Fully Homomorphic Encryption from Ring-LWE：Identity-Based，Arbitrary Cyclotomic，Tighter Parameters

GU Chun-xiang[①] XIN Dan[①] ZHENG Yong-hui[①] KANG Yuan-ji[①]

[①](*State Key Laboratory of Mathematical Engineering and Advanced Computing , Zhengzhou 450001*)

Abstract: Fully homomorphic is an encryption scheme that allows for data to be stored and processed in an encrypted format, which gives the cloud provider a solution to host and process data without even knowing what the message is. In previous identity-based homomorphic encryption scheme, computing efficiency is complicated and expensive. In this work, based on Regev's work, we propose a sampling trapdoor one-way function in arbitrary cyclotomic rings $R = \mathbb{Z}[X]/(x^n + 1)$. Then construct a leveled identity-based homomorphic encryption scheme from ring learning with errors, which has advantage in computational efficiency and key management, by using user's identity as the unique public key. This scheme is proved IND-CPA secure in the random oracle model, relied to hardness of decision ring learning with errors problem.

Key words: fully homomorphic encryption; identity-based; ring learning with errors; cyclotomic rings;

1 Introduction

Fully homomorphic encryption allows a number of plaintexts additions and multiplications while evaluating only ciphertext. This encryption thought gives a solution for many problems, such as privacy problem on cloud computing, private information retrieval, etc. In 2009, Craig Gentry [1] proposed the first fully homomorphic encryption scheme on ideal lattices, which make a breakthrough in this field.

Gentry constructed a "somewhat homomorphic" scheme at first, which support only a limited number of homomorphism multiplications, then by "bootstrapping" one obtains a fully homomorphic encryption scheme. Since the appearance of Gentry's scheme, there has been put forward a series of homomorphic encryption schemes [2-4] based on different academic and mathematical problems. There has been much discussion in the field whether fully homomorphic encryption has practical value or not. One of reasons is that the existing encryption scheme's public key size is large, which effective key management has always been a problem of the encryption application. Identity based encryption [5] use the user's unique identity (such as E-mail addresses, etc.) as its public key, and user private key generated by the trusted third party, which do not rely on the public key certificate for key management. Naccache [6] first raised at CHES that to construct an identity-based fully homomorphic encryption scheme has been an open problem in 2010.

Gentry et al. [7] constructed an identity-based homomorphic encryption scheme from learning with errors [8], but support only a limited number of homomorphic additions and one time homomorphic multiplication. The encryption systems of Regev [9] proposed fully homomorphic

Henan province outstanding youth science and technology innovation (134100510002)；Henan province basis and research in cutting-edge technologies（142300410002）；State Key Laboratory of Mathematical Engineering and Advanced Computing innovation

Corresponding author : Chunxiang Gu , gcxiang5209@aliyun.com

encryption scheme based on dual Regev system, which has a better computational efficiency, but the size of evaluation key is too large. In 2013, the Gentry et al. [10] proposed a new technique for building identity-based homomorphic encryption scheme using called the approximate eigenvector method, and show how to compile an identity based encryption scheme satisfying a certain conditions to support homomorphism operations. Though their scheme has no evaluation key and easier to understand, the ciphertext has a big expansion.

The first fully homomorphic encryption from ring learning with errors is proposed by Brakerski and Vaikuntanathan[12]. What each sample $(\boldsymbol{a},b)\in \mathbb{Z}_q^n \times \mathbb{Z}_q$ in standard LWE-based applications instead of n samples $(a,b)\in R_q \times R_q$ from RLWE, decrease the size of the public key as well as the secret key by a factor of n .The advantage of RLWE to construct an encryption scheme is too much. Firstly, in RLWE distribution each product $b \approx a \cdot s$ give just a scalar pseudorandom values over R_q in place of n variants, yet it is fairly a few about the cost of computing. Secondly, it can be executed in $O(n\log n)$ scalar operations about polynomial multiplication, using the Fast Fourier Transform (FFT) in practice. With the advantage of RLWE, development recently in lattice cryptography, mostly resulting from the progress of ring-based primitives such as RLWE. On the choice of ring, the class of cyclotomic rings $R \cong \mathbb{Z}[X]/\Phi_m(X)$, which $\Phi_m(X)$ is mth cyclotomic polynomial, has proved very practical in cryptography because of their attractive features. There are especially a sort of cyclotomic rings easy to use, where the index $m = 2^k$ for some $k \geq 1$, called power-of-two cyclotomic rings. Because $n = m/2$ is also a power of two and polynomial arithmetic modulo $\Phi_m(X)$ can be computed very efficiently using an n-dimensional FFT. All RLWE-based fully homomorphic encryption schemes [13, 14] have proposed recently. Unfortunately, for an expected concrete security level, the index of this kind of cyclotomic polynomial must be the power of two, which may be lead to larger key sizes and runtime than necessity in application. Lyubashevsky et al. [15] give a toolkit for RLWE-based cryptography, which extended the index of rings to arbitrary positive integer and support single instruction multiple data (SIMD) operation at the same time. All the algorithms for arbitrary cyclotomic rings are simple, modular, and highly parallel. In a word, the ring-based scheme will have a better character.

Based on the Regev's trapdoor function with preimage sampling, we design the identity-based private key extraction algorithm over rings, for each user identity, which can generate the corresponding user's private key. Through the key switching technology, we make our identity-based somewhat homomorphic encryption scheme manipulate fully homomorphic operations. Compared with general fully homomorphic encryption system, our scheme can effectively improve the key management efficiency without using public key certificate authentication. To contrast with the existing identity-based fully homomorphic encryption scheme, we support multi-bit encryption, stronger resistance to attack ability, homomorphism multiplication faster. Finally, the security of our scheme strictly reduces to hardness of decisional ring learning with errors problem in the random oracle model, which is IND - CPA security.

2 Preliminaries

2.1 Notation

Generally speaking, vectors use lower-case letters in bold, eg $\boldsymbol{v}$ .The ith norm of $\boldsymbol{v}$ will be denoted

by $\boldsymbol{v}^{(i)}$.Matrices in bold capital letters, eg $\boldsymbol{A}^{m\times n}$ .The tensor product of two vectors $\boldsymbol{v}$, $\boldsymbol{u}$ of dimension n , denoted $\boldsymbol{u}\otimes\boldsymbol{v}$, is the n^2 dimensional vector containing all elements of the form $\boldsymbol{v}^{(i)}\boldsymbol{u}^{(j)}$.For a positive integer k , $[k]$ denotes the sets $\{0,\ldots,k-1\}$.The 2 norm of a vector $\boldsymbol{x}$ is denoted by $\boldsymbol{x}=\left(\sum_i\left|\boldsymbol{x}^{(i)}\right|^2\right)^{\frac{1}{2}}$ .For an n-by-n matrix $\boldsymbol{M}$, we denote by $\boldsymbol{s}_1(\boldsymbol{M})$ its largest singular value. Table1.1 provides a glossary of main algebraic objects and notation used in this work, and pointers to further discussion of their properties.

Table 1.1 Algebraic Notations

Notation	Description
$m,\ n,\ \hat{m},\ \mathbb{Z}_m^*$	The cyclotomic index $n=\varphi(m)$ ； if m is even, $\hat{m}=m/2$,otherwise $\hat{m}=m$, $\mathbb{Z}_m^*$ is a set of all positive integers less than m and coprime with m .
$\zeta_m,\ \omega_m$	$\zeta_m\in K,\ \omega_m\in\mathbb{C}$ is primitive mth root of unity.
$K=\mathbb{Q}(\zeta_m)\cong\mathbb{Q}(X)/\Phi_m(X)$	The mth cyclotomic number field K , $\Phi_m(X)=\prod_{i\in\mathbb{Z}_m^*}\left(X-\omega_m^i\right)\in\mathbb{Z}[X]$ is mth cyclotomic polynomial.
$K_{\mathbb{R}}$	$K_{\mathbb{R}}=K\otimes\mathbb{R}$
$\sigma_i:K\to\mathbb{C},i\in\mathbb{Z}_m^*$	σ_i is $K\to\mathbb{C}$ auto-homomorphic, $i\in\mathbb{Z}_m^*,\sigma_i(\zeta_m)=\omega_m^i$.
$R=\mathbb{Z}(\zeta_m)\cong\mathbb{Z}[X]/\Phi_m(X)$	The ring of integers of K .
R_q	For positive integers $q\geq 2, R_q=R/qR$.
$Tr(\cdot):K\to\mathbb{Q}$	The trace $Tr(a):K\to\mathbb{Q}$ ， for $a\in K, Tr(a)=\sum_i\sigma_i(a)$.
$R^\vee, R^\vee=\left\langle t^{-1}\right\rangle, g, t\in R$	The dual of R is $R^\vee=\{a\in K: Tr_{K/\mathbb{Q}}(aR)\subseteq\mathbb{Z}\}$,generated by $t^{-1}=g/\hat{m}$ .Each of $R^\vee$, $g=\prod_p(1-\zeta_p)\in R$, p can be divided all m.
$\boldsymbol{B}=\{\boldsymbol{b}_j\},\ \boldsymbol{p}$	The good basis is consist of sufficient short basis， $\boldsymbol{p}=\left(\zeta_m^j\right)_{j\in[n]}=\left(1,\zeta_m,\ldots,\zeta_m^{n-1}\right)\in K^{[n]}$ over K is powerful basis.

2.2 Ring Learning With Errors

Lyubashevsky et al. [16] give a quantum reduction from approximate (the search version of) the shortest vector problem (SVP) in the worst case on ideal lattices in R to within a fixed poly(n) factor at first. Then any poly(n) number of samples drawn from the RLWE distribution are pseudorandom to any polynomial-time (possibly quantum) attacker.

First two distributions are given: 1) for point $\boldsymbol{c}$ as the center, the standard deviation $r/\sqrt{2\pi}$ of the gaussian distribution $D_{r,\boldsymbol{c}}$ when $\boldsymbol{c}=\boldsymbol{0}$, in a short D_r , and the corresponding discrete gaussian distribution for lattice Λ point $\boldsymbol{c}$ as the center, $D_{\Lambda,r,\boldsymbol{c}}$ when $\boldsymbol{c}=\boldsymbol{0}$, for short $D_{\Lambda,r}$ .2) For secret value $s\in R_q^\vee$ (or $R^\vee$), define a RLWE distribution $A_{s,\psi}$ over $R_q\times\left(K_{\mathbb{R}}/qR^\vee\right)$ the variable is in the form of $\left(a,b=a\cdot s+e\ mod\ qR^\vee\right)$, where each a is uniformly random from distribution R_q , choosing e from distribution ψ .

Definition 1[16] **(RLWE, Search)**

Let Ψ be a family of distribution over $K_{\mathbb{R}}$. The search version of the ring-LWE problem , denoted $\mathrm{RLWE}_{q,\Psi}$,is defined as follows: give access to arbitrarily many independent samples from $A_{s,\psi}$ for some arbitrary $s\in R_q^\vee$ and $\psi\in\Psi$, find s .

Definition 2[16] **(RLWE, Average-Case Decision)**

The average-case decision version of the ring learning with errors problem, denoted $\mathrm{DRLWE}_{q,\psi}$,is to distinguish with non-negligible advantage between arbitrarily many

independent samples from $A_{s,\psi}$, where $s \leftarrow R_q^\vee$ is uniformly random , and the same number of uniformly random and independent samples from $R_q \times \left(K_{\mathbb{R}} / qR^\vee\right)$.

Theorem 1 [16]

Let K be the mth cyclotomic number field having dimension $n = \varphi(m)$ and $R = O_K$ be its ring of integers. Let $a = a(n) > 0$, and let $q = q(n) \geq 2$, $q = 1 mod\, m$ be a poly(n)-bounded prime such that $\alpha q \geq \omega\left(\sqrt{logn}\right)$ .Then there is a polynomial-time quantum reduction from $\tilde{\mathrm{O}}\left(\sqrt{n} / \alpha\right)$-approximate SIVP(or SVP) on ideal lattices in K to the problem of solving $\mathrm{DRLWE}_{q,\psi}$ given only l samples ,where ψ is the Gaussian distribution $D_{\xi,q}$,for $\xi = \alpha \cdot \left(nl / log\left(nl\right)\right)^{1/4}$.

In application it is often useful to work with a version of ring-LWE whose error distribution is discrete. If $\mathrm{RLWE}_{q,\Psi}$ is hard with some number l of samples ,then so is $\mathrm{RLWE}_{q,\Psi}$ with the same number of samples, where the error distribution χ is $\lfloor p \cdot \psi \rceil_{\omega + pR^\vee}$ for some integer p coprime to q, $\lfloor \cdot \rceil$ is any valid discretization to (cosets of) $pR^\vee$, and ω is an arbitrary in $R_p^\vee$ that can vary from samples to samples(even adaptively and adversarially). The paper [16] proved that $\mathrm{DRLWE}_{n,l,q,\chi}$ which two sets of variables respectively from the distribution $A_{s,\chi}$ and uniform distribution $R_q \times R_q^\vee$, is as hard as $\mathrm{RLWE}_{q,\Psi}$.

2.3 One-Way Trapdoor Functions with Preimage Sampling

Gentry et al. [11] generated one-way trapdoor functions with preimage sampling, which can map the discrete gaussian distribution to approximate uniform distribution. And with the trapdoor, the inversion function is existed, which can map the approximate uniform distribution to the discrete gaussian distribution.

Before giving concrete constructions, we recall the result of Ajtai [19] that shows how to sample an essentially uniform $\boldsymbol{A} \in \mathbb{Z}_q^{[n] \times [l]}$, along with a short full-rank "trapdoor "set of lattice vectors $S \subset \Lambda^\perp\left(\boldsymbol{A}, q\right)$.

Proposition 1[11]

For any prime $q = q(n)$ and any $l \geq 5nlogq$,there is a probabilistic polynomial-time algorithm TrapGen $\left(1^n\right)$ that ,on input 1^n ,outputs a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{[n] \times [l]}$ and a full-rank set $S \subset \Lambda^\perp\left(\boldsymbol{A}, q\right) = \left\{\boldsymbol{e} \in \mathbb{Z}_q^{[l]} : \boldsymbol{A} \cdot \boldsymbol{e} = \boldsymbol{0} \bmod q\right\}$,where the distribution $\boldsymbol{A}$ is statistically close to uniform over $\mathbb{Z}_q^{[n] \times [l]}$ and the length $\|S\| \leq l^{2.5}$.

Definition 3 [11] (**One-Way Trapdoor Functions with Preimage Sampling**) :

For matrix algorithm *TrapGen* $\left(1^n\right)$ generation matrix $\boldsymbol{A}$, define functions $f_{\boldsymbol{A}} : \mathbb{Z}_q^{[l]} \to \mathbb{Z}_q^{[n]}$ $f_{\boldsymbol{A}}\left(\boldsymbol{e}\right) = \boldsymbol{A} \cdot \boldsymbol{e} \bmod q$ for vector $\boldsymbol{e} \leftarrow D_{\mathbb{Z}_q^{[l]}, r}$, $r \geq \omega\left(\sqrt{logl}\right)$.In the case of have the trapdoor, function $f_{\boldsymbol{A}}$ is reversible, inverse function is $f_{\boldsymbol{A}}^{-1} : \mathbb{Z}_q^{[n]} \to \mathbb{Z}_q^{[l]}$ .choosing $\boldsymbol{u} \in \mathbb{Z}_q^{[n]}$ in arbitrary, vector $\boldsymbol{e}$ calculation steps are as follows: 1) meet the special solution $\boldsymbol{t}$ of equation $\boldsymbol{A} \cdot \boldsymbol{t} = \boldsymbol{u} \bmod q$;2) before using the trapdoor S as sampling, on distribution $D_{\Lambda^\perp, r, -\mathbf{t}}$ vector $\boldsymbol{v}$;3) output $\boldsymbol{e} = \boldsymbol{t} + \boldsymbol{v}$.

3 Identity-Based Fully Homomorphic Encryption Scheme

Definition 4 (**Identity-Based Fully Homomorphic Encryption**)

Our identity-based fully homomorphic encryption system is a tuple of probabilistic polynomial time (PPT) algorithms {Setup, Extract, Enc, Dec, Eval}.

--Setup $\left(1^\kappa\right)$: for a security parameters κ , and output public parameters *params*, master public

key and master private key (*mpk, msk*).

--**Extract**(mpk,msk,id): take public parameters *params*, master public key, master private key and identity *id* as input, and output a private key sk_{id} and evk_{id}.

--**Enc**(mpk,id,μ): input master public key *mpk*, identity *id* and plaintext μ, output ciphertext c.

--**Dec**(c,sk_{id}): the decryption algorithm, input c and private key sk_{id}, output plaintext μ.

--**Eval**$(f,c_1,...,c_t,evk_{id})$: input a function f and a set of ciphertexts $c_1,c_2,\ldots,c_t$ using the same identity *id*, output a new ciphertext c, satisfying the homomorphism operation properties.

Definition 5 (**identity-based fully homomorphic encryption scheme IND - CPA security**)

Because of the ciphertext homomorphism operation properties, any fully homomorphic encryption system have no possibilities to resist adaptive chosen-ciphertext attack (CCA2). The general notion of security of fully homomorphic encryption scheme is indistinguishability against chosen plaintext attack (IND - CPA).

Security Game:

Initialization: challenger C executes the *Setup* algorithm, generating our scheme of public parameters and master private key, and gives the public parameters to the attacker $\mathcal{A}$.

Phase 1: at this stage, the attacker $\mathcal{A}$ freely chooses an identity $id_i \in \{0,1\}^*$, by private key extract oracle to obtain the identity id_i of the corresponding private key sk_{id_i}, and add id_i to the list P.

Challenge: at the end of phase 1, the attacker $\mathcal{A}$ chooses $id^* \notin P$, and two length equal to the challenge of plaintext $\{\mu_0^*,\mu_1^*\}$, to the challenger C. Selected $b \in \{0,1\}$ at random, using the identity id^* to encrypt μ_b^*, get the target ciphertext $c^* = Enc(id^*,\mu_b^*)$, and return to $\mathcal{A}$.

Phase 2: the attacker freely chooses $id' \in \{0,1\}^*$ satisfying $id' \neq id^*$, and gets the identity of the corresponding private key $sk_{id'}$.

Guess: the attacker $\mathcal{A}$ guesses target ciphertext c^* corresponding plaintext, output $b' \in \{0,1\}$. If $b' = b$, $\mathcal{A}$ wins the game in this attack.

The probability of $\mathcal{A}$ winning this game is defined as $\Pr\left|\mathrm{Adv}_{\mathrm{Game}}[\mathcal{A}]\right|$, and the advantage is defined as $\mathrm{Adv}_{\mathrm{CPA}}[\mathcal{A}] = \left|\Pr\left|Adv_{Game}[\mathcal{A}]\right| - \frac{1}{2}\right|$. If the advantages can be ignored for any attacker in polynomial time, the scheme is IND - CPA security.

4 Construction

Let security parameters κ, positive integer $m = \kappa$, index $n = \varphi(m)$, prime $q = q(n) \geq 2$, $l \geq 5nlogq$, powerful basis $\boldsymbol{p}$ over R, hash function $\mathrm{H}:\{0,1\}^* \to \mathbb{Z}_q^{[n]\times[n]}$. The scheme is described as follows.

4.1 Somewhat Homomorphic Encryption Scheme

- **IBFHE-Setup**(1^κ): input security parameters κ, invoke $TrapGen(1^n)$ to generate a full-rank set *S* as master private key, uniformly random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{[n]\times[l]}$ as master public key and correspond one-way trapdoor functions with preimage sampling f_A as a pair of public parameters.

- **IBSHE-Extract** $(\boldsymbol{A},S,id)$：input public parameters, master private key , identity and powerful basis $\boldsymbol{p}$ over R , compute $\boldsymbol{U}=\mathrm{H}(id)\in\mathbb{Z}_q^{[n]\times[n]}$, let $\boldsymbol{U}=(\boldsymbol{u}_1,\ldots,\boldsymbol{u}_n)$, $\boldsymbol{e}_i=f_A^{-1}(\boldsymbol{u}_i)$ using the inverse function with trapdoor S , $\boldsymbol{E}=(\mathbf{e}_1,\ldots,\mathbf{e}_n)\in\mathbb{Z}_q^{[l]\times[n]}$, output private key $\boldsymbol{e}=\boldsymbol{E}\boldsymbol{p}\in R_q^{[l]}$ 。
- **IBSHE-Enc** $(\boldsymbol{A},id,\mu)$: input master public key, identity and message $\mu\in R_p$, do:
  1. Compute $\boldsymbol{U}=\mathrm{H}(id)\in\mathbb{Z}_q^{[n]\times[n]}$, $u=\boldsymbol{p}^T\boldsymbol{U}\boldsymbol{p}\in R_q$;
  2. Select a uniformly random $r\leftarrow R_q$ and $\boldsymbol{x}^{(0)},\ldots,\boldsymbol{x}^{(l)}\leftarrow\lfloor p\cdot\overline{\psi}\rceil_{pR^\vee}$, $\boldsymbol{x}=\left(\boldsymbol{x}^{(0)},\ldots,\boldsymbol{x}^{(l)}\right)$;
  3. Compute $\rho=ru+x\in R^\vee$, where $x\leftarrow\lfloor p\cdot\overline{\psi}\rceil_{t^{-1}\mu+pR^\vee}$, $\boldsymbol{v}=\left(-r\boldsymbol{p}^T\boldsymbol{A}+p\boldsymbol{x}\right)\in R_q^{1\times[l]}$,output ciphertext $c=(\rho,\boldsymbol{v})\in R_q\times R_q^{[l]}$.
- **IBSHE-Dec** $(c,\boldsymbol{e})$：compute $x=(\rho+\boldsymbol{v}\boldsymbol{e}\ mod\ q)mod\ p$,output plaintext $\mu=t\cdot x\,mod\ pR$ 。

4.2 Homomorphic Operations

The correctness analysis of our scheme is as follows: there is a polynomial $c(Y)=\rho+\boldsymbol{v}Y$ and the decryption process can be seen as

$$\begin{aligned}c(\boldsymbol{e})&=ru+x-r\boldsymbol{p}^T\boldsymbol{A}\boldsymbol{e}+p\boldsymbol{x}\boldsymbol{e}\\&=x+p\boldsymbol{x}\boldsymbol{e}\end{aligned}$$

As long as the noise $\|x+p\boldsymbol{x}\boldsymbol{e}\|<q/4$, the decryption correctly, and then $c(\boldsymbol{e})$ module p to get noise x , compute $\mu=t\cdot x\ mod\ pR$ to obtain the plaintext.

Give ciphertexts $c=(\rho,\boldsymbol{v})$, $c'=(\rho',\boldsymbol{v}')$,which encrypts two messages $\mu,\mu'\in R_p$, with $x\leftarrow\lfloor p\cdot\overline{\psi}\rceil_{t^{-1}\mu+pR^\vee}$, $x'\leftarrow\lfloor p\cdot\overline{\psi}\rceil_{t^{-1}\mu'+pR^\vee}$ respectively. There exist two decrypt polynomials $c(Y)=\rho+\boldsymbol{v}Y$, $c'(Y)=\rho'+\boldsymbol{v}'Y$.

- **IBSHE-Add**:

$$\begin{aligned}c(Y)+c'(Y)&=\rho+\boldsymbol{v}Y+\rho'+\boldsymbol{v}'Y\\&=\rho+\rho'+(\boldsymbol{v}+\boldsymbol{v}')Y\end{aligned}$$

When the variant Y is the private key $\boldsymbol{e}$ ：

$$\begin{aligned}Dec_e\left[c(Y)+c'(Y)\right]&=\rho+\boldsymbol{v}\boldsymbol{e}+\rho'+\boldsymbol{v}'\boldsymbol{e}'\\&=ru+x-r\boldsymbol{p}^T\boldsymbol{A}\boldsymbol{e}+p\boldsymbol{x}\boldsymbol{e}+r'u+x'-r'\boldsymbol{p}^T\boldsymbol{A}\boldsymbol{e}+p\boldsymbol{x}'\boldsymbol{e}\\&=x+x'+p\boldsymbol{x}\boldsymbol{e}+p\boldsymbol{x}'\boldsymbol{e}\end{aligned}$$

If noise $\|x+x'+p\boldsymbol{x}\boldsymbol{e}+p\boldsymbol{x}'\boldsymbol{e}\|<q/4$ ， decryption correctly. We can obtain $x+x'$ which $Dec_e\left[c(Y)+c'(Y)\right]$ module p and compute $\mu+\mu'=t\cdot(x+x')mod\ pR$.

- **IBSHE-Mult**:

$$\begin{aligned}c(Y)\cdot c'(Y)&=(\rho+\boldsymbol{v}Y)\times(\rho'+\boldsymbol{v}'Y)\\&=\rho\rho'+(\rho\boldsymbol{v}'+\rho'\boldsymbol{v})Y+\boldsymbol{v}Y\boldsymbol{v}'Y\end{aligned}$$

When the variant Y is the private key $\boldsymbol{e}$ ：

$$\begin{aligned}Dec_e\left[c(Y)\cdot c'(Y)\right]&=\left(ru+x-r\boldsymbol{p}^T\boldsymbol{A}\boldsymbol{e}+p\boldsymbol{x}\boldsymbol{e}\right)\times\left(r'u+x'-r'\boldsymbol{p}^T\boldsymbol{A}\boldsymbol{e}+p\boldsymbol{x}'\boldsymbol{e}\right)\\&=x\cdot x'+2p^2\boldsymbol{x}\boldsymbol{e}\boldsymbol{x}'\boldsymbol{e}+xp\boldsymbol{x}'\boldsymbol{e}+x'p\boldsymbol{x}\boldsymbol{e}\end{aligned}$$

let $e'=2p^2\boldsymbol{x}\boldsymbol{e}\boldsymbol{x}'\boldsymbol{e}+xp\boldsymbol{x}'\boldsymbol{e}+x'p\boldsymbol{x}\boldsymbol{e}$ ， if the nosie $\|x\cdot x'+e'\|<q/4$ ， decryption correctly，obtain the results $x\cdot x'$ when $Dec_e\left[c(Y)\cdot c'(Y)\right]$ module p ,compute $\mu\mu'=t^2\cdot(x\cdot x')mod\ pR$ .After once

homomorphism multiplication, the ciphertext $\boldsymbol{c}_{mult}=\left(\rho\rho',\rho\boldsymbol{v}'+\rho'\boldsymbol{v},\boldsymbol{v}\otimes\boldsymbol{v}'\right)$。

4.3 Key-switching

After a homomorphism multiplication, the dimension of ciphertext improve to l^2+l+1 from $l+1$. As the homomorphism multiplication continues, the size of ciphertext goes into exponential growth. With the cyclotomic polynomial algebra features, we can make the ciphertext vector dimension always remain $l+1$ by using key switching technique.

Let vector $\boldsymbol{g}=\left(1,2,4,...,2^{b-1}\right)\in\mathbb{Z}_q^{[b]}$, and the matrix $\boldsymbol{G}=I_{[j]}\otimes\boldsymbol{g}^T\in\mathbb{Z}_q^{[j]\times[bj]}$,which I is the identity matrix, $b=\lceil log_2 q\rceil$, $j=l^2+l+1$. As the paper[18]already mentioned, integer lattice $\mathcal{L}^{\perp}\left(\boldsymbol{G}\right)=\left\{\mathbf{z}\in\mathbb{Z}^{[bj]}:\boldsymbol{G}\mathbf{z}=0\in\mathbb{Z}_q^{[j]}\right\}$ has a good basis $\boldsymbol{D}=I_{[j]}\otimes\boldsymbol{S}_{\boldsymbol{g}}\in\mathbb{Z}_q^{[bj]\times[bj]}$.

if $q=2^b$, $S_g=\begin{pmatrix}2&&&&\\-1&2&&&\\&-1&\ddots&&\\&&&2&\\&&&-1&2\end{pmatrix}$, otherwise $S_g=\begin{pmatrix}2&&&&q_0\\-1&2&&&q_1\\&-1&&&q_2\\&&\ddots&&\vdots\\&&&2&q_{b-2}\\&&&-1&q_{b-1}\end{pmatrix}$。

For a prime q, it is a binary representation of the form $q=\left(q_{b-1}\cdots q_1q_0\right)_2=\sum_{i\in[b]}q_i2^i$.Through the paper [15], we know $\boldsymbol{Z}=\boldsymbol{D}\otimes\boldsymbol{p}\in R_q^{[bj]\times[bjn]}$ is a good basis of integer lattice $\Lambda^{\perp}\left(\boldsymbol{G}\right)$, satisfying $\boldsymbol{s}_1\left(\boldsymbol{Z}\right)=\boldsymbol{s}_1\left(\boldsymbol{D}\right)\cdot\boldsymbol{s}_1\left(\boldsymbol{p}\right)=\boldsymbol{s}_1\left(\boldsymbol{D}\right)\cdot\sqrt{\hat{m}}\le 3\sqrt{\hat{m}}$.

After a homomorphism multiplication, ciphertext vector $\boldsymbol{c}\in\mathcal{I}_q^{[j]}$, $\boldsymbol{s}=\left(1,\boldsymbol{e},\boldsymbol{e}\otimes\boldsymbol{e}\right)\in R_q^{[j]}$, $\left\langle\boldsymbol{c},\boldsymbol{s}\right\rangle=emod q\mathcal{I}$, $e\leftarrow t^{-2}\mu+p\mathcal{I}$, where $\mathcal{I}=\left(R^{\vee}\right)^2$.First of all, give a relation $\left\langle\boldsymbol{c},\boldsymbol{s}\right\rangle=emod\ q\mathcal{I}$ by the factor $\hat{m}$, then $\left\langle t\cdot\hat{m}\cdot\boldsymbol{c},t^{-1}\boldsymbol{s}\right\rangle=\hat{m}\cdot emod\ qR^{\vee}$; let $\boldsymbol{y}=t\cdot\hat{m}\cdot\boldsymbol{c}\in R_q^{[j]}$, choose a good basis $\boldsymbol{Z}$ of $\Lambda^{\perp}\left(\boldsymbol{G}\right)$, using coordinate-wise randomized rounding compute $\boldsymbol{x}$, which mentioned in the paper [15], satisfying $\boldsymbol{G}\boldsymbol{x}=\boldsymbol{y}\in R_q^{[j]}$.At last, select the target private key $\boldsymbol{s}'\leftarrow R_q^{[l]}$.

For $i\in[bj]$, $\boldsymbol{\rho}=(\boldsymbol{\rho}^{(i)})_{i\in[bj]}$, $\boldsymbol{V}=\left(\boldsymbol{v}_1,...,\boldsymbol{v}_{bj}\right)$, compute $IBSHE\text{-}Enc\ \left(\boldsymbol{A},id,0\right)=(\boldsymbol{\rho}^{(i)},\boldsymbol{v}_i)$, $c\left(\boldsymbol{s}'\right)mod\ p=\boldsymbol{f}^{(i)}\leftarrow\lfloor\underline{p}\cdot\overline{\psi}\rceil_{pR^{\vee}}$, $\boldsymbol{f}=(\boldsymbol{f}^{(i)})_{i\in[bj]}$,and $\left\langle\boldsymbol{x},\boldsymbol{f}\right\rangle$ is sufficient short. let $\delta=\left(\boldsymbol{h}^{(i)},\boldsymbol{v}_i\right)_{i=0}^{[bj]}$, $\boldsymbol{h}^{(i)}=\boldsymbol{\rho}^{(i)}+\left(t^{-1}\boldsymbol{G}^T\boldsymbol{s}\right)^{(i)}mod\ qR^{\vee}$.

The target ciphertext $c' = (\rho', \boldsymbol{v}')$, $\rho' = \sum_{i \in [bj]} \boldsymbol{h}^{(i)} \boldsymbol{x}^{(i)} = \langle \boldsymbol{x}, \boldsymbol{\rho} \rangle + \langle \boldsymbol{x}, t^{-1} \boldsymbol{G}^T \boldsymbol{s} \rangle$, $\boldsymbol{v}' = \boldsymbol{x}\boldsymbol{V}$, When the variant Y is the target private key $\boldsymbol{s}'$:

$$c(\boldsymbol{s}') = \rho' + \boldsymbol{v}'\boldsymbol{s}' = \langle \boldsymbol{x}, \boldsymbol{\rho} \rangle + \langle \boldsymbol{x}, t^{-1} \boldsymbol{G}^T \boldsymbol{s} \rangle + \boldsymbol{x}\boldsymbol{V}\boldsymbol{s}' mod\ p$$
$$= \langle \boldsymbol{x}, \boldsymbol{f} \rangle + \langle \boldsymbol{x}, t^{-1} \boldsymbol{G}^T \boldsymbol{s} \rangle = \langle \boldsymbol{x}, \boldsymbol{f} \rangle + \hat{m} \cdot e\, mod\ qR^{\vee}$$

Which the noise $e^* = \langle \boldsymbol{x}, \boldsymbol{f} \rangle + \hat{m} \cdot e \in R^{\vee}$, compute message $t \cdot \hat{m} \cdot e = g \cdot \mu\ mod\ pR$

4.4 Identity-Based Fully Homomorphic Encryption Scheme

IBFHE-Setup $(1^{\kappa}, 1^{L})$: input security parameters κ and a number of levels L(maximum circuit depth to support), invoke *IBFHE-Setup* (1^{κ}) algorithm to output public parameters and the master private key.

IBFHE-Extract $(\boldsymbol{A}, S, id)$: invoke *IBSHE-Extract* $(\boldsymbol{A}, S, id)$ algorithm to extract private key $\boldsymbol{e}$.

Set $\boldsymbol{e}_0 = \boldsymbol{e}$, select L vectors $\boldsymbol{e}_1, \boldsymbol{e}_2, ..., \boldsymbol{e}_L$ in uniform distribution over $R_q^{[l]}$ at random and calculate $evk_{id} = \{\delta_{i \to i+1}\}_{i=0}^{L}$ as evaluation key.

IBFHE-Enc $(\boldsymbol{A}, id, \mu)$: using *IBSHE-Enc* $(\boldsymbol{A}, id, \mu)$, output ciphertext $c = (\rho, \boldsymbol{v}, 0)$, where 0 means circuit's level.

IBFHE-Dec $(c_i, \boldsymbol{e}_i)$: for ciphertext $c_i = (\rho_i, \boldsymbol{v}_i, i)$, using the private key $\boldsymbol{e}_i$ to generate $x_i = (\rho_i + \boldsymbol{v}_i \boldsymbol{e}_i mod\ q) mod\ p$ and output message $\mu = t^i \cdot x_i\ mod\ pR$.

IBFHE-Eval $(f, c_1, ..., c_t, evk)$: any f operation can be represented as arbitrary combinations of homomorphism multiplication and addition. The ciphertext form in operation process, sign a l show the "level" of the ciphertext. Homomorphism addition directly invoke *IBSHE- Add* algorithm. When execute homomorphism multiplication, we must firstly obtain the evaluation key $\delta_{i \to i+1}$, then call *IBSHE-Mult* algorithm .

5 Security Proof and Efficiency Analysis

5.1 Security Proof

Theorem 2 let $m = \kappa$, $n = \varphi(m)$, $q = q(n) \geq 2$, $l \geq 5nlogq$, the above cryptosystem is IND-CPA secure in random oracle model assuming the hardness of $\mathrm{DRLWE}_{n,l,q,\chi}$.

Proof. We prove the lemma based on game, $Adv_{\mathrm{Game}}[\mathcal{A}]$ defined as the attacker's advantage in the following game.

Game0: Game0 is standard IND - CPA game, namely the attacker $\mathcal{A}$ chooses a challenge identity id^* and selects two challenges plaintexts $\{\mu_0^*, \mu_1^*\}$ from plaintext space at random to the

challenger C . C computes the corresponding evaluation key evk_{id^*} , generates challenge ciphertext c^* and hands them over to the attacker $\mathcal{A}$. The attacker guesses the plaintext. In this game, the advantage of $\mathcal{A}$ is:

$$Adv_{\mathrm{CPA}}[\mathcal{A}] = |\Pr[\mathcal{A}(id^*, \mathrm{IBFHE\text{-}Enc}(\boldsymbol{A}, id^*, \mu_0^*) = 1] - \Pr[\mathcal{A}(id^*, \mathrm{IBFHE\text{-}Enc}(\boldsymbol{A}, id^*, \mu_1^*) = 1]|$$

Game 1: Game1 changes the generation of $\mathrm{H}(id^*)$ in Game0. In Game 1 , $\mathrm{H}(id^*)$ have no longer available from the access list in random oracle model $\mathrm{H}(\cdot)$, but choose from the uniformly random distribution over $\mathbb{Z}_q^{[n]\times[n]}$ .The attacker is unable to distinguish between Game0 and the modified Game 1, so:

$$|Adv_{\mathrm{Game1}}[\mathcal{A}] - Adv_{\mathrm{CPA}}[\mathcal{A}]| = 0$$

Game2: Game2 is as same as Game 1, where the difference is that the generation of evaluation key evk_{id^*} . The challenger randomly selects a group evk_{id^*} from $R_q^{[bj]}$ to the attacker. So the attacker's advantage difference between Game2 and Game1 is equal to successfully solve the L instances of the probability $\mathrm{DRLWE}_{n,bj,q,\chi}$:

$$|Adv_{Game2}[\mathcal{A}] - Adv_{Game1}[\mathcal{A}]| = 1 - \prod_{i=0}^{L}(1 - Adv_{\mathrm{DRLWE}_{n,bj,q,\chi}}[\mathcal{A}_i])$$

Game3: Game 3 and Game 2 differ in the encryption algorithm. The calculation of the ciphertext $\boldsymbol{v}$ is not through $\boldsymbol{v} = \left(-r\boldsymbol{p}^T\boldsymbol{A} + p\boldsymbol{x}\right)$ but from a random uniform distribution $R_q^{[l]}$. The attacker's advantage difference between Game3 and Game2 is equal to its advantages of solving the problem $\mathrm{DRLWE}_{n,l,q,\chi}$:

$$|Adv_{Game3}[\mathcal{A}] - Adv_{Game2}[\mathcal{A}]| = \mathrm{DRLWE}_{n,l,q,\chi}Adv[\mathcal{A}]$$

Game4: In this game , Challenger C changes the generation of ciphertext , no longer calculate $c^* = (\rho, \boldsymbol{v})$ and selects challenge ciphertext from uniform distribution over $R_q \times R_q^{[l]}$ at random. The public key u choose from the uniform distribution over R_q , therefore $\rho = ru + x \in R^\vee$ is a instance of $\mathrm{DRLWE}_{n,1,q,\chi}$ problem, namely

$$|Adv_{Game4}[\mathcal{A}] - Adv_{Game3}[\mathcal{A}]| = \mathrm{DRLWE}_{n,1,q,\chi}Adv[\mathcal{A}]$$

In game4, public key and the ciphertext are uniform random and has nothing to do with plaintext space, so the advantage of the attacker in Game4 is zero, namely

$$Adv_{Game4}[\mathcal{A}] = 0$$

Therefore, $Adv_{\mathrm{CPA}}[\mathcal{A}]$ is negligible assuming the hardness of $\mathrm{DRLWE}_{n,l,q,\chi}$, so IBFHE is IND-CPA secure.

5.2 Efficiency Analysis

IBFHE scheme proposed in this paper introduce the thought of identity to the homomorphic encryption scheme. By contrast, the scheme proposed by Brakerski[12], must generate the public key certificate for legitimacy certification, which include the public key certificate distribution, management costs and the choice of cyclotomic rings' index must be the power of 2. And the paper[7]is based on identity but only achieve limited homomorphism operation, and IBFHE support leveled homomorphic operation. Compared with the paper[18], IBFHE which is based on RLWE, support multi-bit encryption, improve the encryption computing complexity , ciphertext size is shorter, using fast Fourier transform (FFT) and the multiplication over R_q can be achieved $\mathrm{O}(nlogn)$.

Table 5.1 shows the comparison on computing efficiency of two scheme in the same

parameter approximation SVP cases, for security parameters κ take 100, the paper[18] system $n=\kappa^2$, $q\approx 2^{\sqrt{n}}$;Our scheme IBFHE, m can take any positive integer, $m=\kappa$, $n=\varphi(m)$, prime $q=1 \bmod m$.

Table 5.1 Computing Efficiency Comparison

Scheme	p	n	$\lceil log_2 q \rceil$	Certificate	Encryption (module q)	Decryption (module q)	Ciphertext (module q)
paper[18]	2	10000	30	no	1.5×10^{10} multi 1.5×10^{10} add	1.5×10^{6} multi 1.5×10^{6} add	42.9 Mb
	-	-	-	-	-	-	-
IBFHE	2	40	30	no	1.7×10^{6} multi 4.8×10^{5} add	1.2×10^{6} multi 2.4×10^{5} add	6.9 Mb
	1024	40	30	no	1.7×10^{6} multi 4.8×10^{5} add	1.2×10^{6} multi 2.4×10^{5} add	6.9 Mb

6 Conclusion

Fully homomorphic encryption to solve the problem of cloud computing data privacy protection and private information problem provides a new thought. By using arbitrary cyclotomic rings' algebraic features, we proposed identity-based fully homomorphic encryption scheme from RLWE, which regard identity as a user's public key, so as to make the authentication and management is not rely on the public key certificate and support fully homomorphic operation simultaneously. Compared with the similar scheme from LWE, IBFHE supports the multi-bit encryption, has a shorter ciphertext size and improves computational efficiency tremendously. Although IBFHE is not completely consistent with standard identity-based cryptosystem, it does not affect the fully homomorphism operations in application. Finally, the security of our scheme strictly reduces to hardness of decision ring learning with errors problem in random oracle model.

Reference

[1]. Gentry C. Fully homomorphic encryption using ideal lattices[C]. Proceeding of 29th Annual ACM Symposium on the Theory of Computing, Bethesda, Maryland, USA, 2009.

[2]. Coron J S, Naccache D, and Tibouchi M. Public key compression and modulus switching for fully homomorphic encryption over the integers[C], Proceedings of the 31st Annual Eurocrypt Conference, Cambridge, United Kingdom, 2012.

[3]. Brakerski Z and Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE[J]. SIAM Journal on Computing, 2014, 43(2): 831-871.

[4]. López-Alt A, Tromer E, and Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C].Proceedings of the 44th annual ACM symposium on Theory of computing. ACM, 2012: 1219-1234.

[5]. Shamir A. Identity-based Cryptosystems and Signature Schemes[C]. Proceedings of the 8th Annual International Cryptology Conference, Santa Barbara, USA, 1984.

[6]. Naccache D. Is theoretical cryptography any good in practice[J]. Talk given at CHES, 2010.

[7]. Gentry C, Halevi S,and Vaikuntanathan V. A Simple BGN-Type Cryptosystem from LWE[J]. EUROCRYPT 2010, 2010: 506.

[键入文字]

[8]. Regev O. On lattices, learning with errors, random linear codes, and cryptography[C]. Proceeding of 37th Annual ACM Symposium on the Theory of Computing, Baltimore, MD, USA, 2005.

[9]. Brakerski Z. Fully homomorphic encryption without modulus switching from classical GapSVP[J]. Advances in Cryptology–CRYPTO 2012, 2012: 868-886.

[10]. Gentry C, Sahai A, and Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[C]. Proceedings of the 33th Annual International Cryptology Conference, Santa Barbara, USA, 2013.

[11]. Gentry C, Peikert C, and Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C].Proceedings of the fortieth annual ACM symposium on Theory of computing. ACM, 2008: 197-206.

[12]. Brakerski Z and Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages[C] . Proceedings of the 32th Annual International Cryptology Conference, Santa Barbara, USA, 2013.

[13]. Brakerski Z, Gentry C, and Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping[C]. Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. ACM, 2012: 309-325.

[14]. Gentry C, Halevi S, and Smart N P. Homomorphic Evaluation of the AES Circuit[C], Proceedings of the 32th Annual International Cryptology Conference, Santa Barbara, USA, 2013.

[15]. Lyubashevsky V, Peikert C, and Regev O. A Toolkit for Ring-LWE Cryptography[C].EUROCRYPT. 2013, 13: 35-54.

[16]. Lyubashevsky V, Peikert C, and Regev O. On ideal lattices and learning with errors over rings[J]. Journal of the ACM (JACM), 2013, 60(6): 43.

[17]. Micciancio D and Peikert C. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller[J]. Advances in Cryptology–EUROCRYPT 2012, 2012: 700-718.

[18]. Guang Yan,Zhu Yue-fei,and Gu Chun-xiang et al.Identity-Based Fully Homomorphic Encryption from LWE problem[J]. Journal on Communications, 2014, 35(2): 111-117.

[19]. Ajtai M. Generating hard instances of lattice problems[C].Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, 1996: 99-108.