table 2**, we can see that both of the schemes are based on lattice assumptions (SIS,ISIS), which can resist quantum computer attacks. They are both proved in the random model. Fortunately, our scheme has obvious advantages in terms of communication overhead, and the computation cost in our scheme is a little less than [13]. The explanations can be illustrated as follows: Since the scheme in [13] employs the linearly homomorphic signature scheme based on the k_1-SIS problem [20], together with the Bonsai Trees principles based on lattice [14], with the Bonsai Trees technique, the dimension of the public key, private key and signature will expand twice as much, and thus the corresponding size will also expand twice as much, this leads to much more communication overhead. In addition, as the algorithm **NewBasisDel** in [19] mainly contains the algorithm **RandBasis** , thus the computation of the algorithm **NewBasisDel** almost equals to the algorithm **RandBasis**(**ExtBasis**) . While the computation cost needs to reside in Z_{pq}, thus I, Mu are a little less than I', Mu' respectively. This leads to more computation cost in [13].

Table 2. Performance comparison

Scheme	PP	mk	UPK	USK	LS
[13]	$2\ell nml_{pq}$	$2\ell m^2 l_{pq}$	$2\ell nml_{pq}$	$4\ell m^2 l_{pq}$	$2m\ell l_{pq}$
FIBS	$2\ell nml_q$	$2\ell m^2 l_q$	ℓnml_q	$\ell m^2 l_q$	ℓml_q
Scheme	**CE**	**CS**	**CV**	**HP**	**ROM/SM**
[13]	$\ell T_{Rand(Ext)}$	ℓT_{Sampre}	$t(nI' + Mu')$	SIS	ROM
FIBS	$\ell T_{BasisDel}$	ℓT_{Sampre}	$t(nI + Mu)$	ISIS	ROM

5. Security analysis

In this section, we begin to prove that our fuzzy identity-based scheme (FIBS) is existentially unforgeable against adaptively chosen message and identity attacks (EU-ACMIA) in the random oracle model. Here we assume a challenger that takes as input the precondition ISIS assumption, simulates the **hash queries**, **Extract queries** and **Sign queries**, and finally outputs a solution of the ISIS assumption.

Theorem 1. Our proposed fuzzy identity-based signature scheme is EU-ACMIA secure in the random oracle model provided that the $ISIS_{\{n,m\ell,q,\zeta\}}$ (where $\zeta = (\ell!)^3 \delta_1 \sqrt{mt}$) assumption holds.

Proof. Let the adversary $\mathcal{F}$ be a probability polynomial-time adversary which can attack the security of EU-ACMIA in our proposed scheme with a non-negligible probability. We will construct a challenger $\mathcal{C}$, who will also run $\mathcal{F}$ as a subroutine to solve an $ISIS_{\{n,m\ell,q,\zeta\}}$ instance with a non-negligible probability, thus can lead to a contradiction.

FIBS.Setup: First of all, we assume that the challenger $\mathcal{C}$ receives an ISIS instance $(E,F) \in Z_q^{n\times \ell m} \times Z_q^n$, where $F = Df^*$ $(D = (\ell!)^2)$ is a sufficiently large constant), $f^* = (\langle \mathbf{v}^*, \rho_1^* \rangle, \langle \mathbf{v}^*, \rho_2^* \rangle, \cdots, \langle \mathbf{v}^*, \rho_n^* \rangle)^\top$, and for each $i \in \{1,2,\cdots,n\}$, $\rho_i^* = H_2(\mathbf{v}^* \| i) \in Z_q^m$. $\mathcal{C}'s$ goal is to output a nonzero short vector $\theta^* \in Z_q^{\ell m}$ satisfying $E\theta^* = F$, $0 < \| \theta^* \| \le \zeta$. Parse E as $E = E_1 \| E_2 \| \cdots \| E_\ell$, where $E_j \in Z_q^{n\times m}$ for $j = 1,2,\cdots,\ell$. $\mathcal{C}$ samples ℓ random matrices $R_1^*, R_2^*, \cdots, R_\ell^* \leftarrow \mathcal{D}_{m\times m}$.

The adversary $\mathcal{F}$ announces to $\mathcal{C}$ the target identity ω^* which it intends to attack, then $\mathcal{C}$ constructs the public parameters $PP = \{\Omega_1, \Omega_2\}$ as follows:

(1) Set $P_{1,\omega_1^*} = E_1 R_1^*$, $P_{2,\omega_2^*} = E_2 R_2^*$, $\cdots, P_{\ell,\omega_\ell^*} = E_\ell R_\ell^*$, and denote the set by $\Omega_1 = \{P_{j,\omega_j^*}\}_{j\in[\ell]}$.

(2) Set ℓ matrices $P_{j,\overline{\omega_j^*}} \in Z_q^{n\times m}$, $j \in \{1,2,\cdots,\ell\}$, and denote the set by $\Omega_2 = \{P_{j,\overline{\omega_j^*}}\}_{j\in[\ell]}$.

For each query for H_1, H_2, $\mathcal{C}$ maintains lists L_1, L_2, respectively in its local storage. They are set to be empty initially. The adversary $\mathcal{F}$ queries for the values of H_1, H_2, **Extract** and FIBS.Sign algorithm as follows:

H_1 **hash query**: When $\mathcal{F}$ requests the hash value of the identity $\omega = \{\omega_1, \cdots, \omega_\ell\}$, $\mathcal{C}$

performs as follows:

(1) If ω is in the L_1 list, $\mathcal{C}$ returns $(H_1(\omega_1 \| \omega \| 1), H_1(\omega_2 \| \omega \| 2), \cdots, H_1(\omega_\ell \| \omega \| \ell))$ to the adversary $\mathcal{F}$.

(2) If ω is not in the L_1 list, and if $\omega = \omega^*$, $\mathcal{C}$ performs as follows. For each $j \in \{1, 2, \cdots, \ell\}$, $\mathcal{C}$ stores $(\omega, \omega_j, R_j^*, Q_{j,\omega_j}, \perp)$ into L_1 list, where $Q_{j,\omega_j} = Q_{j,\omega_j^*} = P_{j,\omega_j^*}(R_j^*)^{-1} = E_j$. Finally, $\mathcal{C}$ returns $(R_1^*, \cdots, R_\ell^*)$ to the adversary $\mathcal{F}$. Otherwise, with the querying for $\omega \neq \omega^*$, for each $j \in \{1, 2, \cdots, \ell\}$, $P_{j,\omega_j} \in \{P_{j,\overline{\omega_j^*}}\}_{j\in[\ell]}$, $\mathcal{C}$ executes the algorithm **SampleRwithBasis**(P_{j,ω_j}) to obtain random matrix $R_{j,\omega_j} \leftarrow \mathcal{D}_{m\times m}$ and a short basis S'_{j,ω_j} for $\Lambda_q^\perp(Q_{j,\omega_j})$. Finally, $\mathcal{C}$ stores $(\omega, \omega_j, R_{j,\omega_j}, Q_{j,\omega_j}, S'_{j,\omega_j})$ into the L_1 list, and returns $(R_{1,\omega_1}, R_{2,\omega_2}, \cdots, R_{\ell,\omega_\ell})$ to the adversary $\mathcal{F}$.

H_2 **hash query**: For query for the value of H_2 on $(\mathbf{v}, i)$, $\mathcal{C}$ returns h_{2i}, if it exists in L_2 list. Otherwise, $\mathcal{C}$ randomly chooses $h_{2i} \in Z_q^m$, stores $(\mathbf{v}, i, h_{2i})$ into L_2 list, and returns h_{2i} to the adversary $\mathcal{F}$.

Extract query: Considering a query for the private key of an identity ω, although $\mathcal{C}$ does not know the master private key $\{S_{j,\tau}\}_{j\in[\ell],\tau\in\{0,1\}}$, it can construct the private key for ω where $|\omega^* \cap \omega| < t$. Given $\omega = \{\omega_1, \cdots, \omega_\ell\}$, for all $j \in \{1, 2, \cdots, \ell\}$, $(\omega, \omega_j, R_{j,\omega_j}, Q_{j,\omega_j}, S'_{j,\omega_j})$ is in L_1 list, $\mathcal{C}$ directly returns $(S'_{1,\omega_1}, \cdots, S'_{j,\omega_j}, \cdots, S'_{\ell,\omega_\ell})$ to the adversary $\mathcal{F}$. Otherwise, for each $j \in \{1, 2, \cdots, \ell\}$, the challenger $\mathcal{C}$ runs the algorithm **SampleRwithBasis**(P_{j,ω_j}) (where $P_{j,\omega_j} \in \{P_{j,\overline{\omega_j^*}}\}_{j\in[\ell]}$) to obtain random matrix $R_{j,\omega_j} \leftarrow \mathcal{D}_{m\times m}$ and a short basis S'_{j,ω_j} for $\Lambda_q^\perp(Q_{j,\omega_j})$, where $Q_{j,\omega_j} = P_{j,\omega_j}(R_{j,\omega_j})^{-1}$. Then, $\mathcal{C}$ stores $(\omega, \omega_j, R_{j,\omega_j}, Q_{j,\omega_j}, S'_{j,\omega_j})$ into the L_1 list. Finally, $\mathcal{C}$ returns $(S'_{1,\omega_1}, \cdots, S'_{j,\omega_j}, \cdots, S'_{\ell,\omega_\ell})$ to the adversary $\mathcal{F}$.

Sign query: Given an identity $\omega' = \{\omega'_1, \cdots, \omega'_\ell\}$ and a message $\mathbf{v}' \in Z_q^m$, $\mathcal{C}$ simulates the query for the private key of the identity ω', and guarantees that $\{\omega', \omega'_j, R'_{j,\omega'_j}, Q'_{j,\omega'_j}, S'_{j,\omega'_j}\}_{j\in[\ell]}$ which satisfies $|\omega' \cap \omega^*| < t$ is in the L_1 list. The challenger $\mathcal{C}$ generates the fuzzy identity-based signature of $(\omega', \mathbf{v}')$ as follows:

(1) $\mathcal{C}$ first constructs ℓ shares of $\mathbf{v}' = (v'_1, v'_2, \cdots, v'_m) \in Z_q^m$ using a Shamir secret-sharing technique applied to each coordinate of $\mathbf{v}'$ independently as before. That is, $\mathcal{C}$ gets $\{\overline{v'_1}, \overline{v'_2}, \cdots, \overline{v'_\ell}\}$, such that $\mathbf{v}' = \sum_{k\in\mathcal{I}} \xi_k \overline{\mathbf{v}'_\mathbf{k}} \pmod q$, where $\xi_k = \prod_{i\neq k, i\in\mathcal{I}} \frac{0-i}{k-i}$ is the corresponding fractional lagrangian coefficient.

(2) Calculate n vectors $\rho'_i = H_2(\mathbf{v}' \| i) \in Z_q^m$ for $i \in \{1, 2, \cdots, n\}$.

(3) Compute the inner products $f'_{j,i} = \langle \overline{v'_j}, \rho'_i \rangle$, where $1 \le j \le \ell$ and $1 \le i \le n$, and

parse $f_j^{'} = (f_{j,1}^{'}, \cdots, f_{j,n}^{'})^{\top}$.

(4) Evaluate $\theta_j^{'} \leftarrow SamplePre(P_{j,\omega_j^{'}}(H_1(\omega_j^{'} \| \omega' \| j))^{-1}, S_{j,\omega_j^{'}}^{'}, f_j^{'}, \delta_1)$ for $j \in \{1,2,\cdots,\ell\}$.

Finally, $\mathcal{C}$ outputs the fuzzy identity-based signature $\theta_{\omega',\mathbf{v}'}^{'} = \{\mathbf{v}', (\theta_1^{'}, \theta_2^{'}, \cdots, \theta_\ell^{'}), \omega'\}$ and sends it to the adversary $\mathcal{F}$.

Output: After performing a number of queries above, the adversary $\mathcal{F}$ produces a valid forgery $\{\mathbf{v}^*, (\theta_1^*, \theta_2^*, \cdots, \theta_\ell^*), \omega^*\}$ of the target identity ω^*. We can see that the distribution of the challenger's output is statistically indistinguishable from the distribution of the output in the real fuzzy identity-based signature scheme. Since $\{\mathbf{v}^*, (\theta_1^*, \theta_2^*, \cdots, \theta_\ell^*), \omega^*\}$ is a valid forgery, thus for each $j \in \{1,2,\cdots,\ell\}$, $\theta_j^* \in D_n$ and there exists a subset $\mathcal{I} \subseteq \{1,2,\cdots,\ell\}$ and $|\mathcal{I}| = t$ s.t. $\sum_{j \in \mathcal{I}} \xi_j P_{j,\omega_j^*}(H_1(\omega_j^* \| \omega^* \| j))^{-1} \theta_j^* = f^*$, where $f^* = (\langle \mathbf{v}^*, \rho_1^* \rangle, \langle \mathbf{v}^*, \rho_2^* \rangle, \cdots, \langle \mathbf{v}^*, \rho_n^* \rangle)^{\top}$, and for each $i \in \{1,2,\cdots,n\}$, $\rho_i^* = H_2(\mathbf{v}^* \| i) \in Z_q^m$. Without loss of generality, we consider the case that the subset $\mathcal{I} = \{1,2,\cdots,t\}$, as $\{\mathbf{v}^*, (\theta_1^*, \theta_2^*, \cdots, \theta_\ell^*), \omega^*\}$ is a valid forgery, then get $0 < |\theta_j^*| \le \delta_1 \sqrt{m}$, $1 \le j \le \ell$ and the equation as follows:

$$P_{1,\omega_1^*}(H_1(\omega_1^* \| \omega^* \| 1))^{-1} \xi_1 \theta_1^* + P_{2,\omega_2^*}(H_2(\omega_2^* \| \omega^* \| 2))^{-1} \xi_2 \theta_2^* \cdots + P_{t,\omega_t^*}(H_2(\omega_t^* \| \omega^* \| t))^{-1} \xi_t \theta_t^* = f^*$$

Furthermore, we get that:

$$(P_{1,\omega_1^*}(H_1(\omega_1^* \| \omega^* \| 1))^{-1} \cdots P_{\ell,\omega_\ell^*}(H_1(\omega_\ell^* \| \omega^* \| \ell))^{-1})(\xi_1 \theta_1^*, \cdots, \xi_t \theta_t^*, 0, \cdots, 0)^{\top} = f^*.$$

Since:

$$\begin{aligned} & P_{1,\omega_1^*}(H_1(\omega_1^* \| \omega^* \| 1))^{-1} = P_{1,\omega_1^*}(R_1^*)^{-1} \\ & = E_1, P_{2,\omega_2^*}(H_1(\omega_2^* \| \omega^* \| 2))^{-1} = P_{2,\omega_2^*}(R_2^*)^{-1} \\ & = E_2, P_{\ell,\omega_\ell^*}(H_1(\omega_\ell^* \| \omega^* \| \ell))^{-1} = P_{\ell,\omega_\ell^*}(R_\ell^*)^{-1} = E_\ell \end{aligned}$$

Therefore, $(E_1 \| E_2 \| \cdots \| E_\ell)(\xi_1 \theta_1^*, \cdots, \xi_t \theta_t^*, 0, \cdots, 0)^{\top} = f^*$. Since $D = (\ell!)^2$, and it has been proved in [12] that $D\xi_j \in \mathcal{Z}$ and $|D\xi_j| \le (\ell!)^3$ for all $j \in \{1,2,\cdots,\ell\}$ to clear the denominators of $\xi_j (j \in \{1,2,\cdots,\ell\})$. So $(E_1 \| E_2 \| \cdots \| E_\ell)(D\xi_1 \theta_1^*, \cdots, D\xi_t \theta_t^*, 0, \cdots, 0)^{\top} = Df^*$.

Thus the equation $P(D\xi_1 \theta_1^*, \cdots, D\xi_t \theta_t^*, 0, \cdots, 0)^{\top} = F$ holds. For each θ_j^*, $0 < \| \theta_j^* \| \le \delta_1 \sqrt{m}$, as $\theta^* = (D\xi_1 \theta_1^*, \cdots, D\xi_t \theta_t^*, 0, \cdots, 0)^{\top}$, we have $0 < \| \theta^* \| \le (\ell!)^3 \delta_1 \sqrt{mt}$. Finally, the challenger $\mathcal{C}$ can run the adversary $\mathcal{A}$ as a subroutine to output θ^* as a solution of the $ISIS_{\{n,m\ell,q,(\ell!)^3 \delta_1 \sqrt{mt}\}}$ assumption with a non-negligible probability. Consequently, we conclude that our proposed fuzzy identity-based scheme is EU-ACMIA secure in the random oracle model.

6. Application to biometric authentication

Now we show how our FIBS scheme is used in biometric authentication. A biometric authentication system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that

the person possesses [22]. Since biometrics cannot be lost or forgotten like, e.g. computer passwords, biometric have the potential to offer higher security and more convenience for the users. We adopt the biometric authentication model described in [23]. It consists of two phases: an enrollment phase and an authentication/Verification phase.

Enrollment Phase

(1) First, Alice goes with her biometric data through an enrollment phase at a certification authority (CA). During this procedure the properties of her biometric data are measured with specialized equipment. We model the measurement data as a feature vector $\omega = \{\omega_1, \omega_2, \cdots, \omega_\ell\} \in \{0,1\}^\ell$.

(2) From the measurement data, the private key S_ω is derived using the algorithm NewBasisDel in FIBS.Extract.

(3) Then the reference data $(\theta_1, \theta_2, \cdots, \theta_\ell)$ stored in the database is obtained by applying FIBS.Sign to S_ω using "Alice" as the message. Then the certification authority (CA) stores $f = (\langle "Alice", \rho_1 \rangle, \langle "Alice", \rho_2 \rangle, \cdots, \langle "Alice", \rho_n \rangle)^\top$ ($\rho_i = H_2("Alice" \| i) \in Z_q^m$ for each $i \in \{1, 2, \cdots, n\}$) together with the reference data and the biometric measurement data.

(4) CA then erases the private key S_ω, the message "Alice" and all the intermediate data physically.

Authentication/verification phase

(1) When Alice wants to authenticate herself to Bob at a later point in time, a measurement that extracts analog data η of her biometric data is taken. Alice sends $f = (\langle "Alice", \rho_1 \rangle, \langle "Alice", \rho_2 \rangle, \cdots, \langle "Alice", \rho_n \rangle)^\top$ ($\rho_i = H_2("Alice" \| i) \in Z_q^m$ and η to CA.

(2) Bob computes $f' = (\langle "Bob", \rho_1 \rangle, \langle "Bob", \rho_2 \rangle, \cdots, \langle "Bob", \rho_n \rangle)^\top$, and randomly choose $(\zeta_1, \zeta_2, \cdots, \zeta_\ell)$, where $\zeta_j \in Z_q^m$, $j = 1, 2 \cdots, \ell$. Finally, Bob returns f' and $(\zeta_1, \zeta_2, \cdots, \zeta_\ell)$ to CA.

(3) CA finds the reference data $(\theta_1, \theta_2, \cdots, \theta_\ell)$ and biometric measurement data ω by searching $f = (\langle "Alice", \rho_1 \rangle, \langle "Alice", \rho_2 \rangle, \cdots, \langle "Alice", \rho_n \rangle)^\top$.

(4) CA computes the set $\mathcal{I} = \omega \cap \eta$ and returns $\{\theta_j^{'}\}_{j \in \mathcal{I}}$ and ω to Alice, where $\theta_j^{'} = \theta_j + \zeta_j$, $j = 1, 2 \cdots, \ell$.

(5) Then, Alice sends $(\omega, \{\theta_j^{'}\}_{j \in \mathcal{I}}, "Alice", f' = (\langle "Bob", \rho_1 \rangle, \langle "Bob", \rho_2 \rangle, \cdots, \langle "Bob", \rho_n \rangle)^\top)$ to Bob by a secure channel.

(6) Finally, Bob first get $\{\theta_j\}_{j \in \mathcal{I}}$, each $\theta_j = \theta_j^{'} - \zeta_j$ $j = 1, 2 \cdots, \ell$, then checks whether $f' = (\langle "Bob", \rho_1 \rangle, \langle "Bob", \rho_2 \rangle, \cdots, \langle "Bob", \rho_n \rangle)^\top$ is right, where $\theta_j \in D_n$ for all $j \in \mathcal{I}$, and whether the following equation holds:

$$\sum_{j \in \mathcal{I}} \xi_j P_{j,\omega_j}(H_1(\omega_j \| \omega \| j))^{-1} \theta_j = (\langle "Alice", \rho_1 \rangle, \langle "Alice", \rho_2 \rangle, \cdots, \langle "Alice", \rho_n \rangle)^\top$$

Where $\xi_j = \prod_{i \neq j, i \in \mathcal{I}} \frac{0-i}{j-i}$ is the corresponding fractional lagrangian coefficient. If it holds, Alice passes the authentication. Otherwise, Alice fails the authentication.

7. Conclusions

In this paper, we have proposed a new construction of fuzzy identity-based signature (FIBS) based on lattice assumption, which can resist quantum computer attacks. Our proposed scheme takes advantage of the lattice basis delegation technique to keep the lattice dimension unchanged, thus the size of the fuzzy identity-based signature length is invariant and much shorter. Moreover, our proposed scheme is proved existentially unforgeable under an adaptive chosen message and identity attacks (EU-ACMIA) in the random oracle model. Compared with the previous lattice-based FIBS scheme [13], our proposed FIBS scheme is more efficient, especially in terms of the communication overhead. Due to the feature of FIBS that user's identity is viewed as a set of descriptive attributes instead of a string of characters, our FIBS scheme can be well applied in biometric authentication even in the post-quantum cryptographic communication environments. The extension to an efficient fuzzy identity-based signature scheme from lattice in the standard model is our future work.

8. Acknowledgements

This work is supported by the National Natural Science Foundation of China (No.61370203) and the Young Scholars Development Fund of SWPU (No.201599010139).

References

[1] Shamir, “Identity-based cryptosystems and signature schemes,” in *Proc. of Advances in cryptology-CRYPTO'84*, LNCS, Springger-Verlag, pp.47-53, 1984. Article(CrossRef Link)

[2] A. Sahai, B. Waters, “Fuzzy identity-based encryption,” in *Proc. of advances in cryptology-In Eurocrypt*, LNCS 3494, pp.457-473, 2005. Article(CrossRef Link)

[3] 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*, New York, USA, pp.221-238, 2006. Article(CrossRef Link)

[4] L. Cheung, C. Calvin, “Provably secure ciphertect policy ABE,” in *Proc. of the 13th ACM Conference on Computer and Communication Security*, New York, USA, pp. 456-465, 2007. Article(CrossRef Link)

[5] P. Yang, Z. Cao, X. Dong, “Fuzzy identity based signature with applications to biometric authentication,” *Computers and Electrical Engineering*, vol. 37, no. 4, pp. 532-540, 2011. Article(CrossRef Link)

[6] C. Wang, J. Kim, “Two constructions of fuzzy identity based signature,” in *Proc. of International conference on biomedical engineering and informatics*, pp. 1-5, 2009. Article(CrossRef Link)

[7] C. Wan, W. Che, Y. Liu, “A fuzzy identity based signature scheme,” in *Proc. of International conference on E-business and information system security*, pp. 1-5, 2009. Article(CrossRef Link)

[8] C. Wang, “A provable secure fuzzy identity based signature scheme,” *Science China Information Sciences*, vol. 55, no. 9, pp. 2139-2148. 2012. Article(CrossRef Link)

[9] L. Zhang, Q. Wu, Y. Hu, "Fuzzy Biometric Identity-Based Signature in the Standard Model,” *Applied Mechanics and Materials*, vols. 44-47, pp. 3350-3354, 2011. Article(CrossRef Link)

[10] P. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484-1509, 1999 Article(CrossRef Link)

[11] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. of the thirty-seventh annual ACM symposium on Theory of computing*, pp.84-93, 2005. Article(CrossRef Link)

[12] S. Agrawal, X. Boyen, Vaikuntanathan, P. Voulgaris, H. Wee, "Functional encryption for threshold functions (or Fuzzy IBE) from Lattices," *Public Key Cryprography*, pp. 280-297, 2012. Article(CrossRef Link)

[13] Y. Yao, Z. Li, "A novel fuzzy identity based signature scheme based on the short integer solution problem," *Computers and Electronical Engineering*, vol. 40, no. 6, pp.1930-1939, 2014. Article(CrossRef Link)

[14] D. Cash, D. Hofhein, E. Kiltz, C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Proc. of Advances in Cryptology-Eurocrypto 2010*, LNCS, Springer-Verlag: Heidelberg, vol.6110, pp.523-552, 2010. Article(CrossRef Link)

[15] V. Lyubashevsky, D. Micciancio, "Asymptotically efficient lattice-based digital signatues," in *Proc. of Theory of Cryptography Conference*, LNCS, Berlin, Springer-Verlag, vol. 4948, pp.37-54, 2008. Article(CrossRef Link)

[16] M. Ajtai, "Generating hard instances of the short basis problem," in *Proc. of Automata, languages and Programming ICALP 1999*, LNCS, Springer Verlag; Prague, Czech Republic,vol. 1644, pp.1-9, 1999. Article(CrossRef Link)

[17] J. Alwen, C. Peikert, "Generating shorter bases for hard random lattices," *Theory of Computing Systems*, vol. 48, no. 535, pp.75-86, 2009. Article(CrossRef Link)

[18] C. Gentry, C. Peiker, V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. of the fortieth annual ACM symposium on Theory of computing*, pp.197-206, 2008. Article(CrossRef Link)

[19] 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*, LNCS, Springer-Verlag, vol. 6223, pp.98-115, 2010. Article(CrossRef Link)

[20] D. Boneh, D. Freeman, "Linearly homomorphic signatures over binary fields and new tools for lattice-based signature," in *Proc. of PKC 2011*, Berlin:Springer-Verlag, vol. 6571, pp.1-16, 2011. Article(CrossRef Link)

[21] F. Wang, Y. Hu, B. Wang, "Lattice-based linearly homomorphic signature scheme over binary field," *Science China Information Sciences*, vol. 56, no. 11, pp.1-9, 2013. Article(CrossRef Link)

[22] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric recognition: security and privacy concerns," *IEEE Security and Privacy*, vol. 1, no. 2, pp.33-42, 2003. Article(CrossRef Link)

[23] E. Verbitskiy, P. Tuyls, D. Denteneer, J. P. Linnartz, "Reliable biometric authentication with privacy protection," in *Proc. of the 24th symposium on information theory*, pp.125-132, 2004. Article(CrossRef Link)

Xiaojun Zhang received the B.S. degree in mathematics and applied mathematics from Hebei Normal University in 2009 and received M.S. degree in pure mathematics from Guangxi University in 2012. He received Ph.D. degree in infor- mation security at University of Electronic Science Technology of China in 2015. He is a lecturer in the School of Computer Science, Southwest Petroleum University, he also works as a Postdoctoral Fellow at University of Electronic Science Technology of China from 2016. He is now presently engaging in cryptography, network security and cloud computing security.

Chunxiang Xu received her B.Sc., M.Sc. and Ph.D. degrees at Xidian University, in 1985, 1988 and 2004 respectively, P.R.C. She is presently engaged in information security, cloud computing security and cryptography as a professor at University of Electronic Science Technology of China (UESTC). She is now presently engaging in cryptography, network security and cloud computing security.

Yuan Zhang received his B.Sc. degree in University of Electronic Science Technology of China (UESTC) in 2013,P.R.China. He is currently a doctoral student in School of Computer Science and Engineering at University of Electronic Science Technology of China. His research interests are cryptography, network security and Cloud Computing security.