Identity-based Fully Homomorphic Encryption from
Ring-LWE: Arbitrary Cyclotomics, Tighter Parameters, Efficient Implementations

Dan Xin*, Linna Yang, Lina Yan and Xiaofeng Song
Test Training Base, Xi’ an Shaanxi China
*Corresponding author

Abstract—Fully homomorphic encryption allows for data to be stored and processed in an encrypted format, which gives the cloud computing provider a way to process data without even knowing what the data is. At present, most identity-based homomorphic encryption schemes from ring learning with errors have focused on the special classes of rings such as power-of-two cyclotomic rings, which significantly limits its application efficiency in cloud computing. To solve this problem, we construct the first identity-based fully homomorphic encryption scheme from ring learning with errors, which has advantage of high efficiency of encryption and decryption. The security of our scheme is equal to hardness of decision ring learning with errors problem in the random oracle model.

Keywords—fully homomorphic encryption; cyclotomic rings; cloud computing; ring learning with errors

I. INTRODUCTION

Fully homomorphic encryption is a new cryptographic which users can compute encrypted data and have no need to decrypt. This encryption technology gives a new solution for many problems, such as privacy protection problem on cloud computing, private information retrieval, etc. 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[2-4] based on different kinds of mathematical problems has been constructed. But the public keys of existing schemes generally is too large, and key management complexity has greatly influenced the application efficiency of scheme in cloud computing. Identity-based encryption[5] utilizes user’s identity(such as the E-mail address)as the scheme’s public key and the trusted third party generate private key, which has advantages over independent of the public key certificate management. Based on this idea,in CRYPTO 2010,Naccache[6] considered the design of identity-based fully homomorphic encryption scheme as one of the important problems to be solved.

Based on the learning with errors [8] problem, Gentry[7] construct an identity-based homomorphic encryption scheme, which only supports several times the homomorphism addition and multiplication. In 2013, Gentry[11] proposed an identity-based fully homomorphic encryption scheme using approximate eigenvectors, but this scheme ciphertext expansion serious. GUANG Yan[13] design an identity-based fully homomorphic encryption with preimage sampling trapdoor one-way function to extract the private key, but this scheme can’t support multi-bit encryption.

Using key-switching technology, we construct an identity-based fully homomorphic encryption scheme. In this paper, we innovatively used non-power-of-two cyclotomic rings, not using power-of-two cyclotomic rings as usual. Finally, the security of our scheme is equal to hardness of decisional ring learning with errors problem in the random oracle model.

II. PRELIMINARIES RING LEARNING WITH ERRORS

Lyubashevsky [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.

First two distributions are given: 1) for point $e$ as the center, the standard deviation $\frac{e}{\sqrt{2\pi}}$ of the gaussian distribution $D_x$, when $e = \theta$, in a short $D_x$, and the corresponding discrete gaussian distribution for lattice $A$ point $e$ as the center, $D_{A,e}$ when $e = \theta$, for short $D_{A,e}$. 2) For secret value $s \in R_q^*$ (or $R_q^*$), define a RLWE distribution $A_{\omega}$ over $R_q^* \times (K_q / qR^*)$ the variable is in the form of $(a,b = a \cdot s + e \mod qR^*)$, where each $a$ is uniformly random from distribution $R_q^*$, choosing $e$ from distribution $\Psi$.

Definition1 (RLWE, Search): Let $\Psi$ be a family of distribution over $K_q$. The search version of the ring-LWE problem, denoted RLWE$_{\omega,e}$, is defined as follows: give access to arbitrarily many independent samples from $A_{\omega}$ for some arbitrary $s \in R_q^*$ and $\psi \in \Psi$, find $\omega'$. 

Copyright © 2019, the Authors. Published by Atlantis Press. 
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).
Definition 2 (RLWE, Average-Case Decision): The average-case decision version of the ring learning with errors problem, denoted DRLWE, is to distinguish with non-negligible advantage between arbitrarily many independent samples from $A_{\omega}$, where $s \sim R_q$ is uniformly random, and the same number of uniformly random and independent samples from $R \times \langle K_q / qR_q \rangle$.

Theorem 1 Let $K$ be the $m$th cyclotomic number field having dimension $n = \varphi(m)$ and $R = O_q$ be its ring of integers. Let $a = a(n) > 0$, and let $q = q(n) \geq 2$, $q \equiv 1 \mod m$. Then there is a polynomial-time quantum reduction from $\tilde{O}(\sqrt{n} / \alpha)$-approximate SIVP (or SVP) on ideal lattices in $K$ to the problem of solving DRLWE given only $l$ samples, where $\Psi$ is the Gaussian distribution $D_{\alpha}$, for $\xi = a \cdot (n! / \log(n))^u$.

In application it is often useful to work with a version of ring-LWE whose error distribution is discrete. If RLWE$_{e,v}$ is hard with some number $l$ of samples, then so is the average distribution $D_{\alpha,v}$ and uniform distribution $R_{e,v}$, as is hard as RLWE$_{e,v}$.

III. CONSTRUCTION

Let security parameters $\kappa$, positive integer $m = \kappa$, index $n = \varphi(m)$, prime $q = q(n) \geq 2$, $l \geq 5n \log q$, powerful basis $P$ over $R$, hash function $H : \{0,1\} \rightarrow Z_q^{[n]}$. The scheme is described as follows.

A. Somewhat Homomorphic Encryption Scheme

IBFHE-Setup ($\nu^\prime$): input security parameters $\kappa$, invoke TrapGen($\nu^\prime$) to generate a full-rank set $S$ as master private key, uniformly random matrix $A \sim Z_q^{[n] \times [\kappa]}$ as master public key and correspond one-way trapdoor functions with preimage sampling $f_s$ as a pair of public parameters.

IBFHE-Extract ($A,S,id$): input public parameters, master private key, identity and powerful basis $P$ over $R$, compute $U = H(id) \sim Z_q^{[\kappa]}$, let $U = (u_1, \ldots, u_n)$, $e = f_s(u_i)$, using the inverse function with trapdoor $S$, $E = (e_1, \ldots, e_n) \in Z_q^{[n]}$, output private key $e = Ep \in R_q^\kappa$.

IBFHE-Enc ($A,id,\mu$): input master public key, identity and message $\mu \in R_q$, do:

- Compute $U = H(id) \sim Z_q^{[\kappa]}$, $u = puU \in R_q$; Select a uniformly random $r \sim R_q$ and $x^{(0)}, x^{(1)} \sim [P, \Psi]$,

- Compute $\rho = ru + x \in R_q$, where $x \sim [P, \Psi]$, $v = (-pB + px) \in R_q^\kappa$; output ciphertext $c = (\rho, v) \in R \times R_q^\kappa$.

IBFHE-Dec ($c,e$): compute $x = (\rho + ve \mod q) / p \mod R$, output plaintext $\mu = t \cdot x \mod pR$.

B. Homomorphic Operations

The correctness of our scheme is as follows: there is a polynomial $c(Y) = \rho + vY$ and the decryption process can be seen as $c(e) = x + px$.

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

Give ciphertexts $c = (\rho, v)$, $c' = (\rho', v')$, which encrypts two messages $\mu, \mu' \in R_q$, with $x \sim [P, \Psi]$ and $x' \sim [P, \Psi]$ respectively. There exist two decrypt polynomials $c(Y) = \rho + vY$, $c'(Y) = \rho' + v'Y$.

IBFHE-Add: $c(Y) + c'(Y) = \rho + vY + \rho' + v'Y = \rho + \rho' + (v + v')Y$.

When the variant $Y$ is the private key: $Dec_y[c(Y) + c'(Y)] = x + x' + px + px'$. If noise $\|x + x' + px + px'\| < q / 4$, decryption correctly. We can obtain $x + x'$ which $Dec_y[c(Y) + c'(Y)]$ module $P$ and compute $\mu + \mu' = t \cdot (x + x') \mod pR$.

IBFHE-Mult:

$c(Y) \cdot c'(Y) = (\rho + vY) \times (\rho' + v'Y) = \rho \rho' + (\rho v' + \rho' v)Y + vY v'Y$.

When the variant $Y$ is the private key $e$:

$Dec_y[c(Y) - c'(Y)] = x + 2 \rho' s e + px e' + x' p x e$. 


let $e' = 2p\cdot x\cdot e\cdot x' + x\cdot p\cdot x', \text{ if the noise } |x\cdot x' + e'| < q/14$, decryption correctly, obtain the results $x \cdot x'$ when $\text{Dec}_0(c(y)) = \text{Dec}_0(c(y)) \mod p$, compute $\mu' = t \cdot (x \cdot x') \mod pR$. After once homomorphism multiplication, the ciphertext $e_{\text{cwt}} = (p\cdot e', \rho\cdot e', \rho\cdot v, v \otimes v')$.

C. Key-switching

After a homomorphism multiplication, the dimension of ciphertext improve to $t^2 + 1 + 1$ from $t + 1$. As the homomorphism multiplication continues, the size of ciphertext goes into exponential growth. With the cyclotomic polynomial algebra, choose a good basis $L$ that $\lambda^L(G)$ has a good basis $\{\hat{e}, \hat{f}\}$, which mentioned in the paper [15], satisfying $Gx = y \in R^q$. At last, select the target private key $x \leftarrow R^q$.

For $i \in [b]$, $p = (\rho^i, \rho^0)_{\in [b]}$, $V = (v_1, ..., v_b)$, compute IBSHE-Enc $(A, id, 0) = (\rho^i, v)$, $c(s) \mod p = f^i \cdot e' - [p \cdot \mu'] \cdot v$, $f = (\rho^i, v)$ and $\langle x, f \rangle$ is sufficient short. let $\delta = (h^i, v)_{\in [b]}$, $h^i = \rho^i + (e^i \cdot G^i s) \mod qR^e$.

The target ciphertext $c' = (\rho^i, v')$,

$$c'(x') = \rho' + v' \cdot x' = \langle x, f \rangle + \hat{m} \cdot e \mod qR^e$$

Which the noise $c' = (x, f) + \hat{m} \cdot e \in R^e$, compute message

$$t \cdot \hat{m} \cdot e = g \cdot \mu \mod pR$$

D. Identity-Based Fully Homomorphic Encryption Scheme

IBFHE-Setup $(1^t, 1^t)$: input security parameters $\kappa$, as well as the supporting circuit layer $L$, invoke IBFHE-Setup $(1^t)$ algorithm to output public parameters and the master private key.

IBFHE-Extract $(A, S, id)$: invoke IBSHE-Extract $(A, S, id)$ algorithm to extract private key $e^i$. Set $e^i = e^i$, select L vectors $e_1, e_2, ..., e_L$ in uniform distribution over $R^{[q]}$ at random and calculate $evk_{id} = \{\delta^i_{\text{v},id} \}_{i \in [l]}$ as the evaluation key.

IBFHE-Extract $(A, id, \mu)$: using IBSHE-Extract $(A, id, \mu)$ output ciphertext $c = (\rho, v, 0)$, where 0 means circuit’s level.

IBFHE-Dec $(c, e)$: for ciphertext $c = (\rho, v, e)$, using the private key $e$, to generate $c_t = (\rho, v, e \mod q) \mod qR^e$ and output message $\mu = t \cdot x \mod pR$.

IBFHE-Eval $(f, c_1, ..., c_n, evk)$: any $f$ operation can be represented as arbitrary combinations of homomorphism multiplication and addition. The ciphertext form in operation process, sign a 1 show the "level" of the ciphertext. Homomorphism addition directly invoke IBSHE- Add algorithm. When execute homomorphism multiplication, we must firstly obtain the evaluation key $\delta_{t \cdot x}^i$, then call IBSHE-Mult algorithm.
E. Security Proof and Efficiency Analysis

Security Proof: Theorem 2 let \( m = k \), \( n = \varphi(m) \), \( q = q(n) \geq 2 \), \( l \geq 5 \log q \), the above cryptosystem is IND-CPA secure in random oracle model assuming the hardness of DRLWE\(_{n,l,q\cdot r}^v\).

Proof. We prove the lemma based on game, \( Adv_{Game}[\mathcal{A}] \) 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:

\[
Adv_{Game}[\mathcal{A}] = |Pr[\mathcal{A}(id^0,IBFHE-Enc(A,id^0,\mu^0_0)=1] - Pr[\mathcal{A}(id^1,IBFHE-Enc(A,id^0,\mu^1_0]=1]|\]

Game 1: Game1 changes the generation of \( H(id^0) \) in Game0. In Game 1, \( H(id^0) \) have no longer available from the access list in random oracle model \( H(\cdot) \), but choose from the uniformly random distribution over \( Z_{q^{\ell}} \). The attacker is unable to distinguish between Game0 and the modified Game 1, so:

\[
|Adv_{Game_1}[\mathcal{A}] - Adv_{Game}[\mathcal{A}]| = 0
\]

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 \( \mathbb{R}_{q^{\ell}}^v \) to the attacker. So the attacker’s advantage difference between Game2 and Game1 is equal to successfully solve the L instances of the probability DRLWE\(_{n,l,q\cdot r}^v\):

\[
|Adv_{Game_2}[\mathcal{A}] - Adv_{Game}[\mathcal{A}]| = 1 - \prod_{j=0}^{L}(1 - Adv_{DRLWE_{n,l,q\cdot r}^v}[\mathcal{A}])
\]

Game3: Game 3 and Game 2 differ in the encryption algorithm. The calculation of the ciphertext \( v \) is not through \( v = (\rho^T A + px) \) but from a random uniform distribution \( \mathbb{R}_{q^{\ell}}^v \). The attacker’s advantage difference between Game3 and Game2 is equal to its advantages of solving the problem DRLWE\(_{n,l,q\cdot r}^v\):

\[
|Adv_{Game_3}[\mathcal{A}] - Adv_{Game_2}[\mathcal{A}]| = DRLWE_{n,l,q\cdot r}^v Adv[\mathcal{A}]
\]

Game4: In this game, Challenger \( C \) changes the generation of ciphertext, no longer calculate \( c^* = (\rho, v) \) and selects challenge ciphertext from uniform distribution over \( R_{q^{\ell}}^v \) at random. The public key \( u \) choose from the uniform distribution over \( R_q^\ell \), so IBFHE is IND-CPA secure. Therefore,

\[
Adv_{Game_4}[\mathcal{A}] = 0
\]

F. 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 \( R_q^\ell \) can be achieved \( O(\log n) \).

Table 1 shows the comparison on computing efficiency of two scheme in the same parameter approximation SVP cases, for security parameters \( k \) take 100, the paper[18] system \( n = k^2 \), \( q \approx 2^{65} \). Our scheme IBFHE, \( m \) can take any positive integer, \( m = k \), \( n = \varphi(m) \), prime \( q = 1 \mod m \).
### TABLE I. COMPUTING EFFICIENCY COMPARISON

| Scheme  | $p$ | $n$ | $[\log q]$ | Certificate | Enc (module $q$) | Dec (module $q$) | Ciphertext (module $q$) |
|---------|-----|-----|-------------|-------------|-----------------|-----------------|---------------------|
| paper[18] | 2   | 10000 | 30 | no | $1.5 \times 10^6$ multi | $1.5 \times 10^6$ multi | 42.9 Mb |
| IBFHE   | 2   | 40   | 30 | no | $1.7 \times 10^6$ multi | $1.2 \times 10^6$ multi | 6.9 Mb |
|         | 1024 | 40   | 30 | no | $1.7 \times 10^6$ multi | $1.2 \times 10^6$ multi | 6.9 Mb |

### REFERENCES

[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 Cryptosystem 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.

[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.