A Fuzzy Identity-Based Signcryption Scheme from Lattices

Xiuhua Lu [1,2], **Qiaoyan Wen** [1], **Wenmin Li** [1], **Licheng Wang** [3], **and Hua Zhang** [1]
[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications
Beijing, 100876 - China
[e-mail: luxiuhua2015@163.com]
[2] Faculty of Mathematics and Information Science, Langfang Teachers University
Langfang, 065000 - China
[e-mail: luxiuhua2015@163.com]
[3] Information Security Center, Beijing University of Posts and Telecommunications
Beijing, 100876 - China
[e-mail: wanglc2012@126.com]
*Corresponding author: Xiuhua Lu

Received July 18, 2014; revised September 9, 2014; accepted October 1, 2014; published November 30, 2014

Abstract

Fuzzy identity-based cryptography introduces the threshold structure into identity-based cryptography, changes the receiver of a ciphertext from exact one to dynamic many, makes a cryptographic scheme more efficient and flexible. In this paper, we propose the first fuzzy identity-based signcryption scheme in lattice-based cryptography. Firstly, we give a fuzzy identity-based signcryption scheme that is indistinguishable against chosen plaintext attack under selective identity model. Then we apply Fujisaki-Okamoto method to obtain a fuzzy identity-based signcryption scheme that is indistinguishable against adaptive chosen ciphertext attack under selective identity model. Thirdly, we prove our scheme is existentially unforgeable against chosen message attack under selective identity model. As far as we know, our scheme is the first fuzzy identity-based signcryption scheme that is secure even in the quantum environment.

Keywords: Fuzzy identity-based cryptography; signcryption; lattice-based cryptography; LWE problem; SIS problem

This research was supported by NSFC (Grant Nos. 61300181, 61272057, 61202434, 61170270, 61100203, 61121061, 61402015), the Fundamental Research Funds for the Central Universities (Grant No. 2012RC0612), Langfang Teachers University Youth Funds (Grant No. LSZQ201303), Langfang Municipal Science and Technology Support Program (Grant No. 2014011029), Hebei Education Funds for Youth Project (Grant No. QN20131047).

http://dx.doi.org/10.3837/tiis.2014.11.031

1. Introduction

In public key cryptography, a user has a pair of public key and a private key, and this pair is bounded with the user by a trusted third party. For security consideration, the user and the matching public/private key should be updated frequently, and it is complicated to maintain public key infrastructure to support key authenticity. In order to solve this problem, Shamir introduced identity-based cryptography[1]. In identity-based cryptography, a user's identity is viewed as his public key, and the associated private key is generated by a private key generator, and the relation between a user and his public/private key is natural. Identity-based cryptography doesn't depend on the complex public key infrastructure, simplifies the user key management, and leads to more practical cryptosystems[2, 3].

However, one person must ascertain the receiver, in public key cryptography and identity-based cryptography, when he encrypts a message. The truth of the matter is that, the sender couldn't ascertain the receiver in such situations as pay-TV systems and cloud storages, for the group of receivers is of a dynamic change. To adapt to this environment, we may introduce access control structure in encryption, and allow people, who are admitted by the access control structure, to decrypt the ciphertext. When the access control structure is specific to threshold structure, it is fuzzy identity-based cryptography. Fuzzy identity-based cryptography is an error-tolerant identity-based cryptography. In other words, a ciphertext or signature obtained via an identity id can be decrypted or verified via an identity id' if and only if the difference between id and id' is within a certain range, and the range is the threshold value.

Fuzzy identity-based encryption(FIBE) was introduced by Sahai and Waters[4]. Sahai and Waters formalized the model of fuzzy identity-based encryption and provided two fuzzy identity-based encryption schemes which are secure against chosen plaintext attack under selective identity model. Subsequently, Baek et al. gave two more efficient fuzzy identity-based encryption schemes[5] using Pirretti et al.'s results[6], and Li et al. proposed a fuzzy identity-based encryption scheme with dynamic threshold[7].

When it comes to digital signature, Yang et al. firstly introduced the notion of fuzzy identity-based signature(FIBS)[8] and gave a specific construction based on Sahai and Waters's fuzzy identity-based encryption schemes[4]. Afterward, Wang proposed a fuzzy identity-based signature scheme with shorter parameters and more efficient verification[9], and Wu also proposed a fuzzy identity-based signature scheme with the generalized selective identity security[10].

Aiming at further improvement in the practicability of cryptographic system, Zheng introduced the notion of signcryption to combine encryption and signature[11]. Signcryption is a cryptographic primitive that can perform the functions of public key encryption and digital signature in a logic step, so that it cuts down the cost of computation and communication without security compromise. To meet the needs of biometric identity, Zhang et al.[12] and Li et al. [13] introduced fuzziness property into signcryption respectively, and proposed fuzzy signcryption schemes.

So far, all the literatures mentioned above are based on the traditional numerical assumptions, and Shor's groundbreaking results[14] show that these schemes are not secure in the quantum era. Thus, it is a rewarding work to build quantum secure cryptographic schemes. Lattice-based cryptography is an outstanding representative of post-quantum cryptography, and there exist many public key encryption schemes[15, 16, 17] and digital signature schemes[18, 19, 20] based on lattice theory. But as far as we know, there aren't fuzzy identity-based signcryption schemes based on lattice assumptions.

In this paper, we give the first fuzzy identity-based signcryption scheme based on lattice assumptions. According to the technique in [21], we take the signature associated with the message as an error vector, to disturb the lattice point associated with the message. As a result, we bind the encrypted message and the signature to realize confidentiality and authentication simultaneously. And we reduce the frequency of sampling errors compare with the generic sign-then-encrypt method. To accomplish ukeyExtract queries in the proof of existential unforgeability against chosen message attack under selective identity model, we introduce identity information to public key for encryption. In order to further decrease the length of the ciphertext, we make use of the technique of the lattice basis delegation in fixed dimension[16]. In addition, we apply the Fujisaki-Okamoto method[22] to increase our scheme's security from indistinguishability against chosen plaintext attack under selective identity model(IND-sID-CPA) to indistinguishability against adaptive chosen ciphertext attack under selective identity model(IND-sID-CCA2).

The following is the roadmap of our paper. Section 2 includes preliminaries that are necessary in our construction, Section 3 gives the formal definition of a fuzzy identity-based signcryption scheme. Section 4 introduces the security definitions of a fuzzy identity-based signcryption scheme. Section 5 gives our new scheme and its consistency analysis. Section 6 gives the security analysis of our scheme. Section 7 provides its efficiency analysis and performance comparison with other related schemes. Finally, Section 8 is summary and conclusions.

2. Preliminaries

In this section, we give an overview of basic notions and results that are involved in our construction about lattice-based cryptography. We refer readers to [15, 16, 23] for more details.

Definition 2.1 *A lattice is a discrete addition subgroup in* R^m, *and if it is generated by* n *linearly independent vectors* $a_1,\cdots,a_n \in \mathrm{R}^m$, *then matrix* $A=[a_1|\cdots|a_n]$ *is a basis of the lattice, and the lattice can be denoted by* $\Lambda(A)$.

Definition 2.2 *Two integer lattices, as well as a lattice shift, are often used in lattice-based cryptography, and we give their definitions as follows. For* $A \in Z_q^{n\times m}$ *and* $u \in Z_q^n$,

$$\Lambda_q(A)=\{e\in Z^m \mid \exists s\in Z_q^n \text{ such that } e=A^{\mathrm{T}}s(\bmod q)\}$$

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

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

Definition 2.3 *For* $\Lambda \subseteq Z^m$, $\mathbf{c}\in \mathrm{R}^m$, $\sigma \in \mathrm{R}^+$, *let* $\rho_{\sigma,c}(x)=exp(-\pi\frac{\|x-c\|^2}{\sigma^2})$, $\rho_{\sigma,c}(\Lambda)=\sum_{x\in\Lambda}\rho_{\sigma,c}(x)$, *then* $\forall y\in\Lambda, \mathrm{D}_{\Lambda,\sigma,c}(y)=\frac{\rho_{\sigma,\mathbf{c}}(y)}{\rho_{\sigma,c}(\Lambda)}$ *is a discrete Gaussian distribution over* Λ, *whose center is* c *and parameter is* σ. *When* $c=0$ *or* $\sigma=1$, *we can omit them.*

Lemma 2.4 *With integer* $q\geq 3$, $m\geq Cn\log q$, *where* $C>1$ *is a fixed constant, algorithm*

TrapGen *outputs* $A \in Z_q^{n\times m}$ *and* $T \in Z^{m\times m}$*, which satisfy the following properties.*

1. The statistical distance between the distribution of A and uniform distribution on $Z_q^{n\times m}$ is negligible.
2. $AT = 0(\mathrm{mod}\, q)$.
3. $\|T\| \le O(n\log q)$ and $\|\tilde{T}\| \le O(\sqrt{n\log q}) = L$.

Definition 2.5 *Let* $\sigma_R = L\cdot\omega(\sqrt{\log m})$, $D_{m\times m}$ *is the distribution* $(D_{Z^m,\sigma_R})^m$ *and if* $R \leftarrow D_{m\times m}$*, then* R *is* $Z_q -$*invertible.*

Lemma 2.6 *For* $A\in Z_q^{n\times m}$ *with rank* n, $R\leftarrow D_{m\times m}$*, a short basis* T_A *of* $\Lambda_q^{\perp}(A)$*, and Gaussian parameter* $\sigma_1 > L^2\cdot\sqrt{m}\cdot\omega(\log^2 m)$*, algorithm* ***BasisDel*** *outputs a basis* T_B *of* $\Lambda_q^{\perp}(B)$ *for* $B = AR^{-1}$*, where* $\|\tilde{T}_B\| \le L\cdot m^{\frac{3}{2}}\cdot\omega(\log^2 m)$.

Lemma 2.7 *Algorithm* ***SampleRwithBasis***(A) *is important in security proof. Its input is a matrix* A*, which comes from* $Z_q^{n\times m}$ *uniformly and randomly. Its output are matrices* R *and* T*, where* R *follows the distribution* $D_{m\times m}$, T *is a short basis of* $\Lambda_q^{\perp}(AR^{-1})$.

Lemma 2.8 *For* $B\in Z_q^{n\times m}$*, a short basis* T_B *of* $\Lambda_q^{\perp}(B)$, $u\in Z_q^n$*, and Gaussian parameter* $\sigma_2 \ge \|\tilde{T}_B\|\cdot\omega(\sqrt{\log m})$*, algorithm* ***SamplePre*** *outputs some* $e\in Z^m$ *such that* $\|e\|\le\sigma_2\cdot\sqrt{m}$ *and* $Be = u(\mathrm{mod}\, q)$.

Definition 2.9 *For a size parameter* $n\ge 1$*, a modulus* $q\ge 2$*, and an appropriate normal distribution* X *on* Z_q, $\mathbf{A}_{s,X}$ *is the distribution obtained by selecting a vector* $a\in Z_q^n$ *uniformly, sampling* $x \sim X$*, and outputting* $(a, a^{\mathrm{T}}s + x)\in Z_q^n\times Z_q$.

An $(Z_q, n, X)-$LWE problem instance is composed of access to an unspecified challenge oracle O, which is, either, a pseudo-random sampler O_s associated with some random secret $s\in Z_q^n$, or, a random sampler O_u.

O_s: outputs such samples as $(a_i, b_i) = (a_i, a_i^{\mathrm{T}}s + x_i)\in Z_q^n\times Z_q$, where a_i follows uniform distribution on Z_q^n, x_i follows distribution X.

O_u: outputs such samples as (a_i, b_i) which follows uniform distribution on $Z_q^n\times Z_q$.

Given an $(Z_q, n, X)-$LWE problem instance, if there is an efficient algorithm to decide which oracle is accessed, then there is an efficient algorithm to approximate the SIVP and GapSVP problems in the worst case.

Definition 2.10 *The* $(n,m,q,\beta)-$ *small integer solution problem* $SIS_{n,m,q,\beta}$ *is that for* $A\in Z_q^{n\times m}$*, and a real* β*, find a vector* $e\in Z^m$ *such that* $Ae = 0(\mathrm{mod}\, q)$ *and* $0 < \|e\|_2 \le \beta$*, where* $\|\cdot\|_2$ *is the Euclidean norm.*

Given an $SIS_{n,m,q,\beta}$ problem instance, if there is an efficient algorithm to find its small integer solution e, then there is an efficient algorithm to approximate the SIVP problem in the worst case.

3. Formal definition of a fuzzy identity-based signcryption

In this section, we give the formal definition of a fuzzy identity-based signcryption.

A fuzzy identity-based signcryption scheme has five PPT algorithms as follows.

- Setup $(1^n, d, d')$ – On input system security parameter 1^n, two thresholds d and d', this algorithm outputs public parameter PP and master secret key msk.
- uKeyExtract (msk, id) – On input master secret key msk, an identity id, this algorithm outputs the unsigncryption key uk_{id}.
- sKeyExtract (msk, id) – On input master secret key msk, an identity id, this algorithm outputs the signature key sk_{id}.
- Signcrypt (M, sk_{id_s}, id_e) – On input a message M, an identity id_e for encryption, an identity id_s as well as its signature key sk_{id_s}, this algorithm outputs a ciphertext C.
- Unsigncrypt (C, uk_{id_u}, id_v) – On input a ciphertext C, an identity id_v for verification, an identity id_u as well as its unsigncryption key uk_{id_u}, if $|id_u \cap id_e| \geq d$ and $|id_v \cap id_s| \geq d'$, this algorithm gets the message M, and verifies the validity of the message and its signature. If verification is successful, this algorithm returns the message M, otherwise returns $\perp$.

These five algorithms must satisfy consistency property of a fuzzy identity-based signcryption, that is, if $C = Signcrypt(M, sk_{id_s}, id_e)$, and $|id_u \cap id_e| \geq d$, $|id_v \cap id_s| \geq d'$, then we should have $M = Unsigncrypt(C, uk_{id_u}, id_v)$.

4. Security notions

The security of a fuzzy identity-based signcryption scheme includes two factors: message confidentiality and ciphertext unforgeability, which are illuminated in detail as follows.

4.1 Message confidentiality

With regard to the message confidentiality of a fuzzy identity-based signcryption scheme, we define two definitions of different security levels: indistinguishability against chosen plaintext attack under selective identity model(IND-sID-CPA), and indistinguishability against adaptive chosen ciphertext attack under selective identity model(IND-sID-CCA2).

The following game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ describes the indistinguishability against adaptive chosen ciphertext attack under selective identity model(IND-sID-CCA2).

- Target – The adversary $\mathcal{A}$ decides an identity id^* to be his attack target, and returns it to the challenger $\mathcal{C}$.
- Setup – The challenger $\mathcal{C}$ inputs secure parameter 1^n, two thresholds d and d', invokes

Setup$(1^n, d, d')$ algorithm to get public parameter PP and master secret key msk. Public parameter PP is sent to the adversary $\mathbb{A}$ and master secret key msk is kept secret.

• Phase 1 – In this phase, the adversary $\mathbb{A}$ has the right to ask the following queries with a number of polynomial bounded, and the challenger $\mathbb{C}$ must return reasonable answers.

uKeyExtract(id) – The adversary $\mathbb{A}$ asks for the unsigncryption key for an identity id with $|id \cap id^*| < d$. The challenger $\mathbb{C}$ invokes algorithm uKeyExtract(msk, id) and returns its result to $\mathbb{A}$.

sKeyExtract(id) – The adversary $\mathbb{A}$ asks for the signature key for an identity id. The challenger $\mathbb{C}$ invokes algorithm sKeyExtract(msk, id) and returns its result to $\mathbb{A}$.

Unsigncrypt(C, id_u, id_v) – The adversary $\mathbb{A}$ provides a ciphertext C, an identity id_u for unsigncryption, and an identity id_v for verification. The challenger $\mathbb{C}$ computes uk_{id_u} = uKeyExtract(id_u), then invokes algorithm Unsigncrypt(C, uk_{id_u}, id_v) and returns its result to $\mathbb{A}$.

• Challenge – When Phase 1 ends, the adversary $\mathbb{A}$ selects two messages M_0, M_1 with same length, and an identity id_s^* for signature, sends all of them to the challenger $\mathbb{C}$ for challenge ciphertext. $\mathbb{C}$ selects a bit b randomly, computes the signature key $sk_{id_s^*}$ = sKeyExtract(id_s^*) and returns C^* = Signcrypt$(M_b, sk_{id_s^*}, id^*)$ to $\mathbb{A}$.

• Phase 2 – The adversary $\mathbb{A}$ repeats what he did in Phase 1, with the exception that he couldn't execute Unsigncrypt query on (C^*, id_u, id_v) with $|id_u \cap id^*| \geq d$ and $|id_v \cap id_s^*| \geq d'$.

• Guess – The adversary $\mathbb{A}$ gives his guess b' for b which the challenger $\mathbb{C}$ used in Challenge phase. If $b' = b$, we say the adversary $\mathbb{A}$ wins the game.

The advantage of adversary $\mathbb{A}$ in this game is denoted as $Adv(\mathbb{A}) = |Pr[b' = b] - \frac{1}{2}|$.

Definition 4.1 *If all polynomially bounded adversaries have negligible advantages in the above game, then a fuzzy identity-based signcryption scheme is indistinguishable against adaptive chosen ciphertext attack under selective identity model. In other words, a fuzzy identity-based signcryption scheme is IND-sID-CCA2 secure.*

If the Unsigncrypt query is forbidden in the above game, then the game and the associated definition 4.1 describe the indistinguishability against chosen plaintext attack under selective identity model(IND-sID-CPA).

4.2 Ciphertext unforgeability

With regard to the ciphertext unforgeability of a fuzzy identity-based signcryption scheme, we define the following game between a challenger $\mathbb{C}$ and an adversary $\mathbb{A}$ to describe the existential unforgeability against chosen message attack under selective identity model(EUF-sID-CMA).

• Target – The adversary $\mathbb{A}$ decides an identity id^* to be his attack target, and returns it to the challenger $\mathbb{C}$.

• Setup – The challenger $\mathcal{C}$ inputs secure parameter 1^n, two thresholds d and d', invokes Setup$(1^n, d, d')$ algorithm to get public parameter PP and master secret key msk. Public parameter PP is sent to the adversary $\mathcal{A}$ and master secret key msk is kept secret.
• Query – In this phase, the adversary $\mathcal{A}$ has the right to ask the following queries with a number of polynomial bounded, and the challenger $\mathcal{C}$ must return reasonable answers.
uKeyExtract(id) – The adversary $\mathcal{A}$ asks for the unsigncryption key for an identity id. The challenger $\mathcal{C}$ invokes algorithm uKeyExtract(msk, id) and returns its result to $\mathcal{A}$.
sKeyExtract(id) – The adversary $\mathcal{A}$ asks for the signature key for an identity id, which satisfy $|id \cap id^*| < d'$. The challenger $\mathcal{C}$ invokes algorithm sKeyExtract(msk, id) and returns its result to $\mathcal{A}$.
Signcrypt(M, id_s, id_e) – The adversary $\mathcal{A}$ provides a message M, an identity id_s for signature, an identity id_e for encryption. The challenger $\mathcal{C}$ computes sk_{id_s} = sKeyExtract(id_s), then invokes algorithm Signcrypt(M, sk_{id_s}, id_e) and returns its result to $\mathcal{A}$.
• Forge – The adversary $\mathcal{A}$ replies to $\mathcal{C}$ with a ciphertext C^* as well as an encryption identity id_e^*. If adversary $\mathcal{A}$'s reply is valid, that is to say, there exist id_u and id_v which satisfy $|id_u \cap id_e^*| \geq d$ and $|id_v \cap id^*| \geq d'$, Unsigncrypt $(C^*, uk_{id_u}, id_v) = M \neq \perp$ for uk_{id_u} = uKeyExtract(id_u) and $\mathcal{A}$ didn't make Signcrypt(M, id^*, id_e^*) query, then we say the adversary $\mathcal{A}$ wins the game.

The advantage of adversary $\mathcal{A}$ in this game is denoted by $Adv(\mathcal{A}) = Pr[\mathcal{A}\ wins]$.

Definition 4.2 *If all polynomially bounded adversaries have negligible advantages in the above game, then a fuzzy identity-based signcryption scheme is existentially unforgeable against chosen message attack under selective identity model. In other words, a fuzzy identity-based signcryption scheme is EUF-sID-CMA secure.*

5. Our fuzzy identity-based signcryption scheme

At first, we give an IND-sID-CPA secure fuzzy identity-based signcryption scheme – Construction 1, then we apply Fujisaki-Okamoto method to Construction 1 to obtain an IND-sID-CCA2 secure fuzzy identity-based signcryption scheme – Construction 2.

5.1 Construction 1

• **Setup**(n, d, d') On input security parameter $n = l^{\frac{1}{\varepsilon}}$, where l is the length of an identity, $\varepsilon \in (0,1)$ is a constant, and two thresholds d and d',

1. For $q = poly(n)$ and $pq \in [n^6 \cdot 2^{5l}, 2n^6 \cdot 2^{5l}]$, let $m = n^{1.5}$,
$\sigma_0 = O(\sqrt{n\log(pq)})\omega(\sqrt{\log m})$, $\sigma = O(n\log(pq))\sqrt{m}\omega(\log^2 m)$,
$\sigma' = O(\sqrt{n\log(pq)})m^{\frac{3}{2}}\omega(\log^{\frac{5}{2}} m)$, $\mathcal{D}_n = \{e \in \mathbb{Z}^m : \|e\| \leq \sigma'\sqrt{m}\}$.

2. For $i \in [l], b \in \{0,1\}$, invoke algorithm $TrapGen(n)$ to obtain $(A_{i,b}, T_{i,b})$, with the condition that

(a) $A_{i,b} \in Z_{pq}^{n\times m}$ follows uniform distribution with overwhelming probability.

(b) $T_{i,b}$ is a short basis of $\Lambda_{pq}^{\perp}(A_{i,b})$ and $\|T_{i,b}\| \le O(\sqrt{n\log(pq)})$.

3. For message space $\mathbb{M} = \{0,1\}^k$, let $t \in [k]$, select $u_t = (u_{t1}, \cdots, u_{tn}) \in Z_{pq}^n$ uniformly and randomly.

4. Let $\mathbb{D}_{m\times m}$ be the Gaussian distribution $(\mathbb{D}_{Z^m,\sigma_0})^m$, $H_1, H_2 : \{0,1\}^* \to \mathbb{D}_{m\times m}$, and $H_3 : \{0,1\}^* \to Z_p^n$ are three different hash functions.

5. Output $PP = (\{A_{i,b}\}_{i\in[l],b\in\{0,1\}}, \{u_t\}_{t\in[k]}, H_1, H_2, H_3)$ and $msk = (\{T_{i,b}\}_{i\in[l],b\in\{0,1\}})$.

• **uKeyExtract** (msk, id) On input $msk = (\{T_{i,b}\}_{i\in[l],b\in\{0,1\}})$ and an identity $id = (id_1, \cdots, id_l)$, the unsigncryption key uk_{id} is obtained as follows.

1. For $t \in [k]$, select a random polynomial vector $f_t \in \mathbb{R}^n$ of degree $d-1$ such that $\mathbb{R} = Z_{pq}[x]$ and $f_t(0) = u_t$. Let $u_{ti} = f_t(i) \in Z_{pq}^n$ for $i \in [l]$. By Shamir's (d,l) threshold scheme, for $I \subseteq [l]$ such that $|I| \ge d$, $u_t = \Sigma_{i\in I} L_i \cdot u_{ti} (\bmod pq)$, where L_i is the associated Lagrangian coefficient.

2. For $i \in [l]$, let $R_{i,id_i} = H_1(id_i \| i)$, invoke algorithm $BasisDel(A_{i,id_i}, R_{i,id_i}, T_{i,id_i}, \sigma)$ to get a short basis T_{i,id_i}' for lattice $\Lambda_{pq}^{\perp}(B_{i,id_i})$, where $B_{i,id_i} = A_{i,id_i} R_{i,id_i}^{-1}$.

3. For $t \in [k], i \in [l]$, run $SamplePre(B_{i,id_i}, T_{i,id_i}', u_{ti}, \sigma')$ to get $e_{ti} \in Z^m$ satisfying $B_{i,id_i} \cdot e_{ti} = u_{ti}$.

4. Output the unsigncryption key for the identity id as $\{e_{ti}\}_{t\in[k],i\in[l]}$.

• **sKeyExtract** (msk, id) On input $msk = (\{T_{i,b}\}_{i\in[l],b\in\{0,1\}})$ and an identity $id = (id_1, \cdots, id_l)$, the signature key sk_{id} is obtained as follows.

1. For $i \in [l]$, let $R_{id,id_i} = H_2(id \| id_i \| i)$, invoke algorithm $BasisDel(A_{i,id_i}, R_{id,id_i}, T_{i,id_i}, \sigma)$ to get a short basis T_{id,id_i}' for lattice $\Lambda_{pq}^{\perp}(B_{id,id_i})$, where $B_{id,id_i} = A_{i,id_i} R_{id,id_i}^{-1}$.

2. Output the signature key for the identity id as $\{T_{id,id_i}'\}_{i\in[l]}$.

• **Signcrypt** (M, sk_{id_s}, id_e) On input the message $M \in \{0,1\}^k$, the signature key $sk_{id_s} = \{T'_{id_s,id_{si}}\}_{i\in[l]}$ for id_s, and $id_e = (id_{e1}, \cdots, id_{el})$ used for encryption,

1. Let $D = (l!)^2, u = H_3(M)$.

2. Select a random polynomial vector $f \in \mathbb{A}^n$ of degree $d'-1$ such that $\mathbb{A} = Z_p[x]$ and $f(0) = u$. Let $u_j = f(j) \in Z_p^n$ for $j \in [l]$. By Shamir's (d', l) threshold scheme, for

$J \subseteq [l]$ such that $|J| \geq d'$, $u = \Sigma_{j \in J} L_j \cdot u_j \pmod{p}$, where L_j is the associated Lagrangian coefficient.

3. For $i \in [l]$, compute $R_{id_s, id_{si}} = H_2(id_s \| id_{si} \| i)$, $B_{id_s, id_{si}} = A_{i, id_{si}} R^{-1}_{id_s, id_{si}}$.

4. For $i \in [l]$, sample $e_i = SamplePre(B_{id_s, id_{si}}, T_{id_s, id_{si}}, qu_i, \sigma') \in \mathbb{Z}^m$.

5. Select $s \in \mathbb{Z}^n_{pq}$ randomly, compute $c = s + qu$.

6. For $t \in [k]$, let $c_{t0} = u_t^{\mathrm{T}} s + Dx_t + M_t \lfloor \frac{pq}{2} \rfloor$, where $x_t \leftarrow D_{\mathbb{Z}, \sigma'}$.

7. For $i \in [l]$, let $R_{i, id_{ei}} = H_1(id_{ei} \| i)$, $B_{i, id_{ei}} = A_{i, id_{ei}} R^{-1}_{i, id_{ei}}$.

8. For $i \in [l]$, let $c_i = B^{\mathrm{T}}_{i, id_{ei}} s + De_i$.

9. Output the ciphertext $C = (id_e, id_s, c, \{c_{t0}\}_{t \in [k]}, \{c_i\}_{i \in [l]})$.

• **Unsigncrypt** (C, uk_{id_u}, id_v) On input the ciphertext $C = (id_e, id_s, c, \{c_{t0}\}_{t \in [k]}, \{c_i\}_{i \in [l]})$, the unsigncryption key $uk_{id_u} = \{e_{ti}\}_{t \in [k], i \in [l]}$ for id_u, and $id_v = (id_{v1}, \cdots, id_{vl})$ used for verification,

1. Let $I = id_u \cap id_e$ denote the set of matching bits in id_u and id_e, and $J = id_v \cap id_s$ denote the set of matching bits in id_v and id_s. If $|I| < d$ or $|J| < d'$, output $\perp$ and reject. Otherwise, continue.

2. For $i \in [l]$, let $R_{i, id_{ui}} = H_1(id_{ui} \| i)$, $B_{i, id_{ui}} = A_{i, id_{ui}} R^{-1}_{i, id_{ui}}$. By Shamir's (d, l) threshold scheme, we have $\Sigma_{i \in I} L_i B_{i, id_{ui}} e_{ti} = u_t \pmod{pq}$ for $t \in [k]$.

3. For $t \in [k]$, compute $r_t = c_{t0} - \sum_{i \in I} L_i e^{\mathrm{T}}_{ti} c_i \pmod{pq}$. Let $r_t \in [-\lfloor \frac{pq}{2} \rfloor, \lfloor \frac{pq}{2} \rfloor) \subset \mathbb{Z}$. If $|r_t| < \frac{pq}{4}$, output $M_t = 0$, otherwise output $M_t = 1$. In this step, we retrieve the message M.

4. Compute $s = c - qH_3(M)$.

5. For $i \in [l]$, compute $R_{i, id_{ei}} = H_1(id_{ei} \| i)$, $B_{i, id_{ei}} = A_{i, id_{ei}} R^{-1}_{i, id_{ei}}$, and $e_i = D^{-1}(c_i - B^{\mathrm{T}}_{i, id_{ei}} s)$.

6. For $i \in [l]$, compute $R_{id_s, id_{si}} = H_2(id_s \| id_{si} \| i)$, $B_{id_s, id_{si}} = A_{i, id_{si}} R^{-1}_{id_s, id_{si}}$.

7. Verify whether $\Sigma_{j \in J} L_j B_{id_s, id_{sj}} e_j = qH_3(M)$ and $e_j \in D_n$ for $j \in [l]$. If all conditions hold, accept M as a valid message. Otherwise, output $\perp$ and reject.

5.2 Consistency of Construction 1

Let $I = id_u \cap id_e$ denote the set of matching bits in id_u and id_e, $J = id_v \cap id_s$ denote the set of matching bits in id_v and id_s, and $|I| \geq d$, $|J| \geq d'$. Then for $t = 1, \cdots, k$,

$r_t = c_{t0} - \sum_{i \in I} L_i e^{\mathrm{T}}_{ti} c_i \pmod{pq}$

$$= u_t^{\mathrm{T}} s + Dx_t + M_t \lfloor \frac{pq}{2} \rfloor - \sum_{i\in I} L_i e_{ti}^{\mathrm{T}} (B_{i,id_{ei}}^{\mathrm{T}} s + De_i) (\bmod pq)$$

$$= u_t^{\mathrm{T}} s + Dx_t + M_t \lfloor \frac{pq}{2} \rfloor - \sum_{i\in I} L_i e_{ti}^{\mathrm{T}} (B_{i,id_{ui}}^{\mathrm{T}} s + De_i) (\bmod pq)$$

$$= M_t \lfloor \frac{pq}{2} \rfloor + (u_t^{\mathrm{T}} s - \sum_{i\in I} (L_i B_{i,id_{ui}} e_{ti})^{\mathrm{T}} s) + (Dx_t - \sum_{i\in I} DL_i e_{ti}^{\mathrm{T}} e_i) (\bmod pq)$$

$$= M_t \lfloor \frac{pq}{2} \rfloor + (u_t^{\mathrm{T}} s - u_t^{\mathrm{T}} s) + (Dx_t - \sum_{i\in I} DL_i e_{ti}^{\mathrm{T}} e_i) (\bmod pq)$$

$$= M_t \lfloor \frac{pq}{2} \rfloor + (Dx_t - \sum_{i\in I} DL_i e_{ti}^{\mathrm{T}} e_i) (\bmod pq)$$

According to parameters setting in **Setup** of our scheme, $| Dx_t - \sum_{i\in I} DL_i e_{ti}^{\mathrm{T}} e_i | \le D | x_t | + \Sigma_{i\in I} D^2 | e_{ti}^{\mathrm{T}} e_i | < \frac{pq}{4}$ with overwhelming probability, then $M_t \lfloor \frac{pq}{2} \rfloor + (Dx_t - \sum_{i\in I} DL_i e_{ti}^{\mathrm{T}} e_i) (\bmod pq) \approx M_t \lfloor \frac{pq}{2} \rfloor$. Therefore, if $| r_t | < \frac{pq}{4}$, then $M_t = 0$; otherwise $M_t = 1$. And $M = (M_1, \cdots, M_k)$.

Then $s = c - qH_3(M)$ and $e_i = D^{-1}(c_i - B_{i,id_{ei}}^{\mathrm{T}} s)$ for $i \in [l]$. Because of $e_i = SamplePre(B_{id_s,id_{si}}, T_{id_s,id_{si}}, qu_i, \sigma')$ and $u = H_3(M) = \Sigma_{j\in J} L_j \cdot u_j (\bmod p)$, we have $\Sigma_{j\in J} L_j B_{id_s,id_{sj}} e_j = qH_3(M)$ and $e_j \in \mathrm{D}_n$ for $j \in [l]$.

As a result, as long as the ciphertext is got following our scheme religiously, a valid unsigncrypter can obtain the original message with overwhelming probability.

5.3 IND-sID-CPA security of Construction 1

Theorem 5.1 *Assuming that the LWE problem is hard, Construction 1 is indistinguishable against chosen plaintext attack under selective identity model (IND-sID-CPA).*

Proof. We prove Theorem 5.1 by contradiction. Suppose that there exists a PPT adversary A who can attack the IND-sID-CPA security of Construction 1, we can construct a challenger C to solve an LWE problem instance, which is a contradiction with the hardness of the LWE problem. In other words, Construction 1 is IND-sID-CPA secure under the hardness of the LWE problem.

To end this aim, the adversary A and the challenger C behave as follows.

- Target – The adversary A decides an encryption identity id^* to be his attack target, and returns id^* to the challenger C.
- Instance – The challenger C requests samples from the oracle O to get $(w_t, v_t) \in \mathrm{Z}_{pq}^n \times \mathrm{Z}_{pq}$ for $t = 1, \cdots, k$, and $\{(w_1^{(i)}, v_1^{(i)}), (w_2^{(i)}, v_2^{(i)}), \cdots, (w_m^{(i)}, v_m^{(i)})\} \in \{\mathrm{Z}_{pq}^n \times \mathrm{Z}_{pq}\}^m$ for $i \in [l]$. These samples follow LWE oracle O_s or uniform distribution oracle O_u, which will be decided by challenger C with the aid of A' attack ability to Construction 1.
- Setup – The public parameter PP is given by challenger C in the following manner.

1. Matrices $A_{i,id_i^*}' = \{(w_1^{(i)}), (w_2^{(i)}), \cdots, (w_m^{(i)})\}$ for $i \in [l]$.

2. Sample l random matrices $R_1^*, \cdots, R_l^* \leftarrow \mathcal{D}_{m\times m}$, and let $A_{i,id_i^*} = A_{i,id_i^*}' R_i^*$ for $i \in [l]$.

3. For $i \in [l]$, $A_{i,1-id_i^*}$ is obtained by algorithm $TrapGen$, together with a short basis $T_{i,1-id_i^*}$ for $\Lambda_{pq}^{\perp}(A_{i,1-id_i^*})$.

4. Vectors $u_t = w_t$ for $t \in [k]$.

Then $PP = (\{A_{i,b}\}_{i\in[l],b\in\{0,1\}}, \{u_t\}_{t\in[k]})$ is returned to the adversary $\mathcal{A}$.

• Phase 1 – In this phase, the adversary $\mathcal{A}$ has the right to ask the following queries with a number of polynomial bounded, and the challenger $\mathcal{C}$ must return reasonable answers.

◊ H_1 **queries** – The adversary $\mathcal{A}$ asks for $H_1(id)$ for an identity $id = (id_1, \cdots, id_l)$, and the challenger $\mathcal{C}$ answers as follows.

For $(id_i \| i)$, $i \in [l]$,

1. If $id_i = id_i^*$, let $H_1(id_i \| i) = R_i^*$.

2. If $id_i \neq id_i^*$, sample $R_{i,id_i} \leftarrow \mathcal{D}_{m\times m}$ randomly, let $H_1(id_i \| i) = R_{i,id_i}$.

Then save $(id, ((id_i \| i), H_1(id_i \| i))_{i\in[l]})$ in list $\mathcal{H}_1$ and return $((id_i \| i), H_1(id_i \| i))_{i\in[l]}$.

◊ H_2 **queries** – The adversary $\mathcal{A}$ asks for $H_2(id)$ for an identity $id = (id_1, \cdots, id_l)$, and the challenger $\mathcal{C}$ answers as follows.

For $(id \| id_i \| i)$, $i \in [l]$,

1. If $id_i = id_i^*$, run algorithm $SampleRwithBasis(A_{i,id_i^*})$ to obtain a random $R_{id,id_i} \leftarrow \mathcal{D}_{m\times m}$ and a short basis T_{id,id_i}' for lattice $\Lambda_{pq}^{\perp}(B_{id,id_i})$, where $B_{id,id_i} = A_{i,id_i^*} R_{id,id_i}^{-1}$. Let $H_2(id \| id_i \| i) = R_{id,id_i}$.

2. If $id_i \neq id_i^*$, sample $R_{id,id_i} \leftarrow \mathcal{D}_{m\times m}$ randomly, let $H_2(id \| id_i \| i) = R_{id,id_i}$, invoke algorithm $BasisDel(A_{i,id_i}, R_{id,id_i}, T_{i,id_i}, \sigma)$ to get a short basis T_{id,id_i}' for lattice $\Lambda_{pq}^{\perp}(B_{id,id_i})$, where $B_{id,id_i} = A_{i,id_i} R_{id,id_i}^{-1}$.

Then save $(id, ((id \| id_i \| i), R_{id,id_i}, B_{id,id_i}, T_{id,id_i}')_{i\in[l]})$ in list $\mathcal{H}_2$ and return $((id \| id_i \| i), R_{id,id_i})_{i\in[l]}$.

◊ **uKeyExtract queries** – The adversary $\mathcal{A}$ asks for the unsigncryption key for an identity id with $|id \cap id^*| = |I| = d_0 < d$. The challenger $\mathcal{C}$ does the following steps to reply.

1. For simplicity, we assume that the first d_0 bits of id and id^* are equal, then the challenger $\mathcal{C}$ has trapdoors for the matrices associated with the set $\overline{I}$, where $|\overline{I}| = l - d_0$.

2. For $t \in [k]$, let the shares of u_t be $u_{ti} = u_t + a_{t1} i + a_{t2} i^2 + \cdots + a_{td-1} i^{d-1}$, where $a_{t1}, \cdots, a_{td-1}$ are vector variables with length n.

3. For $i \in [l]$, execute $H_1(id)$ query to obtain $R_{i,id_i} = H_1(id_i \| i)$, and let $B_{i,id_i} = A_{i,id_i} R_{i,id_i}^{-1}$.

4. For $t \in [k]$, $i \in [d_0]$, select $e_{ti} \leftarrow D_{Z^m,\sigma'}$, and let $u_{ti} = B_{i,id_i} \cdot e_{ti}$.

5. For $t \in [k]$, $i \in \{d_0+1,\cdots,d-1\}$, choose $d-1-d_0$ shares $u_{td_0+1},\cdots,u_{td-1}$ randomly, then the values for $a_{t1},\cdots,a_{td-1}$ are fixed and all l shares $u_{t1},\cdots,u_{tl}$ are known.

6. For $t \in [k]$, $i \in \{d_0+1,\cdots,l\}$, since T_{i,id_i} is known, invoke algorithm $BasisDel(A_{i,id_i}, R_{i,id_i}, T_{i,id_i}, \sigma)$ to get a short basis T_{i,id_i}' for lattice $\Lambda_{pq}^{\perp}(B_{i,id_i})$, then invoke algorithm $SamplePre(B_{i,id_i}, T_{i,id_i}', u_{ti}, \sigma')$ to get $e_{ti} \in Z^m$ satisfying $B_{i,id_i} \cdot e_{ti} = u_{ti}$.

7. Return the unsigncryption key for the identity id as $\{e_{ti}\}_{t\in[k],i\in[l]}$.

◊ **sKeyExtract queries** – The adversary A asks for the signature key for an identity id. The challenger C executes $H_2(id)$ query to obtain $((id \| id_i \| i), R_{id,id_i}, B_{id,id_i}, T_{id,id_i}')_{i\in[l]}$, then returns $\{T_{id,id_i}'\}_{i\in[l]}$.

• Challenge – When Phase 1 ends, the adversary A selects two messages $M^{(0)}$ and $M^{(1)}$ with same length, and a signature identity id_s^*, sends all of them to the challenger C for challenge ciphertext. C selects $b \in \{0,1\}$ randomly, does the following steps.

1. Let $c_{t0} = Dv_t + M_t^{(b)} \lfloor \frac{pq}{2} \rfloor$ for $t \in [k]$.

2. Let $c_i = (Dv_1^{(i)}, Dv_2^{(i)}, \cdots, Dv_m^{(i)})$ for $i \in [l]$.

3. Select $c \in Z_{pq}^n$ randomly.

Then $(id^*, id_s^*, c, \{c_{t0}\}_{t\in[k]}, \{c_i\}_{i\in[l]})$ is returned.

• Phase 2 – The adversary A repeats what he did in Phase 1.

• Guess – The adversary A gives his guess b' for b which the challenger C used in Challenge phase. If $b' = b$, C decides the samples follow LWE oracle O_s; otherwise, C decides the samples follow uniform distribution oracle O_u.

5.4 Construction 2

We apply Fujisaki-Okamoto method to Construction 1 to obtain an IND-sID-CCA2 secure fuzzy identity-based signcryption scheme – Construction 2, which is illustrated as follows.

• **Setup** (n,d,d') On input security parameter $n = l^{\frac{1}{\varepsilon}}$, where l is the length of an identity, $\varepsilon \in (0,1)$ is a constant, and two thresholds d and d',

1. For $q = poly(n)$ and $pq \in [n^6 \cdot 2^{5l}, 2n^6 \cdot 2^{5l}]$, let $m = n^{1.5}$,
$\sigma_0 = O(\sqrt{n\log(pq)})\omega(\sqrt{\log m})$, $\sigma = O(n\log(pq))\sqrt{m}\omega(\log^2 m)$,
$\sigma' = O(\sqrt{n\log(pq)})m^{\frac{3}{2}}\omega(\log^{\frac{5}{2}} m)$, $D_n = \{e \in Z^m : \|e\| \le \sigma'\sqrt{m}\}$.

2. For $i \in [l], b \in \{0,1\}$, invoke algorithm $TrapGen(n)$ to obtain $(A_{i,b}, T_{i,b})$, with the

condition that

(a) $A_{i,b} \in Z_{pq}^{n\times m}$ follows uniform distribution with overwhelming probability.

(b) $T_{i,b}$ is a short basis of $\Lambda_{pq}^{\perp}(A_{i,b})$ and $\|T_{i,b}\| \le O(\sqrt{n\log(pq)})$.

3. Let (E,D) be a one-time secure symmetric encryption scheme, whose message space is $\mathrm{M}' = \{0,1\}^*$, key space is $\mathrm{K} = \{0,1\}^{k'}$.

4. Let $G:\{0,1\}^k \to \{0,1\}^{k'}$ and $H:\{0,1\}^* \to \{0,1\}^*$ be hash functions. For $t\in[k]$, select $u_t = (u_{t1},\cdots,u_{tn}) \in Z_{pq}^n$ uniformly and randomly.

5. Let $\mathrm{D}_{m\times m}$ be the Gaussian distribution $(\mathrm{D}_{Z^m,\sigma_0})^m$, $H_1, H_2 : \{0,1\}^* \to \mathrm{D}_{m\times m}$ and $H_3 : \{0,1\}^* \to Z_p^n$ are three different hash functions.

6. Output $PP = (\{A_{i,b}\}_{i\in[l],b\in\{0,1\}}, \{u_t\}_{t\in[k]}, G, H, H_1, H_2, H_3)$ and $msk = (\{T_{i,b}\}_{i\in[l],b\in\{0,1\}})$.

• **uKeyExtract** (msk, id) This algorithm is same as the **uKeyExtract** algorithm in Construction 1.

• **sKeyExtract** (msk, id) This algorithm is same as the **sKeyExtract** algorithm in Construction 1.

• **Signcrypt** (M, sk_{id_s}, id_e) On input the message $M\in\{0,1\}^*$, the signature key $sk_{id_s} = \{T'_{id_s,id_{si}}\}_{i\in[l]}$ for id_s, and $id_e = (id_{e1},\cdots,id_{el})$ used for encryption,

1. Select random $\rho\in\{0,1\}^k$, let $c_M = \mathrm{E}(G(\rho), M)$, $h = H(\rho, c_M)$.

2. Let $D = (l!)^2$, $u = H_3(M,\rho)$.

3. Using randomness h, execute Construction 1. **Signcrypt**. step 2 – step 5.

4. For $t\in[k]$, let $c_{t0} = u_t^{\mathrm{T}} s + Dx_t + \rho_t \lfloor \frac{pq}{2} \rfloor$, where $x_t \leftarrow \mathrm{D}_{Z,\sigma'}$.

5. For $i\in[l]$, let $R_{i,id_{ei}} = H_1(id_{ei} \Vert i)$, $B_{i,id_{ei}} = A_{i,id_{ei}} R_{i,id_{ei}}^{-1}$.

6. For $i\in[l]$, let $c_i = B_{i,id_{ei}}^{\mathrm{T}} s + De_i$.

7. Output the ciphertext $C = (id_e, id_s, c_M, c, \{c_{t0}\}_{t\in[k]}, \{c_i\}_{i\in[l]})$.

• **Unsigncrypt** (C, uk_{id_u}, id_v) On input the ciphertext $C = (id_e, id_s, c_M, c, \{c_{t0}\}_{t\in[k]}, \{c_i\}_{i\in[l]})$, the unsigncryption key $uk_{id_u} = \{e_{ti}\}_{t\in[k],i\in[l]}$ for id_u, and $id_v = (id_{v1},\cdots,id_{vl})$ used for verification,

1. Let $I = id_u \cap id_e$ denote the set of matching bits in id_u and id_e, and $J = id_v \cap id_s$ denote the set of matching bits in id_v and id_s. If $|I| < d$ or $|J| < d'$, output $\perp$ and reject. Otherwise, continue.

2. For $i\in[l]$, let $R_{i,id_{ui}} = H_1(id_{ui} \Vert i)$, $B_{i,id_{ui}} = A_{i,id_{ui}} R_{i,id_{ui}}^{-1}$. By Shamir's (d,l) threshold scheme, we have $\Sigma_{i\in I} L_i B_{i,id_{ui}} e_{ti} = u_t \pmod{pq}$ for $t\in[k]$.

3. For $t\in[k]$, compute $r_t = c_{t0} - \sum_{i\in I} L_i e_{ti}^{\mathrm{T}} c_i \pmod{pq}$. Let $r_t \in [-\lfloor \frac{pq}{2} \rfloor, \lfloor \frac{pq}{2} \rfloor) \subset Z$. If

$|r_t| < \frac{pq}{4}$, output $\rho_t = 0$, otherwise output $\rho_t = 1$. In this step, we retrieve ρ.

4. Let $M = \mathcal{D}(G(\rho), c_M)$ and $h = H(\rho, c_M)$.

5. Using randomness h, execute the above **Signcrypt**. step 3 – step 6 again. If $(c, \{c_{t0}\}_{t\in[k]}, \{c_i\}_{i\in[l]})$ obtained here is same as $(c, \{c_{t0}\}_{t\in[k]}, \{c_i\}_{i\in[l]})$ in the ciphertext, continue. Otherwise, reject and output $\perp$.

6. Compute $s = c - qH_3(M, \rho)$.

7. For $i \in [l]$, compute $R_{i,id_{ei}} = H_1(id_{ei} \| i)$, $B_{i,id_{ei}} = A_{i,id_{ei}} R^{-1}_{i,id_{ei}}$, and $e_i = D^{-1}(c_i - B^{\mathrm{T}}_{i,id_{ei}} s)$.

8. For $i \in [l]$, compute $R_{id_s, id_{si}} = H_2(id_s \| id_{si} \| i)$, $B_{id_s, id_{si}} = A_{i,id_{si}} R^{-1}_{id_s, id_{si}}$.

9. Verify whether $\Sigma_{j\in J} L_j B_{id_s, id_{sj}} e_j = qH_3(M, \rho)$ and $e_j \in \mathcal{D}_n$ for $j \in [l]$. If all conditions hold, accept M as a valid message. Otherwise, output $\perp$ and reject.

6. Security analysis of Construction 2

6.1 Ciphertext indistinguishability of Construction 2

Theorem 6.1 *Assuming that the LWE problem is hard, Construction 2 is indistinguishable against chosen ciphertext attack under selective identity model (IND-sID-CCA2).*

Proof. We prove Theorem 6.1 by contradiction. Suppose that there exists a PPT adversary $\mathcal{A}$ who can attack the IND-sID-CCA2 security of Construction 2, we can construct a challenger $\mathcal{C}$ to solve an LWE problem instance, which is a contradiction with the hardness of the LWE problem. In other words, Construction 2 is IND-sID-CCA2 secure under the hardness of the LWE problem.

To end this aim, the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ behave as follows.

• Target – The adversary $\mathcal{A}$ decides an encryption identity id^* to be his attack target, and returns id^* to the challenger $\mathcal{C}$.

• Instance – The challenger $\mathcal{C}$ requests samples from the oracle $\mathcal{O}$ to get $(w_t, v_t) \in \mathbb{Z}^n_{pq} \times \mathbb{Z}_{pq}$ for $t = 1, \cdots, k$, and $\{(w^{(i)}_1, v^{(i)}_1), (w^{(i)}_2, v^{(i)}_2), \cdots, (w^{(i)}_m, v^{(i)}_m)\} \in \{\mathbb{Z}^n_{pq} \times \mathbb{Z}_{pq}\}^m$ for $i \in [l]$. These samples follow LWE oracle $\mathcal{O}_s$ or uniform distribution oracle $\mathcal{O}_u$, which will be decided by challenger $\mathcal{C}$ with the aid of $\mathcal{A}$' attack ability to Construction 2.

• Setup – The public parameter PP is given by challenger $\mathcal{C}$ in the following manner.

1. Matrices $A_{i,id^*_i}{}' = \{(w^{(i)}_1), (w^{(i)}_2), \cdots, (w^{(i)}_m)\}$ for $i \in [l]$.

2. Sample l random matrices $R^*_1, \cdots, R^*_l \leftarrow \mathcal{D}_{m\times m}$, and let $A_{i,id^*_i} = A_{i,id^*_i}{}' R^*_i$ for $i \in [l]$.

3. For $i \in [l]$, $A_{i,1-id^*_i}$ is obtained by algorithm $TrapGen$, together with a short basis $T_{i,1-id^*_i}$ for $\Lambda^{\perp}_{pq}(A_{i,1-id^*_i})$.

4. Vectors $u_t = w_t$ for $t \in [k]$.

Then $PP = (\{A_{i,b}\}_{i\in[l],b\in\{0,1\}}, \{u_t\}_{t\in[k]})$ is returned to the adversary $\mathcal{A}$.

• Phase 1 – In this phase, the adversary $\mathcal{A}$ has the right to ask the following queries with a number of polynomial bounded, and the challenger $\mathcal{C}$ must return reasonable answers.

◊ H_1 **queries** – The adversary $\mathcal{A}$ asks for $H_1(id)$ for an identity $id = (id_1, \cdots, id_l)$, and the challenger $\mathcal{C}$ answers as follows.

For $(id_i \| i)$, $i \in [l]$,

1. If $id_i = id_i^*$, let $H_1(id_i \| i) = R_i^*$.

2. If $id_i \neq id_i^*$, sample $R_{i,id_i} \leftarrow \mathcal{D}_{m\times m}$ randomly, let $H_1(id_i \| i) = R_{i,id_i}$.

Then save $(id, ((id_i \| i), H_1(id_i \| i))_{i\in[l]})$ in list $\mathcal{H}_1$ and return $((id_i \| i), H_1(id_i \| i))_{i\in[l]}$.

◊ H_2 **queries** – The adversary $\mathcal{A}$ asks for $H_2(id)$ for an identity $id = (id_1, \cdots, id_l)$, and the challenger $\mathcal{C}$ answers as follows.

For $(id \| id_i \| i)$, $i \in [l]$,

1. If $id_i = id_i^*$, run algorithm $SampleRwithBasis(A_{i,id_i^*})$ to obtain a random $R_{id,id_i} \leftarrow \mathcal{D}_{m\times m}$ and a short basis T_{id,id_i}' for lattice $\Lambda_{pq}^{\perp}(B_{id,id_i})$, where $B_{id,id_i} = A_{i,id_i^*} R_{id,id_i}^{-1}$. Let $H_2(id \| id_i \| i) = R_{id,id_i}$.

2. If $id_i \neq id_i^*$, sample $R_{id,id_i} \leftarrow \mathcal{D}_{m\times m}$ randomly, let $H_2(id \| id_i \| i) = R_{id,id_i}$, invoke algorithm $BasisDel(A_{i,id_i}, R_{id,id_i}, T_{i,id_i}, \sigma)$ to get a short basis T_{id,id_i}' for lattice $\Lambda_{pq}^{\perp}(B_{id,id_i})$, where $B_{id,id_i} = A_{i,id_i} R_{id,id_i}^{-1}$.

Then save $(id, ((id \| id_i \| i), R_{id,id_i}, B_{id,id_i}, T_{id,id_i}')_{i\in[l]})$ in list $\mathcal{H}_2$ and return $((id \| id_i \| i), R_{id,id_i})_{i\in[l]}$.

◊ H_3 **queries** – The adversary $\mathcal{A}$ asks for $H_3(M, \rho)$ for some $M \in \{0,1\}^*$ and $\rho \in \{0,1\}^k$, the challenger $\mathcal{C}$ selects $h_{M,\rho} \in \mathbb{Z}_p^n$ uniformly and randomly, saves $(M, \rho, h_{M,\rho})$ in list $\mathcal{H}_3$ and returns $H_3(M, \rho) = h_{M,\rho}$.

◊ G **queries** – The adversary $\mathcal{A}$ asks for $G(\rho)$ for some $\rho \in \{0,1\}^k$, the challenger $\mathcal{C}$ selects $G_\rho \in \{0,1\}^{k'}$ uniformly and randomly, saves (ρ, G_ρ) in list $\mathcal{G}$ and returns $G(\rho) = G_\rho$.

◊ H **queries** –The adversary $\mathcal{A}$ asks for $H(\rho, c_M)$ for some $\rho \in \{0,1\}^k$ and $c_M \in \{0,1\}^*$, the challenger $\mathcal{C}$ selects $h_{\rho,c_M} \in \{0,1\}^*$ uniformly and randomly, saves $(\rho, c_M, h_{\rho,c_M})$ in list $\mathcal{H}$ and returns $H(\rho, c_M) = h_{\rho,c_M}$.

◊ **uKeyExtract queries** – The adversary $\mathcal{A}$ asks for the unsigncryption key for an identity id with $|id \cap id^*| = |I| = d_0 < d$. The challenger $\mathcal{C}$ does the following steps to reply.

1. For simplicity, we assume that the first d_0 bits of id and id^* are equal, then the challenger

$\mathcal{C}$ has trapdoors for the matrices associated with the set $\overline{I}$, where $|\overline{I}| = l - d_0$.

2. For $t \in [k]$, let the shares of u_t be $u_{ti} = u_t + a_{t1}i + a_{t2}i^2 + \cdots + a_{td-1}i^{d-1}$, where $a_{t1}, \cdots, a_{td-1}$ are vector variables with length n.

3. For $i \in [l]$, execute $H_1(id)$ query to obtain $R_{i,id_i} = H_1(id_i \| i)$, and let $B_{i,id_i} = A_{i,id_i} R_{i,id_i}^{-1}$.

4. For $t \in [k]$, $i \in [d_0]$, select $e_{ti} \leftarrow \mathcal{D}_{\mathbb{Z}^m, \sigma'}$, and let $u_{ti} = B_{i,id_i} \cdot e_{ti}$.

5. For $t \in [k]$, $i \in \{d_0 + 1, \cdots, d-1\}$, choose $d - 1 - d_0$ shares $u_{td_0+1}, \cdots, u_{td-1}$ randomly, then the values for $a_{t1}, \cdots, a_{td-1}$ are fixed and all l shares $u_{t1}, \cdots, u_{tl}$ are known.

6. For $t \in [k]$, $i \in \{d_0 + 1, \cdots, l\}$, since T_{i,id_i} is known, invoke algorithm $BasisDel(A_{i,id_i}, R_{i,id_i}, T_{i,id_i}, \sigma)$ to get a short basis T_{i,id_i}' for lattice $\Lambda_{pq}^{\perp}(B_{i,id_i})$, then invoke algorithm $SamplePre(B_{i,id_i}, T_{i,id_i}', u_{ti}, \sigma')$ to get $e_{ti} \in \mathbb{Z}^m$ satisfying $B_{i,id_i} \cdot e_{ti} = u_{ti}$.

7. Return the unsigncryption key for the identity id as $\{e_{ti}\}_{t\in[k], i\in[l]}$.

◊ **sKeyExtract queries** – The adversary $\mathcal{A}$ asks for the signature key for an identity id. The challenger $\mathcal{C}$ executes $H_2(id)$ query to obtain $((id \| id_i \| i), R_{id,id_i}, B_{id,id_i}, T_{id,id_i}')_{i\in[l]}$, then returns $\{T_{id,id_i}'\}_{i\in[l]}$.

◊ **Unsigncrypt queries** – The adversary $\mathcal{A}$ provides a ciphertext $C = (id_e, id_s, c_M, c, \{c_{t0}\}_{t\in[k]}, \{c_i\}_{i\in[l]})$, an identity id_u for unsigncryption, and an identity id_v for verification. $\mathcal{C}$ does the following steps to answer.

1. If $|id_u \cap id^*| < d$, compute uk_{id_u} = uKeyExtract (id_u), then invoke algorithm Unsigncrypt(C, uk_{id_u}, id_v) and return its result to $\mathcal{A}$.

2. If $|id_u \cap id^*| > d$, $|id_u \cap id_e| > d$ and $|id_v \cap id_s| > d'$, search lists $\mathcal{H}_3$, $\mathcal{G}$ and $\mathcal{H}$ to look for tuples $(M, \rho, h_{M,\rho})$, (ρ, G_ρ) and $(\rho, c_M, h_{\rho,c_M})$, such that

(1) $c_M = \mathcal{E}(G_\rho, M)$; (2) Let $s = c - qh_{M,\rho}$, and $e_i = D^{-1}(c_i - B_{i,id_{ei}}^{\mathrm{T}} s)$ for $i \in [l]$;

(3) $\Sigma_{j\in J} L_j B_{id_s, id_{sj}} e_j = qh_{M,\rho}$ and $e_j \in \mathcal{D}_n$ for $j \in [l]$.

If such tuples exist, return M. Otherwise, output $\perp$ and reject.

• Challenge – When Phase 1 ends, the adversary $\mathcal{A}$ selects two messages $M^{(0)}$ and $M^{(1)}$ with same length, and a signature identity id_s^*, sends all of them to the challenger $\mathcal{C}$ for challenge ciphertext. $\mathcal{C}$ selects $b \in \{0,1\}$ randomly, does the following steps.

1. Select random $\rho \in \{0,1\}^k$, let $c_M = \mathcal{E}(G(\rho), M_b)$.

2. Let $c_{t0} = Dv_t + \rho_t \lfloor \frac{pq}{2} \rfloor$ for $t \in [k]$.

3. Let $c_i = (Dv_1^{(i)}, Dv_2^{(i)}, \cdots, Dv_m^{(i)})$ for $i \in [l]$.

4. Select $c \in \mathbb{Z}_{pq}^n$ randomly.

Then $(id^*, id_s^*, c_M, c, \{c_{t0}\}_{t\in[k]}, \{c_i\}_{i\in[l]})$ is returned.

• Phase 2 – The adversary $\mathcal{A}$ repeats what he did in Phase 1, with the exception that he couldn't execute Unsigncrypt query on $(id_u, id_v, c_M, c, \{c_{t0}\}_{t\in[k]}, \{c_i\}_{i\in[l]})$ with $|id_u \cap id^*| \geq d$ and $|id_v \cap id_s^*| \geq d'$.

• Guess – The adversary $\mathcal{A}$ gives his guess b' for b which the challenger $\mathcal{C}$ used in Challenge phase. If $b' = b$, $\mathcal{C}$ decides the samples follow LWE oracle $\mathcal{O}_s$; otherwise, $\mathcal{C}$ decides the samples follow uniform distribution oracle $\mathcal{O}_u$.

6.2 Ciphertext unforgeability of Construction 2

Theorem 6.2 *Let $\beta = (l!)^3 \cdot \sigma' \cdot \sqrt{md'}$. If the $SIS_{n,2ml,q,\beta}$ problem is hard to solve, then Construction 2 is existentially unforgeable against chosen message attack under selective identity model. In other words, Construction 2 is EUF-sID-CMA secure under the hardness of the $SIS_{n,2ml,q,\beta}$ problem.*

Particularly, let $\mathcal{A}$ be a PPT adversary attacking EUF-sID-CMA security of Construction 2, then there exists a challenger $\mathcal{C}$ that can solve an $SIS_{n,2ml,q,\beta}$ problem instance.

Proof. Let $A = U_1 \| X_1 \| \cdots \| U_l \| X_l$, $U_i, X_i \in \mathbb{Z}_q^{n\times m}$. The challenger $\mathcal{C}$ will construct a non-zero short vector $e^{**} \in \mathbb{Z}^{2ml}$, such that $Ae^{**} = 0$ and $\left\|e^{**}\right\|_2 \leq \beta$.

To end this aim, the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ behave as follows.

• Target – The adversary $\mathcal{A}$ decides a signature identity id^* to be his attack target, and returns id^* to the challenger $\mathcal{C}$.

• Setup – The challenger $\mathcal{C}$ gives the public parameter PP in the following manner.

1. For $i \in [l]$, select $U_i', X_i' \in \mathbb{Z}_p^{n\times m}$ randomly. Use the Chinese remainder theorem to obtain $U_i'' \in \mathbb{Z}_{pq}^{n\times m}$, $X_i'' \in \mathbb{Z}_{pq}^{n\times m}$ such that $U_i'' = U_i (\bmod q)$, $U_i'' = U_{i'} (\bmod p)$, $X_i'' = X_i (\bmod q)$, $X_i'' = X_{i'} (\bmod p)$.

2. For $i \in [l]$, Sample $R_{i,0}^*, R_{i,1}^* \leftarrow \mathcal{D}_{m\times m}$, let $A_{i,0} = U_i'' R_{i,0}^*, A_{i,1} = X_i'' R_{i,1}^*$.

3. For $t \in [k]$, select $u_t = (u_{t1}, \cdots, u_{tn}) \in \mathbb{Z}_{pq}^n$ uniformly and randomly.

4. Return the public parameter $PP = (\{A_{i,b}\}_{i\in[l], b\in\{0,1\}}, \{u_t\}_{t\in[k]})$.

• Query – In this phase, the adversary $\mathcal{A}$ has the right to ask the following queries with a number of polynomial bounded, and the challenger $\mathcal{C}$ must return reasonable answers.

◊ H_1 **queries** – The adversary $\mathcal{A}$ asks for $H_1(id)$ for an identity $id = (id_1, \cdots, id_l)$, and the challenger $\mathcal{C}$ answers as follows.

1. For $id = (id_1, \cdots, id_l)$, $i \in [l]$, run algorithm *SampleRwithBasis*(A_{i,id_i}) to obtain a random $R_{i,id_i} \leftarrow \mathcal{D}_{m\times m}$ and a short basis T_{i,id_i}' for lattice $\Lambda_{pq}^{\perp}(B_{i,id_i})$, where $B_{i,id_i} = A_{i,id_i} R_{i,id_i}^{-1}$.

2. Save $(id, ((id_i \| i), R_{i,id_i}, B_{i,id_i}, T_{i,id_i}')_{i\in[l]})$ in list $\mathcal{H}_1$ and return $(H_1(id_i \| i) = R_{i,id_i})_{i\in[l]}$.

◊ H_2 **queries** – When $\mathcal{A}$ asks for $H_2(id)$ for an identity $id = (id_1, \cdots, id_l)$, the challenger

$\mathcal{C}$ performs as follows.

1. If $id = id^*$, for $i \in [l]$, when $id_i = 0$, let $H_2(id \| id_i \| i) = R^*_{i,0}$; when $id_i = 1$, let $H_2(id \| id_i \| i) = R^*_{i,1}$. Save $(id, (H_2(id \| id_i \| i), A_{i,id_i} \cdot H_2(id \| id_i \| i)^{-1}, \perp)_{i\in[l]})$ in list $\mathcal{H}_2$, and return $(H_2(id \| id_i \| i))_{i\in[l]}$.

2. If $id \neq id^*$, for $i \in [l]$, invoke algorithm *SampleRwithBasis*(A_{i,id_i}) to obtain R_{id,id_i} and a short basis T_{id,id_i}' for lattice $\Lambda^{\perp}_{pq}(B_{id,id_i})$, where $B_{id,id_i} = A_{i,id_i} R^{-1}_{id,id_i}$. Save $(id, (R_{id,id_i}, B_{id,id_i}, T_{id,id_i}')_{i\in[l]})$ in list $\mathcal{H}_2$, and return $(H_2(id \| id_i \| i) = R_{id,id_i})_{i\in[l]}$.

◊ **uKeyExtract queries** – The adversary $\mathcal{A}$ asks for the unsigncryption key of an identity $id = (id_1, \cdots, id_l)$, and the challenger $\mathcal{C}$ answers as follows.

1. For $t \in [k]$, select a random polynomial vector $f_t \in \mathcal{R}^n$ of degree $d-1$ such that $\mathcal{R} = \mathbb{Z}_{pq}[x]$ and $f_t(0) = u_t$. Let $u_{ti} = f_t(i) \in \mathbb{Z}^n_{pq}$ for $i \in [l]$. By Shamir's (d,l) threshold scheme, for $I \subseteq [l]$ such that $|I| \geq d$, $u_t = \Sigma_{i\in I} L_i \cdot u_{ti} (\bmod pq)$, where L_i is the associated Lagrangian coefficient.

2. Look for list $\mathcal{H}_1$ to get $(id, ((id_i \| i), R_{i,id_i}, B_{i,id_i}, T_{i,id_i}')_{i\in[l]})$. If the tuple doesn't exist, execute $H_1(id)$ query firstly.

3. For $t \in [k], i \in [l]$, run *SamplePre*$(B_{i,id_i}, T_{i,id_i}', u_{ti}, \sigma')$ to get $e_{ti} \in \mathbb{Z}^m$ satisfying $B_{i,id_i} \cdot e_{ti} = u_{ti}$.

4. Return $uk_{id} = \{e_{ti}\}_{t\in[k], i\in[l]}$.

◊ **sKeyExtract queries** – When $\mathcal{A}$ asks for the signature key of an identity $id = (id_1, \cdots, id_l)$, the challenger $\mathcal{C}$ performs as follows.

1. If $|id \cap id^*| \geq d'$, return $\perp$.

2. If $|id \cap id^*| < d'$, look for list $\mathcal{H}_2$ to obtain $(id, (R_{id,id_i}, B_{id,id_i}, T_{id,id_i}')_{i\in[l]})$, return $(T_{id,id_i}')_{i\in[l]}$. If id doesn't exist in list $\mathcal{H}_2$, execute $H_2(id)$ query firstly.

◊ **Signcrypt queries** – When $\mathcal{A}$ asks for the ciphertext associated with message M, the signature identity id_s, and the encryption identity id_e, the challenger $\mathcal{C}$ performs as follows.

1. Select random id' such that $|id_s \cap id'| \geq d'$, search list $\mathcal{H}_2$ to obtain $(id', (R_{id',id_{i'}}, B_{id',id_{i'}}, T_{id',id_{i'}}')_{i\in[l]})$. If id' doesn't exist in list $\mathcal{H}_2$, execute $H_2(id')$ query firstly.

2. Execute **Signcrypt**$(M, (T_{id',id_{i'}}')_{i\in[l]}, id_e)$ to obtain the ciphertext C and return it.

• Forge – The adversary $\mathcal{A}$ replies to the challenger $\mathcal{C}$ with a valid ciphertext C^* as well as an encryption identity id_e^*. Then $\mathcal{C}$ does the following steps to get a non-zero short vector $e^{**} \in \mathbb{Z}^{2ml}$, such that $Ae^{**} = 0$ and $\|e^{**}\|_2 \leq \beta$.

1. Look for list H_1 to get $(id_e^*,((id_{ei}^* \| i),R_{i,id_{ei}^*},B_{i,id_{ei}^*},T_{i,id_{ei}^*}')_{i\in[l]})$. If the tuple doesn't exist, execute $H_1(id_e^*)$ query firstly.
2. Execute **Unsigncrypt** $(C^*,(T_{i,id_{ei}^*}')_{i\in[l]},id^*)$ to obtain a signature $(M^*,\rho^*,(e_1^*,\cdots,e_l^*),id^*)$.
3. C^* is a valid ciphertext, so $(M^*,\rho^*,(e_1^*,\cdots,e_l^*),id^*)$ is valid, that is to say, for $i\in[l]$, $e_i^*\in \mathrm{D}_n$, and there is a subset $J\subseteq[l]$, $|J|=d'$, such that $\Sigma_{j\in J}L_j\cdot(A_{j,id_j^*}R_{j,id_j^*}^{*-1})\cdot e_j^* = qH_3(M^*,\rho^*)$.
4. Without loss of generality, suppose $J=\{1,2,\cdots,d'\}$. For $i\in[d']$, if $id_i^*=1$, $e_i^{**}=[0_{m\times 1};e_i^*]$; if $id_i^*=0$, $e_i^{**}=[e_i^*;0_{m\times1}]$.
5. Output $e^{**}=[D\cdot L_1e_1^{**};\cdots;D\cdot L_{d'}e_{d'}^{**};0;\cdots;0]$ as a solution to the $SIS_{n,2ml,q,\beta}$ problem.

The analysis is as follows.
1. $(M^*,\rho^*,(e_1^*,\cdots,e_l^*),id^*)$ is valid signature, so $e_i^*\in\mathrm{D}_n$, and
$(U_1 \| X_1 \| \cdots \| U_l \| X_l)\cdot[L_1e_1^{**};\cdots;L_{d'}e_{d'}^{**};0;\cdots;0]=0(\bmod q)$, namely,
$A\cdot[D\cdot L_1e_1^{**};\cdots;D\cdot L_{d'}e_{d'}^{**};0;\cdots;0]=0(\bmod q)$.
2. For $i\in[d']$, $\|e_i^{**}\|\le\sigma'\cdot\sqrt{m}$, and $|D\cdot L_i|\le(l!)^3$, then $\|e^{**}\|\le(l!)^3\cdot\sigma'\cdot\sqrt{md'}$.
3. The range of H_3 follows uniform distribution, the probability of $H_3(M,\rho)=0$ is negligible, so that the probability of $e^{**}=0$ is also negligible.

Consequently, e^{**} is a solution to the $SIS_{n,2ml,q,\beta}$ problem.

7. Efficiency analysis of the Construction 2

In this section, we analyze the efficiency of the Construction 2 and make a performance comparison among our construction and the other two primary lattice-based signcryption schemes[24,25]. The details are shown in **Table 1**.

Table 1. Performance comparison

Items	Schemes		
	Public key cryptosystem		Identity-based cryptosystem
	[24]	[25]	ours
(master) Public key sizes	$12n^3\log^3 q$	$6n^2\log^2 q$	$(2ln^{2.5}+n^2\log q)\log(pq)$
(master) Private key sizes	$72n^2\log^2 q\times \log(n\log q)$	$36n^2\log^2 q\times \log(n\log q)$	$2ln^3\log(n\log(pq))$
Ciphertext increments	$n(6n\log^2 q+1)\log q$	$6n\log^2 q+n$	$(1+\log q+ln^{0.5})n\log(pq)$
Signcryption cost	SP+ $n\log q$ (SD+MV) -SD	SP + MV	l (SP+MV)+ $n\log q$ SD

Unsigncryption cost	$(n\log q+2)$ MV	2 MV	l (SP+ $(2+\mathrm{n}\log q)$ MV) $+\mathrm{n}\log q$ SD
Confidentiality	IND-CCA2	IND-CCA2	IND-sID-CCA2
Confidentiality base	LWE	LWE	LWE
Unforgeability	SUF-CMA	SUF-CMA	EUF-sID-CMA
Unforgeability base	SIS	SIS	SIS
Model	RO	RO	RO
Identity fuzziness	N	N	Y

Note: public key size, private key size and ciphertext increments are denoted by number of bits; SP denotes *SamplePre* algorithm; SD denotes the algorithm of sampling from a discrete Gaussian distribution over lattice; MV denotes matrix vector multiplication; and RO denotes the scheme is proved in the random oracle model.

The data of the former two columns come from Ref. [26], and we analyze the data of the third column in details as follows.

The parameters $q=poly(n)$, $m=n^{1.5}$, and $pq\in[n^6\cdot 2^{5l},2n^6\cdot 2^{5l}]$, where l is the length of an identity. As in Ref. [26], we assume the length of the message is $\lceil n\log q\rceil$, which is denoted k in our scheme.

For master public key $(\{A_{i,b}\}_{i\in[l],b\in\{0,1\}},\{u_t\}_{t\in[k]})$, $A_{i,b}\in Z_{pq}^{n\times m}$, $u_t\in Z_{pq}^{n}$, so that the size is $2ln^{2.5}\log(pq)+n\log q\cdot n\log(pq)=(2ln^{2.5}+n^2\log q)\log(pq)$. For master private key $(\{T_{i,b}\}_{i\in[l],b\in\{0,1\}})$, $T\in Z^{m\times m}$ and $\|T_{i,b}\|\le O(n\log(pq))$, let $\|T_{i,b}\|=n\log(pq)$, then the size is $2l(n^{1.5})^2\log(n\log(pq))=2ln^3\log(n\log(pq))$. For ciphertext increments, we assume the symmetric encryption scheme (E,D) has no ciphertext increments, then the ciphertext increments include

$(c,\{c_{t0}\}_{t\in[k]},\{c_i\}_{i\in[l]})$, $c=s+qu\in Z_{pq}^{n}$,

$c_{t0}=u_t^{\mathrm{T}}s+Dx_t+\rho_t\lfloor\frac{pq}{2}\rfloor\in Z_{pq}$, $c_i=B_{i,id_{ei}}^{\mathrm{T}}s+De_i\in Z_{pq}^{m}$,

then the total increments are

$n\log(pq)+n\log q\cdot\log(pq)+ln^{1.5}\log(pq)=n\log(pq)\cdot(1+\log q+ln^{0.5})$.

For computation cost, we lose sight of the simple operations such as addition, single vector inner product, hash, symmetric encryption, etc., and merely think about the following three operations: matrix vector multiplication, MV; sampling from a discrete Gaussian distribution over lattice, SD; *SamplePre* algorithm, SP. Note there is operation of matrix reverse, we ignore it because it can be precomputed in our scheme.

Specific to signcryption cost, it is l (SP+MV)+ $\mathrm{n}\log q$ SD; specific to unsigncryption cost, it is l (SP+ $(2+\mathrm{n}\log q)$ MV)+ $\mathrm{n}\log q$ SD.

In conclusion, Ref. [24] and Ref. [25] belong to public key cryptosystems and our scheme belongs to identity-based cryptosystems, and due to our scheme's fuzziness property, we deal with messages bit by bit, therefore our scheme isn't as efficient as Refs. [24] and [25]. But our scheme has its own advantages as follows: it doesn't base on public key infrastructure; it has more flexible unsigncryption users structure; and comparing with signature-then-encrypt mode, it is more efficient.

8. Summary and conclusions

In this paper, we propose the first fuzzy identity-based signcryption scheme based on lattice assumptions. At first, we give a fuzzy identity-based signcryption scheme that has indistinguishability against chosen plaintext attack under selective identity model. Then we apply Fujisaki-Okamoto method to get a fuzzy identity-based signcryption scheme that has indistinguishability against adaptive chosen ciphertext attack under selective identity model. At last, we prove our scheme is existentially unforgeable against chosen message attack under selective identity model. As we know it, our scheme is the first fuzzy identity-based signcryption scheme that is secure even facing a quantum computer. However, our scheme is proved under the random oracle model, and it is valuable to build a fuzzy identity-based signcryption scheme from lattices under the standard model.

References

[1] A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” *Lecture Notes in Computer Science*, vol. 196, ch. 5, pp. 47–53, 1985. Article (CrossRef Link)

[2] B. Waters, “Efficient Identity-Based Encryption Without Random Oracles,” *Lecture Notes in Computer Science*, vol. 3494, ch. 7, pp. 114–127, 2005. Article (CrossRef Link)

[3] K. Paterson and J. N. Schuldt, “Efficient Identity-Based Signatures Secure in the Standard Model,” *Lecture Notes in Computer Science*, vol. 4058, ch. 18, pp. 207–222, 2006. Article (CrossRef Link)

[4] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” *Lecture Notes in Computer Science*, vol. 3494, ch. 27, pp. 457–473, 2005. Article (CrossRef Link)

[5] J. Baek, W. Susilo, and J. Zhou, “New constructions of fuzzy identity-based encryption,” *ASIACCS '07*, pp. 368--370, 2007. Article (CrossRef Link)

[6] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute-based systems,” *CCS '06* , pp. 99—112, 2006. Article (CrossRef Link)

[7] X. Li, B. Yang, and M. Zhang, “New construction of fuzzy identity-based encryption,” *Information Engineering, ICIE’09*, vol. 1, pp. 647–651, 2009. Article (CrossRef Link)

[8] P. Yang, Z. Cao, and X. Dong, “Fuzzy identity based signature,” *IACR Cryptology ePrint Archive*, vol. 2008, p. 10, 2008.

[9] 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)

[10] Q. Wu, “Fuzzy biometric identity-based signature in the standard model,” *Journal of Computational Information Systems*, vol. 8, no. 20, pp. 8405–8412, 2012.

[11] Y. Zheng, “Digital signcryption or how to achieve cost(signature + encryption) and cost(signature) + cost(encryption),” *Lecture Notes in Computer Science*, vol. 1294, ch. 11, pp. 165–179, 1997. Article (CrossRef Link)

[12] M. Zhang, B. Yang, T. Takagi, Y. Shen, and W. Zhang, “Fuzzy Biometric Signcryption Scheme with Bilinear Pairings in the Standard Model,” *Lecture Notes in Computer Science*, vol. 6122, ch. 10, pp. 77–87, 2010. Article (CrossRef Link)

[13] F. Li and M. K. Khan, “A biometric identity-based signcryption scheme,” *Future Generation Computer Systems*, vol. 28, no. 1, pp. 306–310, 2012. Article (CrossRef Link)

[14] 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, 1997. Article (CrossRef Link)

[15] C. Gentry, C. Peikert, and V. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” *STOC '08*, pp. 197–206, 2008. Article (CrossRef Link)

[16] S. Agrawal, D. Boneh, and X. Boyen, “Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE,” *Lecture Notes in Computer Science*, vol. 6223, ch. 6, pp. 98–115, 2010. Article (CrossRef Link)

[17] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, and H. Wee, “Functional Encryption for Threshold Functions (or Fuzzy IBE) from Lattices,” *Lecture Notes in Computer Science*, vol. 7293, ch. 17, pp. 280–297, 2012. Article (CrossRef Link)

[18] X. Boyen, “Lattice Mixing and Vanishing Trapdoors: A Framework for Fully Secure Short Signatures and More,” *Lecture Notes in Computer Science*, vol. 6056, ch. 29, pp. 499–517, 2010. Article (CrossRef Link)

[19] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, “Lattice Signatures and Bimodal Gaussians,” *Lecture Notes in Computer Science*, vol. 8042, ch. 3, pp. 40–56, 2013. Article (CrossRef Link)

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

[21] C. Gentry, S. Halevi, and V. Vaikuntanathan, “A Simple BGN-Type Cryptosystem from LWE,” *Lecture Notes in Computer Science*, vol. 6110, ch. 26, pp. 506–522, 2010. Article (CrossRef Link)

[22] E. Fujisaki and T. Okamoto, “Secure integration of asymmetric and symmetric encryption schemes,” *Journal of cryptology*, vol. 26, no. 1, pp. 80–101, 2013. Article (CrossRef Link)

[23] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” *J. ACM*, vol. 56, no. 6, pp. 1–40, 2009. Article (CrossRef Link)

[24] F. Wang, Y. Hu, and C. Wang, “Post-quantum secure hybrid signcryption from lattice assumption,” *Applied Mathematics & Information Sciences*, vol. 6, no. 1, pp. 23-28, 2012.

[25] F. Li, F. Muhaya, M. Khan, and T. Takagi, “Lattice-based signcryption,” *Concurrency and Computation: Practice and Experience*, vol. 25, no. 14, pp. 2112-2122, 2013. Article (CrossRef Link)

[26] X. Lu, Q. Wen, Z. Jin, L. Wang, and C. Yang, “A lattice-based signcryption scheme without random oracles,” *Frontiers of Computer Science*, vol. 8, no. 4, pp. 667-675, 2014. Article (CrossRef Link)

Xiuhua Lu received the B.S. degree in Mathematics and Applied Mathematics from Shandong Normal University, Jinan, Shandong, China, in 2002 and the M.S. degree in Applied Mathematics from Captical Normal University, Beijing, China, in 2005. Her research interests include public key cryptography, lattice cryptography, and provable security. She is currently a PhD candidate in Beijing University of Posts and Telecommunications and a lecturer in Langfang Teachers University.

Qiaoyan Wen received the B.S. and M.S. degrees in Mathematics from Shaanxi Normal University, Xi'an, Shaanxi, China, in 1981 and 1984, respectively, and the PhD degree in cryptography from Xidian University, Xi'an, Shaanxi, China, in 1997. Her present research interests include coding theory, cryptography, information security, Internet security, and applied mathematics. She is a professor in Beijing University of Posts and Telecommunications.

Wenmin Li received the B.S. and M.S. degrees in Mathematics and Applied Mathematics from Shaanxi Normal University, Xi'an, Shaanxi, China, in 2004 and 2007, respectively, and the Ph.D. degree in Cryptology from Beijing University of Posts and Telecommunications, Beijing, China, in 2012. She is currently a post-doctoral in Beijing University of Posts and Telecommunications, Beijing, China. Her research interests include cryptography and information security.

Licheng Wang received the B.S. degree from Northwest Normal University in 1995, the M.S. degree from Nanjing University in 2001, and the PhD degree from Shanghai Jiao Tong University in 2007. His current research interests include modern cryptography, network security, trust management, etc. He is an associate professor in Beijing University of Posts and Telecommunications.

Hua Zhang received the B.S. degree in telecommunications engineering from the Xidian University in 1998, the M.S. degree in cryptology from Xidian University in 2005, and the PhD degree in cryptology from Beijing University of Posts and Telecommunications in 2008. Now she is an associate professor in Beijing University of Posts and Telecommunications. Her research interests include cryptography, information security and network security.