PROCEEDINGS OF SCIENCE

Compact CAFED Fully Homomorphic Encryption Scheme

Lang Li[1]

School of Computer Science and Technology, Hengyang Normal University, Hengyang, 421002, China
E-mail: lilang911@126.com

Xiaozhong Yu[2]

School of Computer Science and Technology, Hengyang Normal University,Hengyang, 421002, China
E-mail: 2100295183@qq.com

Yaqiong Yang[3]

School of Computer Science and Technology, Hengyang Normal University,Hengyang, 421002, China
E-mail: 3129555359@qq.com

CAFED scheme is a fully homomorphic encryption scheme that keeps data private; but the homomorphic operation will lead to double increase of the ciphertext size. The compactness of CAFED fully homomorphic scheme was studied over the integers. The improved scheme has smaller ciphertext size by optimizing the ciphertext in homomorphic addition, subtraction and multiplication. This operation will also reduce the influence of homomorphic operation on ciphertext size so that the ciphertext size always remains within $O(\lambda^3)$,where λ is a security parameter. The homomorphic evaluation capability of the optimized scheme was $d < \log(p/16 + 2^{N+1}(1-\|f\|)) - \log\|f\|/\log N$, which makes the ciphertext size not to be increased .

ISCC 2015
18-19, December, 2015
Guangzhou, China

[1] Lang Li(1971-), Ph.D. , his research interests include the embedded computing and information security.

[2] This research is supported by the National Natural Science Foundation of China under Grant No.61572174, Hunan Provincial Natural Science Foundation of China with Grant No.2015JJ40111, the Scientific Research Fund of Hunan Provincial Education Department with Grant No.15A029, the Innovative Training Center of Cultural Hentage and Geographical Information Technology, Hengyang Normal University Experiment Programs of Learning and Innovative for Undergraduates of China with Grant No.CX1531.

[3] Corresponding Author

© *Copyright owned by the author(s) under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License(CC BY-NC-ND 4.0).*

1. Introduction

Homomorphic encryption has been a major with its computation of arbitrary functions on encrypted data without knowing the secret key. In 1978, Rivest, Adleman and Dertouzos has presented the first privacy homomorphism, which can operate the ciphertext directly. The typical public key cryptosystem has the homomorphic properties such as RSA[1], ElGamal[2], Paillier[3] schemes; but, they can't support the homomorphic addition and multiplication. These schemes don' t have the computing ability for fully homomorphic encryption. In 2009, Gentry described the first fully-homomorphic encryption scheme based on lattice[4]. Currently, the homomorphic encryption schemes are divided into three classes: the first fully homomorphic encryption schemes based on ideal lattice. The optimized schemes have been researched from different aspects[5,6,7,8,9];the second fully homomorphic encryption schemes over the integers, which are typically represented by DGHVscheme and CAFED [10,11] scheme. Tang had a detailed summary of DGHV scheme and presented the fast integer fully homomorphic encryption scheme over the integer[12]; the third fully homomorphic encryption scheme based on Learning With Error(LWE)[13]. BGV scheme is the most efficient fully homomorphic encryption scheme. Gentry proposed the first fully homomorphic encryption scheme based on the mathematical ideal lattice structure and the computational complexity. In 2010, Dijk proposed the first DGHV scheme based on integer which can avoid the complex algebraic structure. Subsequently, Gentry proposed the fully homomorphic encryption scheme based on the integer. It is named CAFED scheme, a data privacy protection of fully homomorphic encryption scheme. The operation is based on integer and easy to understand.

In CAFED scheme, the operation of the somewhat homomorphic encryption has not modular operation so that the ciphertext size is increased. The optimal compact homomorphic encryption scheme can controll the ciphertext size. If there is a polynomial $f = f(\lambda)$ which can make the output of decryption algorithm which does not exceed the length of the f ,it is called the compact homomorphic encryption scheme.

The compactly optimization of CAFED scheme is studied in the paper. We research that they meet the compactness for the somewhat homomorphic encryption and the fully homomorphic encryption scheme. The ciphertext size is reduced from the original $O(\lambda^5)$ to $O(\lambda^3)$ when the optimize scheme update the ciphertext. It can keep the cipher size without growth for the decryption algorithm. At the same time, the optimization scheme of homomorphism computation ability and the number of polynomial is proposed. Our improved scheme has smaller ciphertext size in comparison to the original CAFED scheme.

2. CAFED Fully Homomorphic Encryption Scheme

2.1 Related Definition

Definition 2.1.(Homomorphic Encryption) A homomorphic encryption scheme is mainly composed of four probabilistic polynomial-time algorithms such that $\varepsilon = (KeyGen, Encrypt, Decrypt, Evaluate)$.

$KeyGen_{\varepsilon}$: generate a key-pair (pk, sk) according to security parameter λ .

Enc_{ε}: given the plaintext m , use the public key pk to encrypt plaintext, then get ciphertext c .

Dec_{ε}: given the private key sk and the ciphertext c ,use the decryption algorithm to get plaintext m .

PoS(ISCC2015)061

$Evaluate_\varepsilon$: input the public key pk , circuit C (including addition and multiplication),the ciphertext vector $c=(c_1,...,c_t)$, Output $c^*=Evaluate_\varepsilon(pk,C,\vec{c})$.It is the case that $Decrypt_\varepsilon(sk,c^*)=C(m_1,...,m_i)$.

Definition 2.2:(somewhat homomorphic encryption scheme) A scheme can support homomorphic addition and multiplication. The degree of polynomial is lower than the decryption algorithm.

Definition 2.3:(compact homomorphic encryption) The scheme is compact if there is the polynomial $f=f(\lambda)$.As to any key-pair: $(sk\,,pk)\leftarrow KeyGen_\varepsilon(\lambda)$

For any gate circuit C and any sequence of ciphertext $c=(c_1,...,c_t)$, $c_i=Encrypt_\varepsilon(pk,m_i)$.

With respect to pk , the size of the ciphertext c^* $.Evaluate_\varepsilon(pk,C,\vec{c})$ is not more than $f(\lambda)$ bits(independently of the size of C.

Definition 2.4:(fully homomorphic scheme) ε is a fully homomorphic scheme if it is correct for all boolean circuits.

Definition 2.5:(correct homomorphic decryption) The scheme $\varepsilon=(KeyGen,Encrypt,Decrypt,Evaluate)$ is correct for a given t-input circuit C (m is limited to {0, 1}),for any key-pair (pk,sk) output by $KeyGen_\varepsilon$,any t plaintext bits $m=m_1,...m_t$ and any ciphertexts $c=(c_1,...,c_t)$, it is the case that: $Dec(Evaluate_\varepsilon(pk,C,\vec{c}),sk)=C(m_1,...,m_t)$

Definition 2.6:(approximate GCD problem) the approximate-GCD problem: given a set of randomly integers $x_1,x_2,\cdots x_n$, each integer x_i is close to their approximate factor p , which p is the prime number. It is difficult to determine the "approximate common factor".

2.2 Somewhat Homomorphic Encryption

CAFED scheme needs to use parameter to control the bit length of variable. Given the security parameter λ ,set $N=\lambda\,,P=\lambda^2\,,Q=\lambda^5$. Let **SHE=** $KeyGen_\varepsilon,Encrypt_\varepsilon,Decrypt_\varepsilon,Evaluate_\varepsilon$ be a somewhat homomorphic encryption scheme. The description of **SHE** as follow:

$KeyGen_\varepsilon(\lambda)$: generate a random P bit odd integer p , set $sk=p$.

$Encrypt_\varepsilon(pk,m)$: to encrypt a bit $m\in\{0,1\}$, set m' to be a random N bit such that $m'=m \bmod 2$,output $c=m'+pq$,where q is a random Q bit number.

$Decrypt_\varepsilon(sk,c)$: Output $m=(c \bmod p) \bmod 2$, when $m'<<p/2$,we can get the right result of decryption: $c \bmod p=m'$, where $c \bmod p$ is in $(-p/2,p/2)$.

$Evaluate_\varepsilon(pk,f,c_1,...c_t)$: given the pubic key pk and t ciphertexts $c=(c_1,c_2...,c_t)$, the boolean function f is expressed as the circuit C with the XOR and AND gates. Let C^* is the same circuit as C. XOR and AND gates are replaced by additional and multiplication gates over the integers. Let f^* be the multivariate polynomial which it corresponds to C^*. It outputs $c=f^*(c_1,...c_t)$.

2.3 CAFED Fully Homomorphic Scheme

We expand somewhat homomorphic encryption scheme to the public key scheme. The bootstrapping is used. Let **FHE=**$(KeyGen,Encrypt,Decrypt,Evaluate)$ be a fully homomorphic encryption scheme, set $N=\lambda\,,P=\lambda^2\,,Q=\lambda^5\,,\lambda$ is the security parameter. The description of **FHE is** as follow:

PoS(ISC2015)061

$KeyGen(\lambda)$： run $KeyGen_{\varepsilon}(\lambda)$ to obtain key-pair(pk,sk),set $sk=p$ .select a vector $\vec{s}\in\{0,1\}^{\beta}$ with Hamming weight α ,set the sparse subset $S\subset 1,\ldots,\beta$ with $\sum_i y_i=1/pmod2$,set $\vec{y}=(1,\ldots,\beta)$. Output $SK=\vec{s}$ and $PK=(pk,\vec{y})$.

$Encrypt(pk,m)$： let $Encrypt_{\varepsilon}(pk,m)$ obtain the ciphertext $c=Encrypt(pk,m)$. Set $z_i=(c\times y_i)\,mod\,2, i=1,\ldots,\beta$, keep only about $\log_2\alpha$ bits of precision after the binary point for each z_i .The new ciphertext is $c^*=\{c,(z_1,\ldots,z_\beta)\}$.

$Decrypt(sk,c)$： output $m'=\sum_i s_i z_i = c\cdot s_i y_i = (c/p)\,mod2$.

$Evaluate(pk,C,\vec{c})$： the gate circuit C is replaced with addition and multiplication over the integers. Then , the ciphertext $c_1,\ldots,c_t$ are inputted. The ciphertext is updated by operating the decryption algorithm. The updated ciphertext c' is inputted to the gate circuit for computing. The gate output is as the main ciphertext c'', usee $\vec{y}$ to generate the corresponding extension ciphertext $\vec{z}$; therefore, the ciphertext $c'=(c'',\vec{z})$. It is operated sequentially to obtain a final output in the circuit.

3. Compactness of CAFED Fully Homomorphic Encryption

3.1 Compact Optimization

The optimization process requires the introduction of some very close multiples of the auxiliary parameters($x_0^{'},x_1^{'},\ldots,x_\theta^{'}$) which close to P multiple. These data are similar to the public key; but the range of parameters are different. Define a distribution for public key generation:

$$x_i^{'}=s_i^{'}+pq_i^{'}, i=1,\ldots,\theta \tag{3.1}$$

Modify to the homomorphic multiplication operation. $c_1^{'}$ and $c_2^{'}$ are two ciphertexts. It will mod x operation when $c_1^{'}$ multiply $c_2^{'}$. Then it will mod $x_\theta^{'},x_{\theta-1}^{'},\ldots,x_0^{'}$ by order. It is the case that:

$$opt(c_1^{'}\times c_2^{'})=(\cdots(((c_1^{'}\times c_2^{'})\,mod\,x_\theta^{'})\,mod\,x_{\theta-1}^{'})\cdots)\,mod\,x_0^{'} \tag{3.2}$$

The homomorphic operation of optimization scheme is divided into three operations:

$$Add(c_1^{'},c_2^{'})=(c_1^{'}+c_2^{'})\bmod x\,,$$

$$Sub(c_1^{'},c_2^{'})=(c_1^{'}-c_2^{'})\bmod x\,,$$

$$Mult(c_{1,}^{'}c_2^{'})=opt(c_1^{'}\times c_2^{'})\ . \tag{3.3}$$

3.2 Noise Analysis of Optimization Scheme

Suppose two plaintext m_1,m_2 ,set $m_1^{'}=m_1 \bmod 2, m_2^{'}=m_2 \bmod 2$ .Run ε to generate ciphertext $c_1^{'},c_2^{'}$,and $c_1^{'}=(m_1^{'}+pq_1)\bmod x, c_2^{'}=(m_2^{'}+pq_2)\bmod x$. There is two integers k_1, k_2 ,let $c_1^{'}=m_1^{'}+pq_1+k_1x$ and $c_2^{'}=m_2^{'}+pq_2+k_2x$. n_1 and n_2 are the noise of $c_1^{'}$ and $c_2^{'}$.

1)Noise analysis of homomorphic addition operation

Set homomorphic additional operation as **SHE**. **Add** $(c_1^{'},c_2^{'})=(c_1^{'}+c_2^{'})\bmod x$.

In CAFED scheme, suppose k_{Add} as the multiply factor of the mod x in homomorphic addition, $|c_1^{'}|<x/2, |c_2^{'}|<x/2$. We can get $|c_1^{'}+c_2^{'}|<x$ from the triangle inequality.

Because $|(c'_1+c'_2)\,modx|\leqslant x/2$,then

PoS(ISCC2015)061

$$|(c'_1+c'_2)modx-(c'_1+c'_2)|\leqslant|(c'_1+c'_2)modx|+|(c'_1+c'_2)|\leqslant 3/2\mathrm{x} \quad (3.4)$$

So

$(c_1^{'}+c_2^{'})\bmod x = c_1^{'}+c_2^{'}+k_{Add}x$, $|k_{Add}\,x|=|(c'_1+c'_2)modx-(c'_1+c'_2)|\leqslant x$,we can know $|k_{Add}|\leqslant 1$.

SHE. **Add** $(c_{_1}^{'},c_{_2}^{'})$ obtain the new noise: $n_{Add}=n_1+n_2+k_{Add}x$. It can be expressed as:

$$|n_{Add}|\leqslant|n_1|+|n_2|+2^N \quad (3.5)$$

2)Noise analysis of homomorphic subtraction operation

Set homomorphic subtraction operation as **SHE**. **Sub** $(c_{_1}^{'},c_{_2}^{'})=(c_{_1}^{'}-c_{_2}^{'})\bmod x$ 。

In CAFED scheme, suppose k_{Sub} as the multiply factor of the mod x in homomorphic subtraction operation, $(c_1^{'}-c_2^{'})modx\leqslant x/2$, $\left|c_1^{'}\right|<x/2,\left|c_2^{'}\right|<x/2$ .We can get $\left|c_1^{'}-c_2^{'}\right|<x$ from the triangle inequality.Then

$$|(c_1^{'}-c_2^{'})modx-(c_1^{'}-c_2^{'})|\leqslant|(c_1^{'}-c_2^{'})\,modx|+|(c_1^{'}-c_2^{'})|\leqslant 3/2\mathrm{x} \quad (3.6)$$

So

$(c_1^{'}-c_2^{'})\bmod x = c_1^{'}-c_2^{'}+k_{Subt}x$, $|k_{Subt}\,x|=|(c_1^{'}-c_2^{'})modx-(c_1^{'}-c_2^{'})|\leqslant x$,we can know $|k_{Add}|\leqslant 1$.

SHE. **Sub** $(c_{_1}^{'},c_{_2}^{'})$ obtain the new noise: $n_{Subt}=n_1-n_2+k_{Sub}x$. It can be expressed as:

$$|n_{Subt}|\leqslant|n_1|-|n_2|+2^N \quad (3.7)$$

3)Noise analysis of homomorphic multiplication operation

Set homomorphic multiplication operation as **SHE**. **Mult** $(c_{_1}^{'},c_{_2}^{'})=opt(c_{_1}^{'}\bullet c_{_2}^{'})$.

In the CAFED scheme, suppose k_{Mult} as the multiply factor of the mod x in homomorphic multiplication operation. It can be expressed as $|(c_1^{'}\times c_2^{'})\,mod\;x_\theta^{'}|=(c_1^{'}\times c_2^{'})+k_{mult}\,x_\theta^{'}$,and $\left|c_1^{'}\right|<x_\theta^{'}/2,\left|c_2^{'}\right|<x_\theta^{'}/2$ 。

The length of new ciphertext is θ bits. The length of $|c_1^{'}\times c_2^{'}|$ is up to 2θ bits. Because of $|(c_1^{'}\times c_2^{'})|\leqslant 2^{2\theta}<2\mathrm{x}_\theta^{'}$, combine with $|(c_1^{'}\times c_2^{'})\,mod\;x_\theta^{'}|\leqslant x_\theta^{'}/2$. According to the triangle inequality,we can get：

$$|k_{Mult}x'_\theta|=|(c_1^{'}\times c_2^{'})\,mod\;x_\theta^{'}-(c_1^{'}\times c_2^{'})|+(c_{1\mathrm{times}}^{'}c_2^{'})\,mod\;x_\theta^{'}+|(c_1^{'}\times c_2^{'})|\leqslant\frac{5}{2}x_\theta^{'} \quad (3.8)$$

According to the order of the modular x operation of the optimization scheme, we can obtain :

$$(((c_1^{'}\times c_2^{'})\,mod\;x_\theta^{'})\,mod\;x_{\theta-1}^{'}\cdots)\,mod\;x_1^{'}=c_1^{'}\times c_2^{'}+k_{mult}\,x_\theta^{'}+k_{mult}\,x_{\theta-1}^{'}+\cdots+k_{mult}\,x_1^{'}$$

with $|(c'_1\times c'_2)modx'_\theta|\leqslant x'_\theta/2<2^{2\mathrm{x}'_\theta-1}<2\mathrm{x}'_{\theta-1}$, $|k_{mult}|\leqslant 2$,we can know $|k_{mult}|\leqslant 2$.

SHE. **Mult** $(c_{_1}^{'},c_{_2}^{'})$ obtain the new noise: $n_{mult}=n_1\times n_2+2\sum_{(i=1)}^{\theta}k_{mult}\,x'_\theta$,It can be expressed as:

$$|n_{mult}|\leqslant n_1\times n_2+2^{N+1} \quad (3.9)$$

From the above we can know:

1)Homomorphic addition: the sum of the length of the cipher text is roughly the same as ciphertext size. The operation of mod x has little operational impact on the homomorphic addition. The upper limit of the newly introduced error can be determined. The noise of new ciphertext size is 2^N by the homomorphic addition encryption.

2)Homomorphic subtraction: the difference of the cipher text length is roughly the same as the input ciphertext size. The operation of mod x has little operational impact on homomorphic

PoS(ISCC2015)061

subtraction. The upper limit of the newly introduced error can be determined. The new ciphertext size noise is 2^N by the homomorphic subtraction encryption.

3)Homomorphic multiplication: multiplication tends to increase the noise larger than addition and subtraction. The product of the length of the cipher text is roughly the same as the size of the input text. The noise of new ciphertext size is 2^{N+1} by the homomorphic multiplication encryption.

3.3 Homomorphic Computing Ability of Optimization Scheme

According to Gentry's idea, gate circuit is expressed as t variables polynomial $f=(x_1,x_2,...x_t)$. Set the number of polynomials d as the CAFED scheme for the calculation of the index. we can know the noise is $X=N$ [11], from which the new ciphertext is generated by $Encrypt(pk,m)$. Set the homomorphic addition and subtraction, introduce the new noise is $A=2^N$. The homomorphic multiplication which introduces the new noise is $B=2^{N+1}$.

The noise analysis of the d time monomial is as follows:

It is known that the noise variation of the homomorphic multiplication is $n_{mult}=|n_1|\times|n_2|+B$ .We can get the noise of the d time monomial is $(\cdots(((X\cdot X+B)\cdot X+B)\cdot X+B)\cdots)\cdot X+B$ .It can be expressed as:

$$X^d+BX^{d-2}+BX^{d-3}+\cdots BX+B=X^d+B(X^{d-1}-1)/(X-1) \tag{3.10}$$

Each polynomial $f=(x_1,x_2,...x_t)$ is amplified to the d time monomial. There is $\|f\|$ for $f=(x_1,x_2,...x_t)$. The homomorphic addition and subtraction need $2(\|f\|-1)$ times. The total noise is introduced to $2(\|f\|-1)A$; therefore, the noise of the comprehensive calculation is:

$$(X^d+B(X^{d-1}-1)/(X-1))\|f\|+2(\|f\|-1)A \tag{3.11}$$

In order to ensure the correctness of decryption, the noise should be less than $p/16$ .From the inequality , we can get:

$$(X^d+B(X^{d-1}-1)/(X-1))\|f\|+2(\|f\|-1)A<p/16 \tag{3.12}$$

$$d<\frac{\log((p/16+2A)/\|f\|-2A+B/(X-1))-\log(1+B/X(X-1))}{\log X} \tag{3.13}$$

Replaced by $X=N$, $A=2^N$, $B=2^{N+1}$,ignored $B/(X-1)$ and $B/X(X-1)$,we can get the ability of the homomorphic computation is:

$$d<\frac{\log(p/16+2^{N+1}(1-\|f\|))-\log\|f\|}{\log N} \tag{3.14}$$

4. Semantic Security

Provable security is the proof of the specific theory based on certain security model. It can draw the security conclusion from the analysis of cipher scheme. The distinguishability of ciphertexts is an important security feature in many encryption schemes. The opponent will not be able to distinguish when an encryption system has a ciphertext indistinguishable based on plaintext encrypted cryptograph.

Definition 4.1 distinguishability of ciphertexts is defined by the game between the attacker and the user under the plaintext attack as chosen.

The proof is as follows:

1) The user generates a key-pair $(sk,pk)\leftarrow KeyGen(\lambda)$ .It sends the public key to attacker. The user saves the private key.

2) The attacker can perform any encryption operation。

PoS(ISCC2015)061

3)The attacker chooses two distinguishable plaintexts m_0 and m_1 and sends them to the user. The user encrypts $C = E(pk, m)$. The ciphertext is sent to the attacker.

4)After the attacker receives the ciphertext, he will operate the ciphertext and guess the result of the plaintext.

If the attacker guess is success, the attacker wins. If the attacker does not win the games in polynomial time in the given probability, the scheme has indistinguishable security or semantic security under the chosen plaintext attack. The homomorphic encryption of CAFED scheme is $Encryption(sk, m): c = m' + pq$. The algorithm is probabilistic polynomial algorithm. That's to say, as to the same plaintext data content, it will get different ciphertext data results after encryption. The plaintext and ciphertext is to map much relationship. The attacker does not analyze the relationship between plaintext and ciphertext; therefore, the attacker's advantages can be ignored in polynomial time which is compared to the random guessing. In this sense, we can conclude that CAFED fully homomorphic encryption should be semantic security.

PoS(ISCC2015)061

5. Analysis of Properties

We list some properties such as ciphertexts size, the ability of the homomorphic computation and the security of our scheme and the CAFED scheme in Table 1.

Scheme	Ciphertexts size	The ability of the homomorphic computation	Security
CAFED scheme	$O(\lambda^5)$	$d < P/(N \cdot logt)$	Approximate-GCD prblem
Our scheme	$O(\lambda^3)$	$d < \log(p/16 + 2^{N+1}(1-\|f\|)) - \log\|f\|/\log N$	Approximate-GCD problem and Semantic security

Table 1: Comparison of Our Scheme and CAFED Scheme

The noise problem affects the ciphertext size and the homomorphic computation ability. From Table 1, the ability of the homomorphic computation is $d < P/(N \cdot logt)$ in original CAFED scheme. The ability of the homomorphic computation is $d < \log(p/16 + 2^{N+1}(1-\|f\|)) - \log\|f\|/\log N$ in our improved scheme. The compact optimization makes the ciphertext size is not increased. This paper introduces the modular operation for homomorphic operation in CAFED scheme. The ciphertext size always remains within $O(\lambda^3)$.

6. Conclusion

The compactly-optimization CAFED fully homomorphic scheme has been studied in the paper. The compactness is the necessary condition for the fully homomorphic encryption scheme. The homomorphic operation will lead to double increase of the ciphertext size. The compact-optimization can control the ciphertext size of homomrphic addition and multiplication. The ciphertext size would remain within a polynomial bound in our improved scheme. In this paper, we introduce the modular operation for the homomorphic encryption. The homomorphic multiplication operation is optimized. We make the CAFED scheme which is compacted. The compactly-optimization scheme makes the decryption algorithm which is not increased.The parameters setting is smaller.

References

[1] R.L.Rivest,A.Shamir,L.Adleman.*A method for obtaining digital signatures public key cryptosystem*[J].Communication of ACM,1978,21(1):120-126.

[2] T.Elgamal.*A public-key cryptosystem and a signature scheme based on discrete logarithms*[J].Information Theory,IEEE Transactions,1985,31(4):469-472.

[3] P.Paillier.*Public-key Cryptosystems based on Composite Degree Residuosity Classes*[C].//In J.Stern,EUROCRYPT'99:Springer,1999:223-238.

[4] C.Gentry.*Fully Homomorphic Encryption Using Ideal Lattices*[C]//Proc of the 41st Annual ACM Symposium on Theory of Computing.New York:ACM Press,2009:169-178.

[5] N.P.Smart,F.Vercauteren.*Fully homomorphic encryption with relatively small key and ciphertext sizes*[C]//Proc of the 13th International Conference on Practice and Theory in Public Key Cryptography.Berlin:Springer ,2010:420-443.

[6] D.Stehle,R.Steinfeld.*Fast fully homomorphic encryption*[C]//Proc of ASICRYPT. Berlin:Springer , 2010:377-394.

[7] Z.Brakerski.*Fully homomorphic encryption without modulus switching from classical GapSVP*[C]//Advances in CryptologyCRYPTO.Berlin:Springer,2012:868-886.

[8] N.P.Smart,F.*Vercauteren.Fully homomorphic SIMD operations*[C]//Designs,Codes and Cryptography.[S.l.]:Springer,2012:1-25.

[9] C.Gentey,S.Halevi.*Implementing Gentry's fully-homomorphic encryption scheme*[C]//Proc of the 30th Annual International Conference on Theory and Applications Cryptographic Techniques:Advances in Cryptology.Berlin:Springer-Verlag,2011:129-148.

[10] Van D M, Gentry C, Halevi S. *Fully homomorphic encryption over the integers*[C]//Proc of Advances in cryptology–EUROCRYPT 2010. Berlin:Springer, 2010: 24-43.

[11] Gentry G.*Computing arbitrary functions of encrypted data*[J].Communications of The ACM, 2010,53(3):97-105.

[12] TANG Dianhua,ZHU Shixiong,CAO Yunfei.*Fast fully homomorphic encryption scheme over integer*[J].Computer Engineering and Applications,2012,48(28):117-1*22.*(In Chinese)

[13] Z.Brakerski,V.Vaikuntanathan.*Efficient fully homomorphic encryption from(standard) LWE*[C]//Proc of the 52nd IEEE Annual Symposium on Foundations of Computer Science.Palm Springs, CA,2011:97-106.

PoS(ISC2015)061