Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/MBE

MBE, 17(6): 8105–8122.
DOI: 10.3934/mbe.2020411
Received: 05 August 2020
Accepted: 21 October 2020
Published: 12 November 2020

Research article

Novel efficient lattice-based IBE schemes with CPK for fog computing

Yanfeng Shi[1,*], Shuo Qiu[2], Jiqiang Liu[3] and Tinghuai Ma[4]

[1] School of Computer Engineering, Nanjing Institute of Technology, Nanjing 211167, China

[2] Jinling Institute of Technology, Nanjing 211169, China

[3] Beijing Jiaotong University, Beijing 100044, China

[4] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China

* **Correspondence:** Email: shiyf@njit.edu.cn.

Abstract: The data security of fog computing is a key problem for the Internet of things. Identity-based encryption (IBE) from lattices is extremely suitable for fog computing. It is able to not only simplify certificate management, but also resist quantum attacks. In this paper, firstly, we construct a novel efficient lattice-based IBE scheme with Combined Public Key (CPK) technique by keeping from consumptive trapdoor generation algorithm and preimage sampling algorithm, which is required by the existing lattice-based IBE schemes based on learning with errors (LWE). In addition, its key storage cost is lower and it is IND-ID-CPA secure in the random oracle model. Furthermore, based on this, an enhanced lattice-based IBE scheme with IND-ID-CCA security is developed by employing strong one-time signature. Our schemes only need $O(n^3/\log n)$ additions of vectors, while the existing schemes need at least $O(n^3)$ of additions and multiplications in Setup and Extract phase.

Keywords: fog computing; learning with errors; identity-based encryption; Combined Public Key

1. Introduction

Cloud computing is a mode of centralized processing of big data. Many cryptography technologies, such as homomorphic encryption [1], searchable encryption [2] and so on, have been widely applied in cloud computing [1]. Powered by the advent of the Internet of things, especially the increase of multimedia data [3–5], the constraints of cloud computing center load and transmission bandwidth become more and more prominent. As an emerging technology, fog computing could mitigate the serious burden on cloud-central process of the huge amount of IoT data [6, 7]. In fog computing, data security for distributed nodes is a significant problem [8–12]. Public Key Infrastructure (PKI), is

widely used in fog computing applications [13, 14]. However, the communication cost of certificate transmission and the computation cost of verifying CA signature is too high.

To deal with the shortcomings of certification management in traditional public key cryptosystems, Shamir proposed identity-based encryption (IBE) [15]. In identity based cryptosytstems, the sender is able to utilize the receiver's identification as the public key to encrypt messages. Thus, the receiver's public key certification is not need to be transmitted to the sender. Boneh et al., put forward the primary efficient IBE scheme based on bilinear maps [16]. IBE is greater suitable for fog computing scenarios, such as [17–20].

In what way, the emergence of quantum computers threatens the routine IBE primarily from traditional RSA or DLP prbolem. For this, lattice-based encryption, as the maximum crucial quantum-resistant cryptology is starting to catch on. Exceptionally, as Micciancio et al.'s affectation, even for quantum adversary, lattice problems are still hard [21]. Fortunately, even in terms of performance, the practical feasibility of lattice operations is proved in implementations.

The first IBE from a lattice problem is proposed by Gentry et al., which is IND-ID-CPA secure based upon learning with errors (LWE) assumption in the random oracle model [22]. Since then, more lattice-based IBE solutions improved it in security or performance [23–28]. It' a pity that the present LWE-based IBE constructions don't seem to be efficient sufficient. Mainly in Setup and Extract phase, it costs too much for trapdoor generation algorithm and preimage sampling algorithm. For this reason, Micciancio et al., presented more efficient trapdoor generation algorithm and preimage sampling algorithm [29]. Furthermore, Ye et al., developed them in performance by means of the implicit extension technique [27] and they are the most efficient algorithms so far. Unfortunately, their solutions can be nonetheless not practical sufficient since they still would like $O(n^3)$ times of multiplication and addition.

Our contributions: There are three main contributions in this paper:

(1) Firstly, we present a variant of LWE assumption, as Twins-Decision-LWE (TDLWE) assumption, and show that it is equivalent to Decision-LWE (DLWE) assumption.

(2) Secondly, based on TDLWE assumption, we construct a novel more practical lattice-based IBE. Our main idea is to utilize Combined Public Key (CPK) technique to keep off the expensive trapdoor generation and preimage sampling algorithm. So it solely desires $O(n^3/\log n)$ additions of vectors in Setup and Extract phase, which are even parallelizable. In addition, in our scheme, Public Key Generator (PKG) solely needs to store little-scale key "seeds" instead of large-scale keys.Our scheme can be shown its IND-ID-CPA security based on TDLWE assumption in the random oracle model. Of course, for balance, the size of public system parameters is larger.

(3) Furthermore, based on this basic scheme, we develop it to an enhanced lattice-based IBE scheme with its IND-ID-CCA security.

2. Preliminaries

2.1. Identity-based encryption (IBE)

Identity-based encryption (IBE) is consisted of following algorithms:

Setup: Private key Generator (PKG) initializes the public system parameters denoted via *PP*, alone with a master secret key. *PP* is public whereas solely PKG is aware of the master secret key.

Extract: Taking the identity $< ID_i >$ of a user, PKG extracts the private key for $< ID_i >$ with the master secret key.

Encrypt: Taking the public system parameters PP and an identity $< ID_i >$ as input, the sender encrypts messages for $< ID_i >$.

Decrypt: Taking the public system parameters PP and the private key as input, the receiver decrypts the ciphertext.

The IND-ID-CPA security model for IBE can be defined as an interactive game played by an adversary and a challenger. [30]

Setup: Given a security parameter n as input, the challenger runs Setup(1^n) and sends the result public system parameters PP to the adversary. Meanwhile, it keeps the master secret key.

Phase 1: Momentarily, the adversary could send the private key queries $< ID_i >$ for $i = 1, 2, ...l$. Then the challenger runs Extract to get the corresponding private key for the queries.

Challenge: Firstly, the adversary outputs a target identity ID^* which was not queried for the private key in Phase 1. Secondly, it outputs two equal-length messages-M_0 and M_1. Thirdly, the challenger picks a random bit $\sigma \in \{0, 1\}$, computes $C = Encrypt(PP, ID, M_\sigma)$, and sends C as the challenge to the adversary.

Phase 2: The adversary continues to make more private key queries as in Phase 1, on condition that the target identity ID^*'s private key can't be queried.

Guess: At last, the adversary returns a guess σ' of σ, and wins if $\sigma' = \sigma$.

We signify the advantage of that the adversary wins in attacking the IBE scheme as: $Pr^{adv} = |Pr[\sigma' = \sigma] - 1/2|$.

Definition 2.1. *(IND-ID-CPA secure). An IBE scheme is (k, ε)-semantically secure against IND-ID-CPA if all probabilistic polynomial time (PPT) adversaries making at most k private key queries have at most ε advantage in breaking the scheme [16].*

The IND-ID-CCA game played by an adversary and a challenger is similar to IND-ID-CPA game, except that in both Phase 1 and Phase 2, the adversary can not only query private key extraction queries, but also make ciphertext queries $< ID_i, C_i >$. When receiving a ciphertext query, the challenger answers with the corresponding plaintext.

Definition 2.2. *(IND-ID-CCA Secure). An IBE scheme is (k, ε)-semantically secure against IND-ID-CCA if all probabilistic polynomial time (PPT) adversaries making at most k private key queries have at most ε advantage in breaking the scheme [16].*

2.2. Combined public key

In 2004, Nan et al., presented a novel key management technology called Combined Public Key (CPK) to improve efficiency and save storage space. After that, CPK is employed in a variety of different applications [31, 32].

The basic idea for CPK is as follows [33]: Suppose that there're two matrixes-a public key matrix $(y_1, y_2, ..., y_{n'})$ together with the corresponding private key matrix $(x_1, ..., x_{n'})$, where $y_i = f(x_i)$, and a collision-resistance hash function $h(\cdot) : \{0,1\}^* \to \{0,1\}^{n'}$. That's to mention, if the identity of a user is id, his/her public key is $y_{id} = \sum_{i=1}^{n'} y_i h_i$ and private key is $x_{id} = \sum_{i=1}^{n'} h_i x_i$, where $y_{id} = f(x_{id})$ and $h(id) = h_1, ..., h_{n'}$.

2.3. Lattices

The formal definition for n-dimensional lattice of rank m is:

$\Lambda = L(B) = \{y \in \mathbb{R}^n \ s.t. \exists s \in \mathbb{Z}^m, y = Bs = \sum_{i=1}^{m} s_i b_i\}$, where $b_1, ..., b_m$ are $m(\leq n)$ linearly independent vectors, called basic vectors.

Distinctly, L is included in $\mathbb{Z}^m$. The special lattice $\mathbb{Z}^m$ is principally used in this paper [22].

2.4. Statistically distance

It is defined that two random variables X and Y in a finite set Ω are statistically close if the statistical distance

$\Delta(X; Y) = \frac{1}{2} \sum_{t \in \Omega} |Pr[X = t] - Pr[Y = t]|$

is a negligible function of λ [23].

2.5. Discrete gaussians distribution

Assuming that for a subset L of $\mathbb{Z}^m$, a positive parameter $r \in \mathbb{R}$ and a vector c, a Gaussian-shaped function on $\mathbb{R}^m$ is defined as:

$\rho_{r,c}(x) = exp(-\pi \frac{\|x-c\|^2}{r^2})$, where $\| \cdot \|$ is an representation of Euclidean l_2 norm. It is with mean 0 and variance r^2;

The sum of $\rho_{r,c}$ on L can be defined as $\rho_{r,c}(L) = \sum_{x \in L} \rho_{r,c}(x)$.

Then, the discrete Gaussian distribution on L can be described as:

$\forall \tilde{x} \in L$, $D_{L,r,c}(\tilde{x}) = \frac{\rho_{r,c}(\tilde{x})}{\rho_{r,c}(L)}$.

In this paper, we are going to utilize a special case of discrete Gaussian distribution $D_{\mathbb{Z}^m,r}$, that is, $L = \mathbb{Z}^m$ and $c = 0$.

In [22], there is a sampling algorithm-SampleD shown as follows: Given a certain n-dimensional basis $B \in \mathbb{Z}^{n \times m}$, with a mean $c \in \mathbb{R}^n$ and an adequate large Gaussian parameter r, get samples from $D_{L(B),r,c}$.

In our constructions, we utilize SampleD to sample random values from $D_{\mathbb{Z}^m,r}$ [22].

2.6. DLWE assumption

In this paper, our schemes are constructed from a variant of decision learning with errors (DLWE) assumption, equivalent to the standard LWE assumption [34]. Here, we tend to introduce DLWE problem.

Definition 2.3. *(Distribution $\bar{\Psi}_\alpha$). Take into account a prime q and a real parameter $\alpha = \alpha(n) \in (0, 1)$. $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ represents the group of reals $[0, 1)$ with mod 1 addition. $\lfloor x \rceil = \lfloor x + 1/2 \rfloor (x \in \mathbb{R})$ is denoted as a nearest integer to x. Ψ_α represents a distribution over $\mathbb{T}$ of a normal variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$ then reduced modulo 1. $\bar{\Psi}_\alpha$ represents the discrete distribution over $\mathbb{Z}_q$ of the random variable $\lfloor qX \rceil$ mod q, where variable $X \in \mathbb{T}$ is selected randomly from distribution Ψ_α [23].*

For convenience, $\bar{\Psi}_\alpha$ is denoted by χ_α or χ.

We tend to redescribe the definition of DLWE problem as follows according to [34–36].

Definition 2.4. *(Decision $-$ $LWE_{q,\alpha}(DLWE_{q,\alpha})$ problem).(All operations are performed in $\mathbb{Z}_q$.) Take into account a positive integer n, a large prime modulus $q \leq poly(n)$, an arbitrary integer $m \leq poly(n)$, together with a distribution $\bar{\Psi}_\alpha(\chi)$ over $\mathbb{Z}_q$, all public. The challenger independently and uniformly selects a matrix $A \in \mathbb{Z}_q^{n\times m}$, a secret vector $s \in \mathbb{Z}_q^n$, and a bit $\tau \in \{0, 1\}$. If $\tau = 1$, it returns $(A, A^T s + x) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$, where $x \in \chi^m$; Else, it returns $(A, d) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$, where $d \in Z^m$ is chosen randomly. Given a tuple, the adversary returns a guess τ' of τ.*

We define the adversary's advantage in solving $DLWE_{q,\alpha}$ problem as [34]

$$Pr^{adv}(DLWE_{q,\alpha}) = |Pr[\tau' = \tau] - \frac{1}{2}|$$

If the advantage in solving $DLWE_{q,\alpha}$ problem for any PPT adversary is negligible, we say that $DLWE_{q,\alpha}$ assumption holds.

For the certain noise distributions χ ($\bar{\Psi}_\alpha$) and a prime q, where $\alpha \cdot q > 2\sqrt{n}$, Even for quantum PPT adversary, $DLWE_{q,\alpha}$ problem is still hard [34]. That's to say, $DLWE_{q,\alpha}$ assumption holds.

Theorem 2.1. *For a prime number q, a positive integer n, and $m \geq 2n \lg q$, the distribution for $u = Ae$ mod q is statistically close to uniform distribution over $\mathbb{Z}^n$, where $e \leftarrow D_{\mathbb{Z}^m,r}$, for any $r \geq \omega(\sqrt{\log m})$ and all but a $2q^{-n}$ fraction of all $A \in \mathbb{Z}_q^{n\times m}$. Notice that $\omega(\cdot)$ is a function: if $g(n) = \omega(f(n))$, increment speed of $g(n)$ is faster than any $cf(n)(c > 1)$ [21].*

3. TDLWE assumption

It is shown that for certain parameters α and q, $DLWE_{q,\alpha}$ assumption holds. Based on it, we propose a variant of $DLWE_{q,\alpha}$ problem and exhibit that it's equivalent to $DLWE_{q,\alpha}$ problem.

Definition 3.1. *(Twins $-$ Decision $-$ $LWE_{q,m,n,r,\alpha}$ ($TDLWE_{q,m,n,r,\alpha}$) problem). (All operations are performed in $\mathbb{Z}_q$.)Take into consideration a positive integer n, a large prime modulus $q \leq poly(n)$, a arbitrary integer $m \leq poly(n)$, and a distribution $\bar{\Psi}_\alpha(\chi)$ over $\mathbb{Z}_q$, all public. Firstly, the challenger selects a matrix $A \in \mathbb{Z}_q^{n\times m}$, a vector e' from discrete Gaussian distribution $D_{\mathbb{Z}^m,r}$, together with a secret vector $s' \in \mathbb{Z}_q^n$ at random. Next, the challenger alternatives a bit $\tau \in \{0, 1\}$ independently and uniformly. If $\tau = 1$, it returns $(A, Ae', A^T s' + x', e'^T A^T s' + x) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n \times \mathbb{Z}_q^m \times \mathbb{Z}_q$, where $x' \in \chi^m$ and $x \in \chi$; Else, it returns $(A, Ae', A^T s' + x', d) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n \times \mathbb{Z}_q^m \times \mathbb{Z}_q$, where $x' \in \chi^m$ and d is selected from $\mathbb{Z}_q$ at random. At last, the adversary returns a guess τ' of τ.*

We define the adversary's advantage in solving $TDLWE_{q,m,n,r,\alpha}$ as

$$Pr^{adv}(TDLWE_{q,m,n,r,\alpha}) = |Pr[\tau' = \tau] - \frac{1}{2}|$$

.

If $Pr^{adv}(TDLWE_{q,m,n,r,\alpha})$ is negligible for any PPT adversary, we say that $TDLWE_{q,m,n,r,\alpha}$ assumption holds.

We tend to analyze the relationship between $DLWE_{q,\alpha}$ assumption and $TDLWE_{q,m,n,r,\alpha}$ assumption. Firstly, the parameters m, n, q, r, α are adjusted to satisfy: (1) $DLWE_{q,\alpha}$ assumption holds. (2) For $e' \leftarrow D_{\mathbb{Z}^m,r}$, Ae' is statistically close to uniform over $\mathbb{Z}_q^n$.

Theorem 3.1. *For some m, n, q, r, α, satisfying $m \geq 2n \lg q$ and $r \geq \omega(\sqrt{\log m})$, $TDLWE_{q,m,n,r,\alpha}$ assumption holds if $DLWE_{q,\alpha}$ assumption holds.*

Proof. For some parameters $m \geq 2n \lg q$ and $r \geq \omega(\sqrt{\log m})$, as known in Theorem 2.1, Ae' is statistically close to uniform B. Thus, TDLWE assumption tuple $(A, Ae', A^T s' + x', e'^T A^T s' + x)$ can be replaced by $(A, B, A^T s' + x', B^T s' + x)$. In addition, if $DLWE_{q,\alpha}$ assumption holds, the tuple $(A, B, A^T s' + x', B^T s' + x)$ is equivalent to $(A, B, C, B^T s' + x)$, where C is randomly and uniformly selected from $\mathbb{Z}_q^m$. Since both A and C are independent from $(B, B^T s' + x)$, which is equivalent to DLWE assumption. Therefore, for certain parameters, $TDLWE_{q,m,n,r,\alpha}$ assumption holds if $DLWE_{q,\alpha}$ assumption holds. □

4. A novel efficient lattice-based IBE construction with CPK

We put forward TDLWE assumption-a variant of DLWE assumption, and then analyzed its reasonableness. In the subsequent part, we'll present a new efficient lattice-based IBE construction using CPK from TDLWE assumption.

4.1. Construction

Setup (1^λ) **£** Taking n as a security parameter, PKG sets q, m, r, α as described in Section 4.2. Then it arbitrarily chooses a common matrix $A \in \mathbb{Z}_q^{n \times m}$ randomly. Notice that all operations are performed over $\mathbb{Z}_q$. PKG selects n' secret vectors $e_i (i = 1, 2, ..., n')$ from the discrete Gaussian $D_{\mathbb{Z}^m,r}$ randomly.

Then PKG sets the master secret key as

$$E = (e_1, e_2, ..., e_{n'}),$$

and the corresponding public key as

$$U = (u_1, u_2, ..., u_{n'}), \text{ where } u_i = Ae_i.$$

Moreover, PKG opts for $H : \{0,1\}^* \rightarrow \{0,1\}^{n'}$ as a collision-resistance hash function.

Finally PKG makes $PP = (n', q, A, U, H)$ as the public system parameters.

Extract (PP, E, id) **£** Let h_i be the ith bit of $H(id)$, $i = 1, 2, ..., n'$.

PKG returns the private key as $e_{id} = \sum_{i=1}^{n'} h_i e_i$ for an identity id .

Encrypt (PP, id, b) **£** Given the public system parameters PP, the receiver's identification id, and a bit $b \in \{0, 1\}$, the sender works:

1). If it's the first time encrypting the bit b for id, set $u_{id} = \sum_{i=1}^{n'} h_i u_i = \sum_{i=1}^{n'} A h_i e_i = A e_{id} \in \mathbb{Z}_q^n$.

2). To encrypt $b \in \{0, 1\}$, select $s \leftarrow \mathbb{Z}_q^n$ at uniform and compute $p = A^T s + x \in \mathbb{Z}_q^m$, where $x \leftarrow \chi^m$. Finally, returns the ciphertext $C = (c_1, c_2) = (p, u_{id}^T s + \bar{x} + b\lfloor q/2 \rfloor) \in \mathbb{Z}_q^m \times \mathbb{Z}_q$, where $\bar{x} \leftarrow \chi$.

Decrypt (PP, e_{id}, C) **£** Given the public system parameters PP, the receiver's private key e_{id} and a ciphertext $C = (c_1, c_2)$, the receiver will do:

1). Calculate $b' = c_2 - e_{id}^T c_1 \in \mathbb{Z}_q$.

2). If b' is closer to 0 than to $\lfloor q/2 \rfloor$ modulo q, output 0; Else, output 1.

4.2. Parameters setting

Refer to Gentry et al.'s description for concerning parameters, we tend to set $r \geq \omega(\sqrt{\log m})$, $q \geq 5r\sqrt{n'}(m+1)$, $\alpha \leq 1/(r\sqrt{n'(m+1)}) \cdot \omega(\sqrt{\log n})$, $q \cdot \alpha > 2\sqrt{n}$, and $m \geq 2n \lg q$ [22]. In line with Theorem 2.1 and Theorem 3.1, on this condition: (1) The public keys u_{id}'s distribution is statistically close to uniform over $\mathbb{Z}_q^n$. (2) $TDLWE_{q,m,n,r,\alpha}$ assumption holds. (3) The ciphertext is decrypted properly with the receiver's private key. (It will be shown in Section 4.3)

4.3. Completeness

The correctness is similar to that in [22]. It is known that the linear combination of independent normal variables is still a normal variable, $e_{id} = \sum_{i=1}^{n'} h_i e_i$ is similarly chosen from $D_{\mathbb{Z}^m, r'}$, where $r' = \sqrt{\sum_{i=1}^{n'} h_i r^2} \leq \sqrt{n'} r \leq \frac{q}{5(m+1)}$.

Decrypt algorithm computes $c_2 - e_{id}^T c_1 = \bar{x} - e_{id}^T x + b\lfloor q/2 \rfloor = \bar{x} - e_{id}^T x + b\lfloor q/2 \rfloor$, then outputs b if $\bar{x} - e_{id}^T x$ is at distance at most $q/5$ from 0 [22]. $\bar{x} - e_{id}^T x$ can be represented as $x'^T \tilde{e}_{id} = x'^T \begin{pmatrix} 1 \\ -e_{id} \end{pmatrix}$, where $x' \leftarrow \chi^{m+1}$.

On the basis of the characteristic of Gaussian distribution, we get $\| \tilde{e}_{id} \| = \sqrt{1 + \| e_{id} \|^2} \leq \sqrt{1 + r'^2 m} \leq r'\sqrt{m+1}$(with overwhelming probability) [22]. Since $x' \sim \chi$, $x_i' = \lfloor q \cdot y_i \rceil \ mod\ q$, $\| x' - qy \| \leq \sqrt{(\frac{1}{2})^2 (m+1)} = \sqrt{m+1}/2$. With Cauchy-Schwarz inequality, we know that $|(x' - qy)^T \tilde{e}_{id}|$ is no more than $r'(m+1)/2 \leq \frac{q}{5(m+1)}(\frac{m+1}{2}) \leq q/10$ and $|x'^T \tilde{e}_{id}| \leq |(x' - qy)^T \tilde{e}_{id}| + q|y^T \tilde{e}_{id}|$.

$y^T \tilde{e}_{id}$ is a normal variable, with mean 0 and standard deviation $\| \tilde{e}_{id} \| \alpha \leq r'\sqrt{m+1}\alpha \leq \sqrt{n'}\sqrt{m+1}\alpha < 1/\omega(\sqrt{\log n})$. By the tail inequality on normal variables, we knows that the probability for $|y^T \tilde{e}_{id}| > 1/10$ is negligible.

Thus, $|x'^T \tilde{e}_{id}| \leq |(x' - qy)^T \tilde{e}_{id}| + q|y^T \tilde{e}_{id}| \leq q/10 + q/10 = q/5$, in other words, $\bar{x} - e_{id}^T x$ is at distance is no more than $q/5$ from 0 (mod q).

4.4. Multi-bit encryption

In common with [22, 23], It's able to reuse the same ephemeral encryption randomness s to encrypt more than one bits message. Assume that the same ephemeral $s \in \mathbb{Z}_q^n$ is used for encrypting a K-bit message, throughout, the overall ciphertext size is $(2m + 1 \times K = 2m + K)$ elements of $\mathbb{Z}_q$.

4.5. Efficiency analysis

This scheme is rather more efficient by means of keeping off complex trapdoor generation algorithm and preimage sampling algorithm. Specifically, in step with Section 4.2, we will set $q \approx n^3$ and $n' = O(n^3/\log n)$. In Setup phase, it just runs SampleD algorithm once to supply n' samples from $D_{\mathbb{Z}^m,r}$. Meanwhile, in [22,23,27], both the public system parameters and the master secret key must be created by complex trapdoor generation algorithm. Furthermore, in Extract phase of our new solution, for every id, it solely requries parallelizable $n'/2$ additions of vectors on the average, whereas in [22, 23], complex preimage sampling algorithm that is with projection and orthogonalization in time $O(m^2) * length(msk, H(id))$ is requried, and in [27], for each id, $O(n^3)$ times of addition and multiplication are needed.

Moreover, thanks to the low computing cost of keys, PKG only needs to storage little-scale key "seeds" instead of large-scale keys.

4.6. Security

As shown in Section 3, for certain parameters, $TDLWE_{q,m,n,r,\alpha}$ problem is hard. During the following part, it will prove the security for our scheme based on $TDLWE_{q,m,n,r,\alpha}$ problem.

Theorem 4.1. *If $\varepsilon(1 - 1/e - 2^{k-n'})/2 - TDLWE_{q,m,n,r,\alpha}$ assumption holds, our scheme is (k, ε)-semantically secure against IND-ID-CPA in the random oracle model.*

Proof. Assume that there is a probabilistic polynomial time (PPT) adversary $\mathfrak{A}$ in the IND-ID-CPA game. It makes not more than k queries and gets a minimum of advantage ε. If we're able to build a PPT simulator $\mathfrak{B}$,given $(A, B = Ae', C = A^T s' + x', Z)$ by the challenger in $TDLWE_{q,m,n,r,\alpha}$ game, playing the IND-ID-CPA game with $\mathfrak{A}$ and $TDLWE_{q,m,n,r,\alpha}$ game with the challenger, can get a minimum of advantage $\varepsilon(1 - 1/e - 2^{k-n'})/2$ to guess τ in $TDLWE_{q,m,n,r,\alpha}$ game, the proof is completed.

Suppose that:

In $TDLWE_{q,m,n,r,\alpha}$ game,

if $\tau = 1$, $Z = e'^T A^T s' + x$, where $x \in \chi_\alpha$;

if $\tau = 0$, $Z = d$, where $d \in \mathbb{Z}_q$ is uniformly selected at random.

Next, the IND-ID-CPA game will be introduced in detail. Based on it, the advantage of $\mathfrak{B}$ guessing τ will be exhibited.

Setup Firstly, $\mathfrak{B}$ selects n' vectors $v_1, v_2, ..., v_{n'}$ from $D_{\mathbb{Z}^m,r}$ severally. And then it selects k n'-dimensional binary vectors $V_i = (h_{1i}, h_{2i}, ..., h_{n'i})^T, i = 1, 2, ..., k$ at random, where each V_i is selected independently and uniformly.

Then $\mathfrak{B}$ selects one of tuples $(w_1, w_2, ..., w_{n'})$, $w_i \in \mathbb{Z}$, which satisfies as follows:

$$(w_1, w_2, ..., w_{n'}) \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1k} \\ h_{21} & h_{22} & \dots & h_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n'1} & h_{n'2} & \dots & h_{n'k} \end{pmatrix} = 0.$$

Then the simulator $\mathfrak{B}$ sets the public key as $U = (u_1, u_2, ..., u_{n'})$, where $u_i = w_i B + A v_i$. Here we have a tendency to guarantee $\sqrt{(\sum w_i)^2 + 1} r \leq \frac{q}{5(m+1)}$ in order that the distribution of e_i and e_{id} is as same as our IBE scheme above.

Clearly, the corresponding master secret key is $E = (e_1, e_2, ..., e_{n'})$ implicitly, where $e_i = w_i e' + v_i$.

Finally, $\mathfrak{B}$ sends the public system parameters (n', q, A, U, H) to the adversary $\mathfrak{A}$.

Phase 1:

Random oracle queries The adversary $\mathfrak{A}$ is permitted to query Random Oracle H to obtain the hash values. In the IND-ID-CPA game played by the adversary $\mathfrak{A}$ and the simulator $\mathfrak{B}$, $\mathfrak{B}$ could respond at most q_H times of random oracle queries for $\mathfrak{A}$.(Here we let q_H be the polynomial upper bound of H-query number.) $\mathfrak{B}$ chooses $V_H \in \{1, 2, ..., q_H\}$ so that $|V_H| = k$. While not loss of generality, suppose that the identity set for private key queries is a subset of the identity set for H-queries. To handle the queries, a list of $< ID_i, H(ID_i), \xi_i >$ is maintained by $\mathfrak{B}$, where ID_i is a user's identity and $\xi_i \in \{0, 1\}$ is set once the query is responded by $\mathfrak{B}$. We tend to use an initially empty H-list to represent a tuple list. When $< ID_i >$ is queried by $\mathfrak{A}$, $\mathfrak{B}$ will answer it in the following situations:

(1) If $< ID_i >$ is within the H-list before now, $H(ID_i)$ is returned by $\mathfrak{B}$ immediately.

(2) If $< ID_i >$ is the i'th newest H-query and $i' \in V_H$ is the i''th smallest element in V_H, $\mathfrak{B}$ sets $H(ID_i) = h_{1i''}...h_{n'i''}$ and $\xi_i = 1$; finally, $H(ID_i)$ is returned by $\mathfrak{B}$ and the tuple $< ID_i, H(ID_i), \xi_i >$ is recorded in H-list.

(3) If $< ID_i >$ is the i'th newest H-query and $i' \notin V_H$, it selects a binary string $h_{1j}h_{2j}...h_{n'j} \in \{0, 1\}^{n'}$ randomly, not listed in H-list yet. And it assigned $H(ID_i) = h_{1j}h_{2j}...h_{n'j}$ and $\xi_i = 0$. lastly, $H(ID_i)$ is returned by $\mathfrak{B}$ and the tuple $< ID_i, H(ID_i), \xi_i >$ is recorded in H-list.

Private key extraction queries $\mathfrak{A}$ is permitted to additionally query different private keys for $< ID_1 >, < ID_2 >, ..., < ID_l >$, where $l \leq k$. $\mathfrak{B}$ will answer it according to the following three cases for each query $< ID_i > (i = 1, 2, ..., l)$:

(1) If ID_i is already in H-list and $\xi_i = 1$, calculate $e_{ID_i} = \sum_{l=1}^{n'} h_{li} v_l$ and return e_{ID_i}, where h_{li} is the lth bit of the record value $H(ID_i)$.

The e_{ID_i} is valid as a result of $e_{ID_i} = \sum_{1}^{n'} h_{li} e_l = \sum_{l=1}^{n'} h_{li}(w_l e' + v_l) = e' \sum_{l=1}^{n'} h_{li} w_l + \sum_{l=1}^{n'} h_{li} v_l = \sum_{l=1}^{n'} h_{li} v_l$.

(2) If ID_i is already in H-list and $\xi_i \neq 1$, or ID_i is not in H-list and all of V_js (which are generated during Setup phase) have already been utilized for answering queries, the IND-ID-CPA game will be restarted by $\mathfrak{B}$. As it should be, in the rebooted game, $\mathfrak{B}$ must re-select the set $V_H \in \{1, 2, ..., q_H\}$. Nevertheless, it should be aware that the game can be restarted up to $C_{q_H}^k - 1$ times. If the number of restarts is over $C_{q_H}^k - 1$, $\mathfrak{B}$ will abort and output a random bit as τ' uniformly.

(3) If ID_i is not in H-list, firstly $\mathfrak{B}$ queries Random Oracle for $< ID_i >$. And then a new related

record in H-list is generated. If $\xi_i = 1$, $\mathfrak{B}$ calculates $e_{ID_i} = \sum_{l=1}^{n'} h_{li} v_l$; Otherwise, it executes similar to (2).

Challenge Firstly, the adversary $\mathfrak{A}$ selects a target identity ID^*, never queried in Phase 1. It sends $(ID^*, b_0 = 0, b_1 = 1)$ to the simulator $\mathfrak{B}$. Secondly, $\mathfrak{B}$ queries Random Oracle for ID^* to obtain the binary string $h_1^* h_2^* ... h_{n'}^* \in \{0,1\}^{n'}$. Check whether if the binary vector $V^* = (h_1^*, h_2^*, ..., h_{n'}^*)^T$ is a linear combination of $V_i (i = 1, 2, ..., k)$. If it is, $\mathfrak{B}$ aborts and returns an bit as τ' uniformly and randomly. Else, $\mathfrak{B}$ calculates $w = \sum_{i=1}^{n'} h_i^* w_i$, $v = \sum_{i=1}^{n'} h_i^* v_i$. and $u_{ID^*} = wB + Av = A(we' + v)$. After that, $\mathfrak{B}$ uniformly selects a bit $\sigma \in \{0,1\}$ randomly. Then $\mathfrak{B}$ sets $C^* = (c_1^*, c_2^*) = (C, wZ + v^T C + b_\sigma \lfloor \frac{q}{2} \rfloor)$, and sends it as a challenge to $\mathfrak{A}$.

Phase 2 $\mathfrak{A}$ keeps on making Random oracle queries and private key queries $< ID_{l+1} >, < ID_{l+2} >, ..., < ID_{\tilde{k}} >$, where $\tilde{k} \leq k$.

Notice that $< ID^* >$ can not be directly be queried by $\mathfrak{A}$. Also, $\mathfrak{B}$ responds the queries similar to that in Phase 1.

Guess $\mathfrak{A}$ returns the guess σ' of σ. If $\sigma' = \sigma$, the simulator $\mathfrak{B}$ outputs $\tau' = 1$; Else it outputs $\tau' = 0$.

We tend to give the analysis for security of our scheme above.

Firstly, we discuss when the event *abort* does not occur, how much advantage the simulator $\mathfrak{B}$ has. Then the probability *abort* occurs will be analyzed.

Claim 4.1. *Under the condition abort doesn't occur, $\mathfrak{B}$'s advantage is not less than $\frac{1}{2}\varepsilon$.*

Proof. (1) If $\tau = 1$, i.e. $Z = e'^T A^T s' + x$, then $C^* = (C, wZ + v^T C + b_\sigma \lfloor \frac{q}{2} \rfloor) = (A^T s' + x', [A(we' + v)]^T s' + b_\sigma \lfloor \frac{q}{2} \rfloor - wx - v^T x')$

Observe $c_2^* - (we' + v) c_1^* = [A(we' + v)]^T s' + b_\sigma \lfloor \frac{q}{2} \rfloor - wx - v^T x' - (we' + v)^T (A^T s' + x') = wx - we' x' + b_\sigma \lfloor \frac{q}{2} \rfloor$. Since $wx - we'x'$ is not more than $w(r(m+1)/2) \leq \sqrt{(\sum w_i)^2 + 1}(r(m+1)/2) \leq q/10$ away from $q/10$, which is similar to Section 4.3.

Thus, there's no difference between C^* and the real ciphertext of IBE scheme.

Suppose that $\mathfrak{A}$'s advantage of breaking our IBE scheme is ε, i.e.

$|Pr[\sigma = \sigma' | \tau = 1 \bigwedge \overline{abort}]| = \frac{1}{2} + \varepsilon$

(2) If $\tau = 0$, i.e.$Z = d$, C^* is a random element from $\mathbb{Z}_q$.

Thus, $|Pr[\sigma \neq \sigma' | \tau = 0 \bigwedge \overline{abort}]| = \frac{1}{2}$.

Consequently, the simulator $\mathfrak{B}$'s advantage is

$|Pr[\tau = \tau' | \overline{abort}] - \frac{1}{2}|$

$= |Pr[\tau = 1 \bigwedge \tau' = 1 | \overline{abort}] + Pr[\tau = 0 \bigwedge \tau' = 0 | \overline{abort}] - \frac{1}{2}|$

$= |Pr[\tau = 1 \bigwedge \sigma = \sigma' | \overline{abort}] + Pr[\tau = 0 \bigwedge \sigma \neq \sigma' | \overline{abort}] - \frac{1}{2}|$

$= |Pr[\sigma = \sigma' | \tau = 1 \bigwedge \overline{abort}] Pr[\tau = 1 | \overline{abort}] + Pr[\sigma \neq \sigma' | \tau = 0 \bigwedge \overline{abort}] Pr[\tau = 0 | \overline{abort}] - \frac{1}{2}|$

$\geq \frac{1}{2}(\varepsilon + \frac{1}{2}) + \frac{1}{2}\frac{1}{2} - \frac{1}{2}$

$= \frac{1}{2}\varepsilon$

□

However, the event *abort* perhaps occurs within the IND-ID-CPA game. Thus the probabilities of *abort* should be investigated. Clearly, $\mathfrak{B}$ may abort with two reasons: (1) In Phase 1 or Phase 2, $\mathfrak{B}$ restarts the game more than $C_{q_H}^k - 1$ times ; (2) In the Challenge phase, the binary vector $V^* = (V_1^*, ..., V_{n'}^*)^T$ is a linear combination of $V_i (i = 1, 2, ..., k)$.

Claim 4.2. *The probability that the simulator $\mathfrak{B}$ aborts due to reason (1) is not more than $\frac{1}{e}$.*

Proof. For our selected V_H, a private key query resulting in the IND-ID-CPA Game restarting is with the probability not more than $1 - \frac{1}{C_{q_H}^k}$. For convenience, let $t = \frac{1}{C_{q_H}^k}$. Since the simulator $\mathfrak{B}$ can restart not more than $1/t$ times, all of t choices of V_H giving rise to restarting is with the probability not more than $(1-t)^{1/t} \approx \frac{1}{e}$. Thus, that $\mathfrak{B}$ aborts due to reason(1) has the probability not more than $\frac{1}{e}$. □

Claim 4.3. *The probability that the simulator $\mathfrak{B}$ aborts for reason (2) is not more than $2^{k-n'}$.*

Proof. We construct a matrix $M_{n'k} = (V_1, V_2, ..., V_k)$ with the rank $k' \leq k$, where $k < n'$. Obviously, there are k' linearly independent rows of $M_{n'k}$. For convenience, here we assume the first k' rows of $M_{n'k}$ are linearly independent. $M_{k'k'}$ denotes as a matrix consisting of k' linearly independent vectors, and each vector is composed of k' linearly independent elements of V_i. Denote V_i' as the k'-dimensional vector composed of the first k' elements of V_i. Therefore, there are not more than $2^{k'}$ choices of $V^{*'}$ which may be a linear combination of combination of $V_i' (i = 1, 2, ..., k)$, where $2^{k'} \leq 2^k$. And because there are a total of $2^{n'}$ n'-dimensional binary vectors. For this reason, $\mathfrak{B}$ aborts due to reason(2) with the probability at most $\frac{2^k}{2^{n'}}$. □

Consequently, in combination with the above two claims, that the simulator $\mathfrak{B}$ aborts has the probability no more than $\frac{1}{e} + 2^{k-n'}$. That's to say, the PPT simulator's advantage in solving $TDLWE_{q,m,n,r,\alpha}$ problem is at least $\frac{\varepsilon}{2}(1 - \frac{1}{e} - 2^{k-n'})$. By now, Theorem 4.1 has been proved completely. □

5. An enhanced CCA-secure lattice-based IBE construction with CPK

On the basis of the above scheme, we utilize strong one-time signature to develop an enhanced IND-ID-CCA secure construction.

5.1. Strong one-time signature

Strong one-time signature is defined by the game played by an adversary $\mathfrak{A}$ and a challenger as follows:

Step 1: The challenger executes $G(1^k)$ and outputs (vk, sk), then sends 1^k and vk to $\mathfrak{A}$

Step 2:$\mathfrak{A}$ may do one of following steps:

(1) Output a pair(C^*, θ^*) and terminate.

(2) Send a signature query C to challenger. The challenger responses the $\theta = Sign_{sk}(C)$ to $\mathfrak{A}$.

With this knowledge, $\mathfrak{A}$ outputs(C^*, θ^*).

It is said that $\mathfrak{A}$ succeeds if $Vrify_{vk}(C^*, \theta^*) = 1$ when $(C^*, \theta^*) \neq (C, \theta)$.

Definition 5.1. *(Strong one-time signature):A signature scheme Sig is a strong one-time signature scheme if the probability that any PPT adversary $\mathfrak{A}$ succeeds in above game is negligible [37].*

5.2. Construction

Refer. [37], we construct our scheme.

Noted that in this construction, we suppose each $id \in \{0,1\}^{l'}$.(Then we can ensure $(id\|vk) = (id'\|vk')$ if and only if $id = id'$ and $vk = vk'$.)

Setup (1^λ) Same as in Section 4.1.

Extract (PP, E, id, vk) Assume that h_i is the ith bit of $H(id\|vk)$, $i = 1, 2, ..., n'$;

return $e_{id\|vk} = \sum_{i=1}^{n'} h_i e_i$.

Encrypt (PP, id, b) 1). Run $G(1^k)$ of Sig(a strong one-time signature scheme) and generate the signing key sk and the corresponding verification key vk.

2). Construct $u_{id\|vk} = \sum_{i=1}^{n'} h_i u_i = \sum_{i=1}^{n'} A h_i e_i = A e_{id\|vk} \in \mathbb{Z}_q^n$, where h_i is the ith bit of $H(id\|vk)$.

3). To encrypt $b \in \{0,1\}$, select $s \leftarrow \mathbb{Z}_q^n$ uniformly and compute $p = A^T s + x \in \mathbb{Z}_q^m$, where $x \leftarrow \chi^m$. We let $c_1 = p$, $c_2 = u_{id\|vk}^T s + \bar{x} + b\lfloor q/2 \rfloor$, where $\bar{x} \leftarrow \chi$. Let $C = (c_1, c_2) \in \mathbb{Z}_q^m \times \mathbb{Z}_q$.

4). Sign the C using $Sign_{sk}$, output the ciphertext $(vk, C, \theta = Sign_{sk}(C))$.

Decrypt (PP, id, vk, C, θ) Given public parameters PP, the identity id, and (vk, C, θ) as input, do:

1).If $Verify_{vk}(C, \theta) \neq 1$, abort.

2). Run Extract(PP, E, id, vk) and get $e_{id\|vk}$, compute $b' = c_2 - e_{id\|vk}^T c_1 \in \mathbb{Z}_q$.

Output 0 if b' is closer to 0 than to $\lfloor q/2 \rfloor$ modulo q; Otherwise output 1.

If the ciphertext is valid, the Decrypt algorithm is the same as our IND-ID-CPA secure construction. So this construction is also completeness.

5.3. Correctness and efficiency

The correctness and efficiency analysis are similar to Sections 4.3 and 4.5.

5.4. Multi-bit encryption

Multi-bit encryption scheme construction is as same as that of the basic scheme. We can reuse the randomness $s \in \mathbb{Z}_q^n$ throughout, then if a K-bit message is encrypted, the ciphertext size is $2m + K$ elements of $\mathbb{Z}_q$ addition to $len(vk) + len(\theta)$.

5.5. Security analysis

Theorem 5.1. *If $\varepsilon(1 - 2/e - 2^{k-n'} - \epsilon)/2 - TDLWE_{q,m,n,r,\alpha}$ assumption holds and $(G(1^k), Sign, Verify)$ is a strong one-time signature scheme, our scheme is (k, ε)-secure against IND-ID-CCA in the random oracle model.*

Proof. The proof of Theorem 5.1 is similar to Theorem 4.1. Assuming that there is a PPT adversary $\mathfrak{A}$ in the IND-ID-CCA game. It makes not more than k queries and gets a minimum of advantage ε. Based on this, if we're able to build a PPT simulator $\mathfrak{B}$, given $(A, B = Ae', C = A^T s' + x', Z)$ by the

challenger in $TDLWE_{q,m,n,r,\alpha}$ game, playing the IND-ID-CCA game with $\mathfrak{A}$ and $TDLWE_{q,m,n,r,\alpha}$ game with the challenger, can get a minimum of advantage $\varepsilon(1 - 2/e - 2^{k-n'} - \epsilon)/2$ to guess τ, then the theorem is completed.

Same as Theorem 4.1, the IND-ID-CCA game will be introduced in detail. Based on it, we exhibit the advantage of $\mathfrak{B}$ guessing τ.

Setup Same as in theorem 4.1.

Phase 1:

Random oracle queries Same as in theorem 4.1 except that we replace $< ID_i >$ with $< ID_i \| vk_i >$.

Private key extraction queries Same as in theorem 4.1 except that $\mathfrak{A}$ makes $l(l \leq k)$ different queries $< ID_i, vk_i >$ instead of $< ID_i >$.

Decryption queries For each decryption query $< ID_i, vk_i, C_i, \theta_i >$ issued by adversary $\mathfrak{A}$, $\mathfrak{B}$ answers as follows:

If $Verify_{vk_i}(C_i, \theta_i) \neq 1$, it responds with $\perp$. If $Verify_{vk_i}(C_i, \theta_i) = 1$,

(1) If $(ID_i \| vk_i)$ is already in H-list and $\xi_i = 1$, then $\mathfrak{B}$ computes $e_{ID_i \| vk_i}$, decrypts C_i using $e_{ID_i \| vk_i}$, and replies the answer to $\mathfrak{A}$.

(2) If $(ID_i \| vk_i)$ is already in H-list and $\xi_i = 0$, or $(ID_i \| vk_i)$ isn't in H-list and all of $V_j (1 \leq j \leq k)$s created in the Setup have been utilized, $\mathfrak{B}$ restarts the IND-ID-CCA game. Noted that $\mathfrak{B}$ must re-select the set V_H. Same as private key extraction queries phase, $\mathfrak{B}$ can restart the game up to $C_{q_H}^k - 1$ times. If the number of restarting exceeds $C_{q_H}^k - 1$, $\mathfrak{B}$ will abort and output a uniformly random bit as τ'.

(3) If $(ID_i \| vk_i)$ isn't in H-list, firstly $\mathfrak{B}$ queries Random Oracle for $< ID_i \| vk_i >$. And a new related record in H-list is generated. If $\xi_i = 1$, $\mathfrak{B}$ does the same as (1), else it executes similar to (2).

Challenge Firstly, the adversary $\mathfrak{A}$ selects a target identity $ID^* \in \{0,1\}^{l'}$, never queried for private key in Phase 1. Secondly, it sends $(ID^*, b_0 = 0, b_1 = 1)$ to $\mathfrak{B}$. $\mathfrak{B}$ runs $G(1^k)$ of the strong one-time signature scheme to produce the signing key sk^* and the corresponding verification key vk^*. Then it queries Random Oracle for $< ID^* \| vk^* >$ to obtain the binary string $h_1^* h_2^* ... h_{n'}^* \in \{0,1\}^{n'}$. If the binary vector $V^* = (h_1^*, h_2^*, ..., h_{n'}^*)^T$ is a linear combination of $V_i (i = 1, 2, ..., k)$, $\mathfrak{B}$ aborts and returns a bit as τ' uniformly at random; Else, $\mathfrak{B}$ calculates $w = \sum_{i=1}^{n'} h_i^* w_i$, $v = \sum_{i=1}^{n'} h_i^* v_i$ and $u_{ID^* \| vk^*} = wB + Av = A(we' + v)$. After that, $\mathfrak{B}$ uniformly selects a random bit $\sigma \in \{0,1\}$, and obtains $C^* = (c_1^*, c_2^*) = (C, wZ + v^T C + b_\sigma \lfloor \frac{q}{2} \rfloor)$.

Then, it signs (C^*) using sk^* and sends $(vk^*, C^*, \theta^* = Sign_{sk^*}(C^*))$ as the challenge to $\mathfrak{A}$.

Phase 2:

Random oracle queries Same as in Phase 1.

Private key extraction queries $\mathfrak{A}$ can continue to make queries $< ID_i, vk_i >$ where $i = l+1, ..., m'(m' \leq k)$.

Decryption queries For each decryption query $< ID_i, vk_i, C_i, \theta_i >$ ($\neq < ID^*, vk^*, C^*, \theta^* >$) issued by adversary $\mathfrak{A}$, $\mathfrak{B}$ answers as follows:

If $Verify_{vk_i}(C_i, \theta_i) \neq 1$, it responds with $\perp$. If $Verify_{vk_i}(C_i, \theta_i) = 1$ and $(ID_i||vk_i) = (ID^*||vk^*)$, $\mathbb{B}$ aborts and returns a random bit τ'. If $Verify_{vk_i}(C_i, \theta_i) = 1$ and $(ID_i||vk_i) \neq (ID^*||vk^*)$,

(1) If $(ID_i||vk_i)$ is already in H-list and $\xi_i = 1$, $\mathfrak{B}$ calculates $e_{ID_i||vk_i}$, decrypts C_i using $e_{ID_i||vk_i}$, and replies the answer to $\mathfrak{A}$.

(2) If $(ID_i||vk_i)$ is already in H-list and $\xi_i = 0$, or $(ID_i||vk_i)$ is not in H-list and all of $V_j (1 \leq j \leq k)$s (which are generated in the Setup) have already been utilized for answering queries, the IND-ID-CCA game will be restarted by the simulator $\mathfrak{B}$. Noted that $\mathfrak{B}$ must re-select V_H. Same as private key extraction queries phase, the game can be restarted up to $C_{q_H}^k - 1$ times. If the number of restarting is over $C_{q_H}^k - 1$, $\mathfrak{B}$ aborts and returns a random bit as τ' uniformly.

(3) If $(ID_i||vk_i)$ is not in H-list, firstly $\mathfrak{B}$ makes a Random Oracle query for $< ID_i||vk_i >$. And then a new related record is generated in H-list. If $\xi_i = 1$, $\mathfrak{B}$ does the same as (1), else it does the same as (2).

Guess Same as in theorem 4.1.

In the next part, the security of our enhanced scheme is analyzed as Theorem 4.1.

Firstly, same as Claim 4.1, we know that under the condition the event *abort* does not occur, $\mathfrak{B}$'s advantage in solving $TDLWE_{q,m,n,r,\alpha}$ problem is not less than $\frac{1}{2}\varepsilon$.

Next, we investigate the probabilities that abort occurs. Observed that, the simulator $\mathfrak{B}$ may abort in three situations:

(1) In phase 1 or Phase 2, private key extraction query may cause aborting if the times of restarting exceeds $C_{q_H}^k - 1$;

(2) In phase 1 or phase 2, decryption query may cause aborting if the times of restarting is over $C_{q_H}^k - 1$;

(3) In phase 1 or phase 2, decryption query may cause aborting if the adversary makes a query $< ID_i, vk_i, C_i, \theta_i >$ such that $(ID_i||vk_i) = (ID^*||vk^*)$ and $Verify_{vk_i}(C_i, \theta_i) = 1$;

(4) In challenge phase, the binary vector $V^* = (h_1^*, ..., h_{n'}^*)^T$ is a linear combination of $V_i (i = 1, 2, ..., k)$.

Same as Claim 4.2 and Claim 4.3, the probability that the simulator $\mathfrak{B}$ aborts due to reason (1) is not more than $\frac{1}{e}$ and aborts due to reason (4) is not more than $2^{k-n'}$.

Claim 5.1. *The simulator $\mathfrak{B}$ aborts for reason (2) with the probability not more than $\frac{1}{e}$.*

The proof is similar to that of Claim 4.2.

Claim 5.2. *The simulator $\mathfrak{B}$ aborts for reason (3) with probability not more than ϵ.*

Proof. Firstly, we show that in Phase 2, the probability that $\mathfrak{A}$ makes a query $(ID_i, vk_i, C_i, \theta_i)$ such that $(ID_i||vk_i) = (ID^*||vk^*)$ and $Verify_{vk_i}(C_i, \theta_i) = 1$ is negligible (ϵ). Suppose the adversary's target identity is $ID^*||vk^*$, and the target ciphertext is (vk^*, C^*, θ^*). Because for $ID \in \{0,1\}^{l'}$, $(ID_i||vk_i) = (ID^*||vk^*)$ if and if only $ID_i = ID^*$ and $vk_i = vk^*$. However, according to the definition of strong one-time signature, when $(C_i, \theta_i) \neq (C^*, \theta^*)$, the adversary can forge the valid ciphertext such that $Verify_{vk^*(vk_i)}(C_i, \theta_i) = 1$

Table 1. Property summary for lattice-based IBE constructions from LWE in the literature and our schemes. (n is the security parameter.)

Schemes	computation complexity	security properties	security assumptions
Scheme1	$O(n^3/\log n)$ additions of vectors(in parallel)	IND-ID-CPA	TDLWE
Scheme2	$O(n^3/\log n)$ additions of vectors(in parallel)	IND-ID-CCA	TDLWE
Gentry et al.'s scheme [22]	$O(n^4)$ additions and multipications	IND-ID-CPA	LWE
Agrawal et al.'s scheme [23]	$O(n^4)$ additions and multipications	IND-sID-CPA	LWE
Ye et al.'s scheme [27]	$O(n^3)$ additions and multipications	IND-sID-CPA	DLWE

with negligible probability ϵ. That's to say, the simulator $\mathfrak{B}$ aborts for reason (3) with probability not more than ϵ. □

Combining Claims 4.1–4.3, Claim 5.1 and 5.2, the advantage of $\mathfrak{B}$ is at least $\frac{\varepsilon}{2}(1-2^{k-n'}-\frac{2}{e}-\epsilon)$. We have proved Theorem 5.1 successfully. □

6. Comparisons

In sections 4.5 and 5.3, we evaluated the asymptotic complexities of Setup and Extract phase for our schemes. Here, we list the complexities, security properties and security assumptions for our schemes and related schemes in the literature in Table 1. Notice that all of the operations are over $\mathbb{Z}_q$. We denote our IND-ID-CPA secure solution as "Scheme1" and our IND-ID-CCA secure solution as "Scheme2".

As shown in Table1, n is the security parameter, $n' = O(n^3/\log n)$. In Setup phase, It just supplies n' samples from $D_{\mathbb{Z}^m,r}$. and in Extract phase, it solely requries $n'/2 = O(n^3/\log n)$ additions of vectors (which can be parallelizable) on the average. While in Gentry et al.'s or Agrawal et al.'s, they requires $O(n^4)$ additions and multiplications, and in Ye et al.'s, it needs $O(n^3)$ additions and multipications.

As we have analyzed, our schemes are much more practical than the existing lattice-based IBE constructions based on LWE(or its variant).

7. Conclusions

In this paper, for data security in fog computing, a novel efficient lattice-based IBE construction with CPK is proposed. It is shown IND-ID-CPA secure in the random oracle model under a variant of DLWE assumption-TDLWE assumption. Based on this, we developed an enhanced construction with strong one-time signature, and showed its IND-ID-CCA security in the random oracle model. Moreover, how to develop CPK to fit the ideal lattice constrution is still an open problem.

Acknowledgment

This work was supported by Natural science research projects of universities (19KJB520033), Beijing Key Laboratory (40184042), Scientific Research Foundation for Talented Scholars of Jinling Institute of Technology (JIT-B-201726), the Scientific Research Foundation of Nanjing Institute of Technology (YKJ201980), and the National Natural Science Foundation of China (No.U1736105).

Conflict of interests

The authors declare there is no conflict of interests.

References

1. M. Alloghani, M. M. Alani, D. Al-Jumeily, T. Baker, J. Mustafina, A. Hussain, et al., A systematic review on the status and progress of homomorphic encryption technologies, *J. Inf. Secur. Appl.*, **48** (2019), 102362.
2. B. A. Al-Maytami, P. Fan, A. J. Hussain, T. Baker, P. Liatsis, An efficient queries processing model based on multi broadcast searchable keywords encryption (mbske), *Ad Hoc Networks*, **98** (2020), 102028.
3. J. Lei, D. Li, Z. Pan, Z. Sun, S. Kwong, C. Hou, Fast intra prediction based on content property analysis for low complexity hevc-based screen content coding, *IEEE Trans. Broadcast.*, **63** (2017), 48–58.
4. Z. Pan, X. Yi, Y. Zhang, B. Jeon and S. Kwong, Efficient in-loop filtering based on enhanced deep convolutional neural networks for hevc, *IEEE Transactions on Image Processing*, **29** (2020), 5352–5366.
5. Z. Pan, X. Yi, Y. Zhang, H. Yuan, F. L. Wang, S. Kwong, Frame-level bit allocation optimization based on video content characteristics for hevc, *ACM Trans. Multimedia Comput. Commun. Appl.*, **16** (2020), 1–20.
6. P. Sun, B. Chen, S. Han, H. Shi, Z. Yang, X. Li, *An evolutionary task offloading schema for edge computing*, in International Conference on Big Data and Security, Springer, 2019.
7. Y. Tu, Q. Su, Y. Geng, *Enabling secure and efficient data sharing and integrity auditing for cloud-assisted industrial control system*, in International Conference on Big Data and Security, Springer, 2019.
8. S. AlHamed, M. AlRodhaan, Y. Tian, *Privacy preservation of future trajectory using dummy rotation algorithm in fog computing*, in International Conference on Big Data and Security, Springer, 2019.
9. Z. Lv, K. Huang, Y. Wang, R. Tao, G. Wu, J. Zhang, et al., *Distributed differential privacy protection system for personalized recommendation*, in International Conference on Big Data and Security, Springer, 2019.
10. T. Ma, Q. Liu, J. Cao, Y. Tian, A. Al-Dhelaan, M. Al-Rodhaan, Lgiem: Global and local node influence based community detection, *Future Gener. Comput. Syst.*, **105** (2020), 533–546.
11. Y. Tian, B. Song, M. Al Rodhaan, C. R. Huang, M. A. Al-Dhelaan, A. Al-Dhelaan, et al., A stochastic location privacy protection scheme for edge computing, *Math. Biosci. Eng.*, **17** (2020), 2636–2649.
12. W. Wang, W. Zhang, Z. Jin, K. Sun, R. Zou, C. Huang, et al., *A novel location privacy protection scheme with generative adversarial network*, in International Conference on Big Data and Security, Springer, 2019.

13. K. Gu, N. Wu, B. Yin, W. Jia, Secure data query framework for cloud and fog computing, *IEEE Trans. Network Serv. Manage.*, **17** (2019), 332–345.

14. S. Kunal, A. Saha, R. Amin, An overview of cloud-fog computing: Architectures, applications with security challenges, *Secur. Privacy*, **2** (2019), e72.

15. A. Shamir, *Identity-based cryptosystems and signature schemes*, in Workshop on the theory and application of cryptographic techniques, Springer, 1984.

16. D. Boneh, M. Franklin, *Identity-based encryption from the weil pairing*, in Annual international cryptology conference, Springer, 2001.

17. T. Baker, M. Asim, Á. MacDermott, F. Iqbal, F. Kamoun, B. Shah, et al., A secure fog-based platform for scada-based iot critical infrastructure, *Software Pract. Exp.*, **50** (2020), 503–518.

18. Y. Lian, X. Wei, *Lightweight identity authentication scheme based on ibc identity cryptograph*, in International Conference on Big Data and Security, Springer, 2019.

19. Y. Shi, S. Qiu, J. Liu, *An efficient lattice-based ibe scheme using combined public key*, in International Conference on Big Data and Security, Springer, 2019.

20. X. Wei, Y. Lian, *Research on identity-based cryptograph and its application in power iot*, in International Conference on Big Data and Security, Springer, 2019.

21. D. Micciancio, O. Regev, Worst-case to average-case reductions based on gaussian measures, *SIAM J. Comput.*, **37** (2007), 267–302.

22. C. Gentry, C. Peikert, V. Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions*, in Proceedings of the fortieth annual ACM symposium on Theory of computing, ACM, 2008.

23. S. Agrawal, D. Boneh, X. Boyen, *Efficient lattice (h) ibe in the standard model*, in Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2010.

24. P. Bert, P. A. Fouque, A. Roux-Langlois, M. Sabt, *Practical implementation of ring-sis/lwe based signature and ibe*, in International Conference on Post-Quantum Cryptography, Springer, 2018.

25. A. Takayasu, Y. Watanabe, *Lattice-based revocable identity-based encryption with bounded decryption key exposure resistance*, in Australasian Conference on Information Security and Privacy, Springer, 2017.

26. S. Yamada, *Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters*, in Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2016.

27. Q. Ye, M. Hu, W. Gao, Y. Tang, *A novel hierarchical identity-based encryption scheme from lattices*, in International Conference on Cloud Computing and Security, Springer, 2018.

28. L. Zhang, Q. Wu, *Adaptively secure hierarchical identity-based encryption over lattice*, in International Conference on Network and System Security, Springer, 2017.

29. D. Micciancio, C. Peikert, *Trapdoors for lattices: Simpler, tighter, faster, smaller,* in Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2012.

30. E. Fujisaki, T. Okamoto, Secure integration of asymmetric and symmetric encryption schemes, *J. Cryptology*, **26** (2013), 80–101.
31. J. Hong, B. Liu, Q. Sun, F. Li, A combined public-key scheme in the case of attribute-based for wireless body area networks, *Wireless Networks*, **25** (2019), 845–859.
32. H. Meng, Z. Chen, J. Hu, Z. Guan, *Establish the intrinsic binding in naming space for future internet using combined public key*, in Proceedings of the 11th International Conference on Future Internet Technologies, ACM, 2016.
33. W. Tang, X. Nan, Z. Chen, *Combined public key cryptosystem*, in Proceedings of International Conference on Software, Telecommunications and Computer Networks (SoftCOM04), 2004.
34. O. Regev, On lattices, learning with errors, random linear codes, and cryptography, *J. ACM*, **56** (2009), 34.
35. D. Micciancio, O. Regev, *Lattice-based cryptography*, Post-quantum cryptography. Springer, Berlin, Heidelberg, 2009. 147–191.
36. S. D. Gordon, J. Katz, V. Vaikuntanathan, *A group signature scheme from lattice assumptions*, in International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2010.
37. D. Boneh, R. Canetti, S. Halevi, J. Katz, Chosen-ciphertext security from identity-based encryption, *SIAM J. Comput.*, **36** (2006), 1301–1328.

AIMS Press