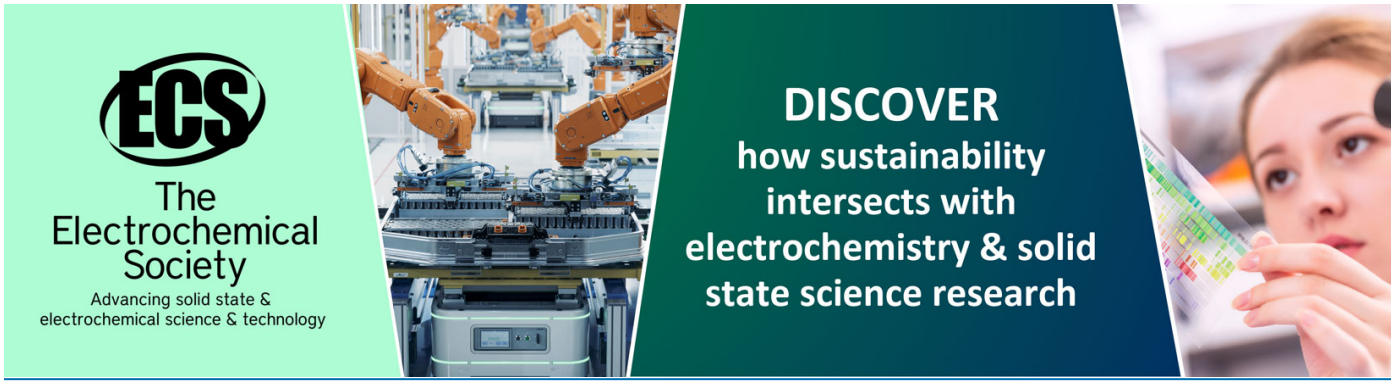
# Efficient Fully homomorphic encryption scheme using Ring-LWE





# Efficient Fully homomorphic encryption scheme using Ring-LWE

**Dan Xin[1*], Jingzhou Ji[1], Feng Jing[1], Mei Gao[1] and Bin Xue[1]**

[1]College of Information Communication, National University of Defense Technology, Xi'an, Shaanxi, 710106, China

[*]Corresponding author's e-mail: xindan625@nudt.edu.cn

**Abstract.** Data can be stored and processed in an encrypted format using fully homomorphic encryption, which makes cloud computing provider can process data well without even knowing data information. However, most existing homomorphic encryption schemes based on ring learning with errors, focus on the special classes of rings, such as power-of-two cyclotomic rings, which significantly limits its application efficiency in cloud computing. Therefore, in this letter, to solve this problem above, an efficient fully homomorphic encryption scheme is proposed based on ring learning with errors in arbitrary cyclotomic rings. Particularly, a "somewhat homomorphic encryption" scheme is firstly proposed based on ring learning with errors. A novel fully homomorphic encryption scheme is further presented using key-switching. With theoretical and experimental verification, the proposed scheme has advantage of high efficiency of encryption and decryption. The security of our scheme strictly reduces to hardness of decision ring learning with errors problem in the random oracle model.

## 1. Introduction

Fully homomorphic encryption is a cryptographic primitive that facilitates arbitrary computation on encrypted data, while users have no need to decrypt. This encryption technology gives a new solution for many problems, such as privacy protection problem in cloud computing as 'Figure1', private information retrieval, etc.

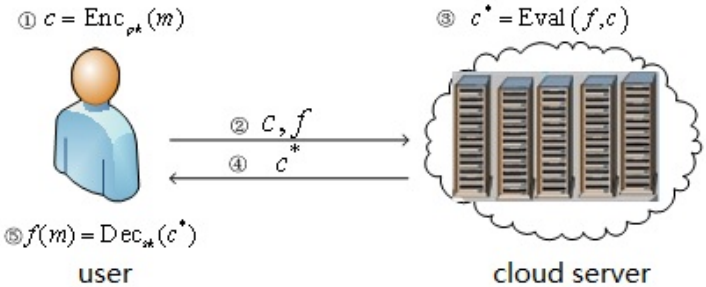



Figure 1. Application diagram of fully homomorphic encryption in cloud computing.

In 2009, Craig Gentry[1]proposed the first fully homomorphic encryption scheme on ideal lattices, which promotes the progress of constructing fully homomorphic encryption. In this paper, Gentry first obtained a "somewhat homomorphic" scheme, supporting only a limited number of ciphertext multiplications, and then using "bootstrapping" technology, one can construct a fully homomorphic encryption scheme. As a result of Gentry's research, a series of homomorphic encryption schemes based on different kinds of mathematical problems has been constructed. In 2012, Brakerski and

Vaikuntanathan[2] first proposed a fully homomorphic encryption scheme from ring learning with errors on CRYPTO. In 2013, Coron[3-5]constructed a fully homomorphic encryption from approximate maximum common factor problem on EUROCRYPT. In 2013, Gentry[6]first proposed an identity-based fully homomorphic Encryption scheme using approximate eigenvectors, but this scheme ciphertext expansion serious.In 2014,GUANG Yan[7]design an identity-based fully homomorphic encryption with pre-image sampling trapdoor one-way function to extract the private key ,but this scheme can't support multi-bit encryption. In 2016, Kang Yuanji[8] construct an identity-based fully homomorphic encryption from ring learning with errors, but only support the ciphertext homomorphic operations by same identity. In 2018, WANG Weili[9]construct an multi-identity-based fully homomorphic encryption from obfuscation, which supports cipher operation in different identities, and can carry out multiple homomorphic operations, but the scheme encryption and decryption efficiency is not high.

Therefore, in this letter, to solve the efficiency problem well, firstly, a "somewhat homomorphic encryption" scheme is proposed based on ring learning with errors problem. And then, a fully homomorphic encryption scheme is presented using key-switching technology. In this paper, non-power-of-two cyclotomic rings is innovatively exploited, instead of power-of-two cyclotomic rings as usual. Finally, the security of the proposed scheme strictly reduces to hardness of decisional ring learning with errors problem in the random oracle model.

## 2.Preliminaries

### *2.1. Notation*

In this paper, the concept of circular field in algebraic number theory are used. For any positive integer $m$ ,the $mth$ primitive unit root is added to $\mathbb{Q}$ to obtain the $mth$ circular domain, which is denoted as $K=\mathbb{Q}(\zeta_m)$ .Similarly, the $mth$ divided ring is recorded as $R=\mathbb{Z}(\zeta_m)$ .If there is a series of integral coefficient polynomials with first 1,the root of the integral coefficient polynomials is $\omega_m^{\ j}$ ,and the least number of them is called circular polynomials, which is denoted as circular polynomials: $\Phi_m(X)=\prod_{i\in\mathbb{Z}_m^*}(X-\omega_m^{\ i})\in \mathrm{Z}[X]$ .where $\omega_m\in\mathbb{C}$ is $mth$ primitive unit root and there is natural isomorphism $K\cong\mathbb{Q}(X)/\Phi_m(X)$ , $R\cong\mathbb{Z}(X)/\Phi_m(X)$ .Regarding $K$ as a $\varphi(m)$ dimensional space over $\mathbb{Q}$ ,then $(\zeta_m^j)_{j\in[\varphi(m)]}$ is called a set of power basis on $K$ where the Euler function $\mathbf{p}=(1,\zeta_m,\ldots,\zeta_m^{\varphi(m)-1})^{\mathrm{T}}$ is less than $m$ and is prime to $m$ .The trace function $Tr=Tr_{K/\mathbb{Q}}:K\to\mathbb{Q}$ is defined as the sum of homomorphisms of all rings from $K$ to $\mathbb{C}$ $Tr(a)=\sum_i\sigma_i(a)$ .For arbitrary $a,b\in K$ ,there is $Tr(a\cdot b)=\sum_i\sigma_i(a)\sigma_i(b)$ .On the basis of the trace function ,give the definition of dual $R^\vee$ of $R$ is given, $R^\vee=\{a\in K:\subseteq Z\}\in R$ , table 1as follows.

Table 1. Algebraic Notations

| Notation | **Description** |
|---|---|
| $m$, $n$, $\hat{m}$, $\mathbb{Z}_m^*$ | The cyclotomic index is $n=\varphi(m)$ ; 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 $m$th cyclotomic numbe field $K$ , $\Phi_m(X)=$ $\prod_{i\in\mathbb{Z}_m^*}\left(X-\omega_m^i\right)\in \mathrm{Z}[X]$ is $m$th cyclotomic polynomial. |
| $K_{\mathrm{R}}$ | $K_{\mathrm{R}}=K\otimes\mathbb{R}$ |
| $\sigma_i:K\to \mathrm{C}, i\in \mathrm{Z}_m^*$ | $\sigma_i$ is $K\to\mathbb{C}$ auto-homomorphic, $i\in \mathrm{Z}_m^*, \sigma_i(\zeta_m)=\omega_m^i$ . |

| | |
|---|---|
| $R=\mathrm{Z}(\zeta_m)\cong \mathrm{Z}[X]/\Phi_m(X)$ | The ring of integers of $K$. |
| $R_q$ | For positive integers $q\geq 2, R_q=R/qR$. |
| $Tr(\cdot):K\to\mathrm{Q}$ | The trace $Tr(a):K\to\mathrm{Q}$, for $a\in K, Tr(a)=\sum_i \sigma_i(a)$. |
| $R^\vee, R^\vee=\langle t^{-1}\rangle, g, t\in R$ | The dual of $R$ is $R^\vee=\{a\in K: Tr_{K/\mathrm{Q}}(aR)\subseteq \mathrm{Z}\}$ ,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, $\boldsymbol{p}=(\zeta_m^j)_{j\in[n]}=(1,\zeta_m,\ldots,\zeta_m^{n-1})\in K^{[n]}$ over $K$ is powerful basis. |

### *2.2. Ring Learning with Errors*

**Definition 1 Ring Learning with Errors**

Let $\Psi$ be a family of distribution over $K_{\mathrm{R}}$. 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 Decision Ring Learning with Errors**

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 $R_q\times(K_{\mathrm{R}}/qR^\vee)$.

**Theorem 1**

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

## 3. Homomorphic Encryption Construction

### *3.1. Somewhat Homomorphic Encryption Scheme*

Somewhat homomorphic encryption **RSHE** include three polynomial time algorithms which is key generation algorithms **KeyGen**, encryption algorithms **Enc** and decryption algorithms **Dec**. Construction as follows: $\lambda$ is safety parameter; $p$ is a positive integer and $q=\mathrm{poly}(n)\geq 2$ are mutually prime.

**RSHE.KeyGen** $(1^\lambda)$: Sample a noise $s'\leftarrow\lfloor\psi\rceil_{R^\vee}$, a ring element $a_1\leftarrow R_q^\vee$ in uniform random and noise $x\leftarrow\lfloor\psi\rceil_{R^\vee}$,output $s=t\cdot s'\in R$ as private key and $pk\triangleq(-a_0,a_1)$ as public key which $a_0$ donate as $a_0=a_1s+px$.

**RSHE.Enc** $(pk,\mu)$: Input public $pk$, plaintext $\mu\in R_p$,and choose rings $u\leftarrow R_q$ elements which polynomial coefficients is $\{0,\pm1\}$, $f\leftarrow\lfloor\psi\rceil_{R^\vee}$, $e\leftarrow\lfloor p\cdot\psi\rceil_{t^{-1}\mu+pR^\vee}$. Compute $\rho=a_0u+e$, $v=a_1u+pf$. Output ciphertext $ct\triangleq(\rho,v)$.

**RSHE.Dec** $(sk,ct)$: Input ciphertext $(\rho,v)$ and private key $s$. Compute $\rho+vs=-pxu+e+pfs$,

$\tilde{e} = -pxu + pfs \in R_q^\vee$ and $e = (\rho + vs) \bmod p$. Output plaintext $\mu = t \cdot e \bmod pR$.

If there are two messages $\mu, \mu' \in R_p$, the noisy is sampled from distribution $e \leftarrow \lfloor p \cdot \psi \rceil_{t^{-1}\mu + pR^\vee}$, $e' \leftarrow \lfloor p \cdot \psi \rceil_{t^{-1}\mu' + pR^\vee}$. Output ciphertext $ct = (\rho, v)$ and $ct' = (\rho', v')$, the polynomials for Y are $c(Y) = \rho + vY$, $c'(Y) = \rho' + v'Y$ which satisfy $c(s) = \rho + vs = e + \tilde{e}$, $c'(s) = \rho' + v's = e' + \tilde{e}'$.

**RSHE.Add**:

$c(Y) + c'(Y) = \rho + vY + \rho' + v'Y = \rho + \rho' + (v + v')Y$ $\mathrm{Dec}_s\left[c(Y) + c'(Y)\right] = \rho + vs + (\rho' + v's) = e + \tilde{e} + e' + \tilde{e}'$,

$e + \tilde{e} + e' + \tilde{e}' \in R_q^\vee$, if $\| e + \tilde{e} + e' + \tilde{e}' \| < q / (2\sqrt{n})$, the decryption correct. Output plaintext $\mu + \mu' = t \cdot (e + e') \bmod pR$.

**RSHE.Mult**:

$c(Y) \cdot c'(Y) = (\rho + vY) \times (\rho' + v'Y) = \rho\rho' + (\rho v' + v\rho')Y + vv'Y^2$, $\mathrm{Dec}_s\left[c(Y) \cdot c'(Y)\right] = (e + \tilde{e})(e' + \tilde{e}')$

$= ee' + (e\tilde{e}' + \tilde{e}e' + \tilde{e}\tilde{e}')$. $e^* = ee' + (e\tilde{e}' + \tilde{e}e' + \tilde{e}\tilde{e}') \in (R_q^\vee)^2$, if $\| e^* \| < q / (2\hat{m}\sqrt{n})$, the decryption correct. After once multiplication, messages is $\boldsymbol{c}_{\mathrm{mult}} = (\rho\rho', \rho v' + \rho' v, vv')$, and private key is $\boldsymbol{s} = (1, s, s^2)$. The decryption can be seen $\langle \boldsymbol{c}_{\mathrm{mult}}, \boldsymbol{s} \rangle \bmod p = e \cdot e'$. Output plaintext $\mu\mu' = t^2 \cdot (e \cdot e') \bmod pR$.

### *3.2.Fully homomorphic encryption using Key Switching*

After once homomorphic multiplication, ciphertext vector is $\boldsymbol{c}_{\mathrm{mult}} = (\rho\rho', \rho v' + \rho' v, vv')$, the ring elements add to three. It can be predict, with the continuation of homomorphic multiplication, the ciphertext elements multiply exponential growth. With the key-switching technology, the ciphertext can be stay two ring elements.

If $\mathrm{I} = (R^\vee)^2$, the homomorphic multiplication ciphertext vector is $\boldsymbol{c} \in \mathrm{I}_q^3$, and private key is $\boldsymbol{s} = (1, s, s^2) \in R_q^3$. There exist a relation about $\langle \boldsymbol{c}, \boldsymbol{s} \rangle = e \bmod q\mathrm{I}$, which $e \leftarrow t^{-2}\mu + p\mathrm{I}$, $\boldsymbol{g} = (1,2,4,...,2^{b-1}) \in Z_q^b$, and $\boldsymbol{G} = \boldsymbol{I} \otimes \boldsymbol{g}^{\mathrm{T}} \in Z_q^{3 \times 3b}$. $\boldsymbol{I}$ is unit matrix, $b = \lceil \log q \rceil$. Choose key-switching keys $s' \leftarrow R$. The key switching technology as follows:

- owing to $\langle \boldsymbol{c}, \boldsymbol{s} \rangle = e \bmod q\mathrm{I}$, multiply the ciphertext vector by m, $\langle t \cdot \hat{m} \cdot \boldsymbol{c}, t^{-1}\boldsymbol{s} \rangle = \hat{m} \cdot e \bmod qR^\vee$;
- If $\boldsymbol{y} = t \cdot \hat{m} \cdot \boldsymbol{c} \in R_q^3$, compute $\boldsymbol{G}\boldsymbol{x} = \boldsymbol{y} \in R_q^3$ to get $\boldsymbol{x}$;
- for $i \in [3b]$, encrypt 0 R-SHE.Enc $(pk, 0)$, get ciphertext $(\boldsymbol{\rho}^{(i)}, \boldsymbol{v}^{(i)})$, by this way compute $3b$ times get vector $\boldsymbol{\rho} = (\boldsymbol{\rho}^{(i)})_{i \in [3b]}$, $\boldsymbol{v} = (\boldsymbol{v}^{(i)})_{i \in [3b]}$;
- Choose noisy $\boldsymbol{f}^{(i)} \leftarrow \lfloor p \cdot \psi \rceil_{pR^\vee}$, $\boldsymbol{f} = (\boldsymbol{f}^{(i)})_{i \in [3b]}$ satisfy $c(\boldsymbol{s}') \bmod p = \boldsymbol{f}^{(i)}$, which $\langle \boldsymbol{x}, \boldsymbol{f} \rangle$ rather small;
- The auxiliary information $\delta = (\boldsymbol{h}^{(i)}, \boldsymbol{v}^{(i)})_{i=0}^{[3b]}$, $\boldsymbol{h}^{(i)} = \boldsymbol{\rho}^{(i)} + (t^{-1}\boldsymbol{G}\boldsymbol{s})^{(i)} \bmod qR^\vee$, the ciphertext after key-switching technology is $c' = (\rho', v')$, the $\rho' = \sum_{i \in [3b]} \boldsymbol{h}^{(i)} \boldsymbol{x}^{(i)} = \langle \boldsymbol{x}, \boldsymbol{\rho} \rangle + \langle \boldsymbol{x}, t^{-1}\boldsymbol{G}^{\mathrm{T}}\boldsymbol{s} \rangle$, $v' = \boldsymbol{x}\boldsymbol{v}$, give $\boldsymbol{s}'$ into $c(Y)$:

$c(\boldsymbol{s}') = \rho' + v'\boldsymbol{s}' = <\boldsymbol{x}, \boldsymbol{\rho}> + <\boldsymbol{x}, t^{-1}\boldsymbol{G}^{\boldsymbol{T}}\boldsymbol{s}> + \boldsymbol{x}\boldsymbol{v}\boldsymbol{s}' \bmod p$

$= \langle \boldsymbol{x}, \boldsymbol{f} \rangle + \langle \boldsymbol{x}, t^{-1}\boldsymbol{G}^{\mathrm{T}}\boldsymbol{s} \rangle = \langle \boldsymbol{x}, \boldsymbol{f} \rangle + \hat{m} \cdot e \bmod qR^\vee$ $g \cdot \mu = t \cdot \hat{m} \cdot e \bmod pR$, $e^* = \langle \boldsymbol{x}, \boldsymbol{f} \rangle + \hat{m} \cdot e \in R_q^\vee$, $\langle \boldsymbol{x}, \boldsymbol{f} \rangle$ gets.

### *3.3. Fully Homomorphic Encryption Scheme*

The RFHE scheme include four polynomial time algorithms, and **KeyGen, Encrypt, Enc, Decrypt and Eval**. Based on the idea of full homomorphism encryption structure proposed by Brakerski et al. A fully homomorphism encryption scheme R-FHE based on RLWE is given as 'Figure2'.

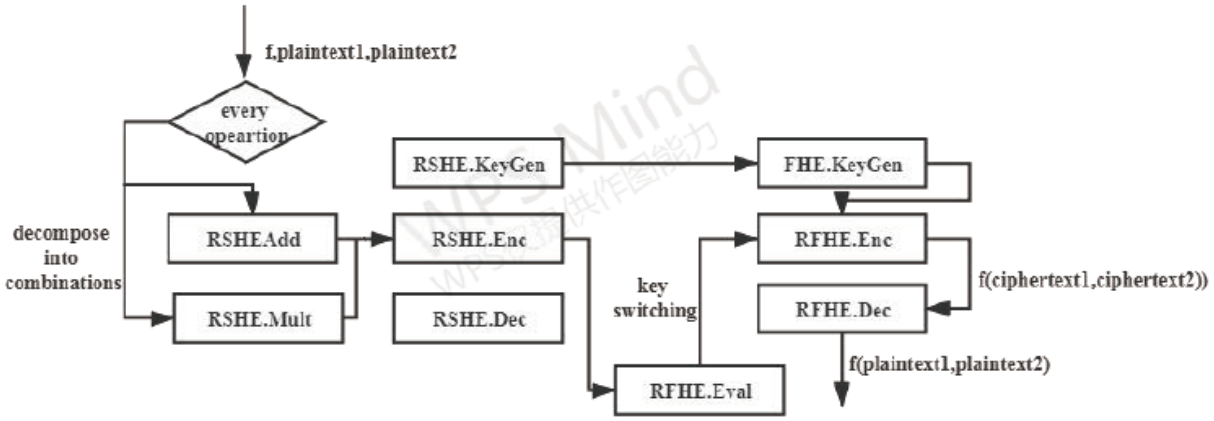



Figure 2. key-swtiching schematic diagram

**RFHE.KeyGen** $(1^{\lambda},1^{L})$ : input security parameters $\lambda$ , and the number of layers of circuit $L$ that the system is required to rocess. Select $L+1$ element $s_0',s_1',...,s_L' \leftarrow \lfloor \psi \rceil_{R^\vee}$ calculate $s_i = t \cdot s_i' \in R$ uniformly randomly select ring element $a_1 \leftarrow R_q^\vee$ and noise $x \leftarrow \lfloor \psi \rceil_{R^\vee}$ , to calculate $a_0 = a_1 s + px$ according to section 3.2 calculate the evaluation key $evk = \{\delta_{i \to i+1}\}_{i=0}^{L}$ out public key $pk \triangleq (-a_0, a_1)$ , private key $sk \triangleq (s_0, s_1, ..., s_L)$ and $evk$ as evaluation key.

**RFHE-Enc** $(pk,\mu)$ : use RSHE-Enc $(pk,\mu)$ , output ciphertext $ct \triangleq (\rho, v)$ , in the system Use additional information to identify the circuit layer in which the ciphertext is located , such as $ct_i \triangleq (\rho_i, v_i, i)$ where $i$ stands for ciphertext layer .

**RFHE.Dec** $(ct_i, s_i)$ : the ciphertext $ct_i = (\rho_i, v_i, i)$ and the private key are decides by the layer of ciphertext , compute $e_i = (\rho_i + v_i s_i) \bmod p \in (R_q^\vee)^i$ , output the plaintext is $\mu = t^i \cdot e_i \bmod pR$ .

**RFHE.Eval** $(f, ct_1, ..., ct_t, evk)$ : every $f$ can be represented a combination of homomoprhism multiplication and addition operation. Homomoprhic addition directly calls add algorithm **RSHE.Add**. When performing homomorphic multiplication, you must first obtain this level of evaluation key and then call algorithm **RSHE.Mult.**

## 4.Security Proof and Efficiency Analysis

### *4.1. Security Proof*

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

**Proof**. The proposed scheme RFHE would be verified based on Game, $Adv_{\mathrm{Game}}[\mathrm{A}]$ defined as the attacker's advantage in the following game.

**Game0**: Game0 is standard IND - CPA game, namely the attacker $\mathrm{A}$ chooses a challenge identity $id^*$ and selects two challenges plaintexts $\{\mu_0^*, \mu_1^*\}$ from plaintext space at random to the challenger $\mathrm{C}$ . $\mathrm{C}$ computes the corresponding evaluation key $evk_{id^*}$ , generates challenge ciphertext $c^*$ and hands them over to the attacker $\mathrm{A}$ . The attacker guesses the plaintext. In this game, the advantage of $\mathrm{A}$ is:

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

**Game 1**: Game1 changes the generation of the generation of public key in Game0. In Game 1 , $pk$ have no longer available from $a_1 s + px$ , but choose from the uniformly random distribution over $R_q^\vee$ . The attacker is unable to distinguish between Game0 and the modified Game 1, so:

$$|Adv_{\mathrm{Game1}}[\mathrm{A}] - Adv_{\mathrm{CPA}}[\mathrm{A}]| = 0 \quad (2)$$

**Game 2**: Game2 is as same as Game 1, where the difference is that the generation of evaluation key $evk = \{\delta_{i\to i+1}\}_{i=0}^{L}$. The challenger randomly selects a group $evk_{id^*}$ from $R_q^{3b}$ to the attacker. So the attacker's advantage difference between Game2 and Game1 is equal to successfully solve the L instances of the probability $\mathrm{DRLWE}_{n,bj,q,\chi}$ :

$$|Adv_{Game2}[A] - Adv_{Game1}[A]| = 1 - \prod_{i=0}^{L}(1 - Adv_{\mathrm{DRLWE}_{n,3b,q,\chi}}[A_i]) \tag{3}$$

**Game 3**: Game 3 and Game 2 differ in the encryption algorithm. The calculation of the ciphertext $\rho$ is not through $\rho = a_0\mu + e$ but from a random uniform distribution $R_q^{\vee}$. The attacker's advantage difference between Game3 and Game2 is equal to its advantages of solving the problem $\mathrm{DRLWE}_{n,l,q,\chi}$ :

$$|Adv_{Game3}[A] - Adv_{Game2}[A]| = \mathrm{DRLWE}_{n,l,q,\chi}Adv[A] \tag{4}$$

**Game 4**: In this game , Challenger $C$ changes the generation of ciphertext , no longer calculate $c^* = (\rho, v)$ and selects challenge ciphertext from uniform distribution over $R_q^{\vee} \times R_q^{\vee}$ at random. The public key $a_1$ choose from the uniform distribution over $R_q^{\vee}$, therefore $v = a_1\mu + pf$ is a instance of $\mathrm{DRLWE}_{n,1,q,\chi}$ problem, namely

$$|Adv_{Game4}[A] - Adv_{Game3}[A]| = \mathrm{DRLWE}_{n,1,q,\chi}Adv[A] \tag{5}$$

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 $Adv_{Game4}[A] = 0$

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

### *4.2. Efficiency Analysis*

Let $\psi$ a continuous Gaussian distribution (parameter $s' = \sqrt{2\pi}\sigma \geq 1$ ),and the bound (defined by Euclidean norm )is $s'\sqrt{n}$ .Scatter $\psi$ to $R^{\vee}$ get $\lfloor\psi\rceil_{R^{\vee}}$ the bound value is increased to $l$ ,where $l = (s' + s_1(\mathbf{d}))\sqrt{n}$ .In order to ensure the safety and correctness of LWE, two aspects are mainly considered in the parameter selection of this experiment.

Firstly, in order to ensure the security and complexity of the system, according to the literature The discriminant attacks are given and combined with the literature .Assuming that the ratio of attack time to discrimination advantage is at least $2^{\lambda}$ there is a relationship $n \geq \frac{\log(q/\sigma)(\lambda+110)}{7.2}$ .Set the initial noise to $E_0 = -pxu + e + pfs$ .The bound of noise $E_0 \leq -pl\sqrt{n/2} + l + pl^2$ In order to decrypt correctly. the condition must be satisfied $q > 2E_0\sqrt{n}$ .

If the safety parameter $\lambda = 128$ a fixed obtain a number of groups $(n,q)$ .In the case of $p = 2,128,1024$ ,refer to the existing BV11b system (n must be a curtain of 2).In the R-FHE system, $n$ can be taken as any positive integer and three sets of values $(n,q)$ are obtained respective .Using magma software to test the encryption and decryption time of the two systems, the experiment running in WIN7 32-bit operating system ,CPU for multi-core intel core i5-2400 processor, main frequency 3.10GHz,internal storage is 4GB,tables 2 as follows. With the experimental results in Table 2, it can be seen that when $p = 2$ ,the BV11b parameter can be taken as minimum $n = 512$ ,but because the noise of R-FHE is taken from $R^{\vee}$ ,the encryption time is slightly amaller than that of R-FHE system; When $p = 128,1024$ ,because the BV11b parameter n must be 2 square screen ,in order to meet the security $n = 1024$ , R-FHE can take any positive integer, the minimum can be $n = 810,910$ , the encryption time of the system is and less than 45%and 46%that of BV11b respectively.

Table 2. Efficiency Comparison.

| | $p$ | $m$ | $n$ | $\lceil \log p \rceil$ | Enc (*ms*) | Dec(ms） |
|---|---|---|---|---|---|---|
| **BV11** | 2 | 1024 | 512 | 19 | 81 | 2 |
| | 128 | 2048 | 1024 | 27 | 155 | 4 |
| | 1024 | 2048 | 1024 | 30 | 162 | 4 |
| **RFHE** | 2 | 577 | 576 | 19 | 77 | 2 |
| | 128 | 811 | 810 | 26 | 84 | 3 |
| | 1024 | 911 | 910 | 29 | 87 | 3 |

## 5. Conclusion and Future Work

In this letter, an efficient fully homomorphic encryption scheme is presented based on ring learning with errors in arbitrary cyclotomic rings. Particularly, a “somewhat homomorphic encryption” scheme is firstly proposed based on ring learning with errors. And then, a novel fully homomorphic encryption scheme is further presented using key-switching. With theoretical and experimental verification, the proposed scheme which has advantage of high efficiency of encryption and decryption. The security of our scheme strictly reduces to hardness of decision ring learning with errors problem in the random oracle model.

Moreover, RFHE using RLWE[10-11] has efficient encryption and decryption. Especially the remarkable cloud computing [12-13] and relation information retrieval [14], will introduce the encryption method of fully homomorphic encryption in future research.

## Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (61872448) and Shaanxi province Natural Science Foundation（2018JM6017）.

## References

[1] Gentry C. Fully homomorphic encryption using ideal lattices[C]//STOC, 2009, 9: 169-178.
[2] Brakerski Z,Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE[J]. SIAM Journal on Computing, 2014, 43(2): 831-871.
[3] Coron J S, Naccache D, Tibouchi M. Public key compression and modulus switching for fully homomorphic encryption over the integers[C]//Proceedings of Conference on Advances in Cryptology.Berlin,Germany: Springer,2012: 446- 464.
[4] Coron J S., Avradip Mandal, David Naccache, Mehdi Tibouchi. Fully homomorphic encryption over the integers with shorter public keys[A]. Proceedings of the 31st Annual International Cryptology Conference[C], Santa Barbara, California, USA, 2011.
[5] Coron J S, Lepoint T, Tibouchi M. Scale-invariant fully homomorphic encryption over the integers[M], Public-Key Cryptography–PKC 2014. Springer Berlin Heidelberg, 2014: 311-328.
[6] 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.
[7] 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.
[8] Kang YJ, Gu CX, Zheng YH, Guang Y. Identity-Based fully homomorphic encryption from eigenvector. RuanJian Xue Bao/Journal of Software, 2016,27(6):1487 1497 (in Chinese). http://www.jos.org.cn/1000-9825/4991.html
[9] WANG W L, HU B. Multi-identity-based fully homomorphic encryption from obfuscation[J]. Journal of Cryptologic Research, 2017, 4(2): 165–175.
[10] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without

bootstrapping[C]. Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. ACM, 2012: 309-325.
[11] Brakerski Z, Gentry C, Halevi S. Packed ciphertexts in LWE-based homomorphic encryption[M], Public-Key Cryptography–PKC 2013. Springer Berlin Heidelberg, 2013: 1-13.
[12] Huang RW, Gui XL, Yu S. Computable encryption method supporting privacy protection in cloud environment, Journal of Computer Science, 2011, 12(34): 2391-2402.
[13] Wang C, Cao N, Li J, et al. Secure ranked keyword search over encrypted cloud data[C].Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010: 253-262.
[14] Gu C, Zhu Y, Pan H. Efficient public key encryption with keyword search schemes from pairings[C].Information Security and Cryptology. Springer Berlin Heidelberg, 2008: 372-383.