A Fully Homomorphic Encryption Scheme With a Smaller Public Key

Shaomin Zhang[a], Kaiqiang Li[b] and Baoyi Wang[c]
School of Control and Computer Engineering, North China Electric Power University, Baoding
[a]email:zhangshaomin@126.com, [b]email:daxuewuhe@163.com, [c]email:wangbaoyiqj@126.com

Keywords: Fully homomorphic encryption, Public key dimension, Two forms, Parameter offset technology

Abstract. In order to improve the efficiency of the homomorphic encryption scheme, an improved homomorphic encryption scheme based on integer is proposed. On the basis of the DGHV scheme, the size of the public key is first reduced to $\tilde{O}(\lambda^4)$ by using the public key element quadratic technique and the parameter offset technique. Then, by changing the modulo 2 operation to modulo 2^koperation, the improved scheme can encrypt the data of k bits at one time, which has smaller public key size and higher efficiency than the original DGHV scheme. Finally, the correctness and security of the scheme are proved by the theory, and the efficiency analysis of the scheme is given.

Introduction

The homomorphic encryption was first proposed by Rivest [1] in 1978. They want to be able to decrypt the cipher text under the conditions of operation, the results obtained after the decryption and the same operation on the plaintext to get the same result. After the idea of homomorphic encryption has been put forward, various schemes have been put forward by scholars all over the world, but the cipher text can not be operate any time in these schemes, and the requirements of the homomorphic encryption system can not be meetted.

The scheme of homomorphic encryption based on the ideal lattice was first proposed by Gentry [2] in 2009, and it was analyzed in detail in his doctoral thesis[3]. Gentry's main idea is: first construct a finite-order homomorphic encryption scheme which can only perform finite order homomorphic computation; then reduce the circuit depth by compressing the decryption circuit; secondly, get a bootstrap scheme by bootstrap transformation.

The integer based somewhat encryption scheme was designed by Dijk[4] in 2010, and according to the idea of Gentry was converted into a full encryption scheme, also known as the DGHV program. The public key parameters by linear form to two form compression scheme was proposed by Coron[5] in 2011 , the public key size by $\tilde{O}(\lambda^8)$ compressed to $\tilde{O}(\lambda^{6.5})$. Coron[6] proposed another scheme for DGHV using parametric offset compression scheme, the public key parameters compression length to $\tilde{O}(\lambda^5)$. In recent years, some domestic scholars have also proposed some improvement schemes, such as Lei, Li Zichen[7][8] were changed to mode 2 operation mode 4 operation and 2^k operation mode, the 1 bit data encryption by only one can respectively into a can encrypt 2 bit and K bit data. DaiHong Yan[9] proposed a method which does not need to be modular 2 and self - lifting. Luo Bingcong, Xiong Wanjun[10][11] uses different public key compression techniques to reduce the size of the public key. How to improve the efficiency of the encryption scheme is still an important and difficult problem in the research of the encryption scheme.

In this paper, we use the basic idea of Gentry to improve the DGHV system :we use the method of [8] to change modulo 2 in the original scheme to modulo 2^k so that the k-bits plaintext data can be encrypted at one time; using the literature idea in [5-6] ,the size of the public key is reduced to $\tilde{O}(\lambda^4)$.Compared with the original DGHV scheme, this scheme has the advantages of smaller public key size and higher efficiency.

Basic Symbols And Definitions

For a real number z,we denote by $\lceil z \rceil$、$\lfloor z \rfloor$ and $[z]$ the rounding of a up, down and to the nearest integer. Namely, these are the unique integers in the half open intervals

$[z] \in [z, z+1), \lfloor z \rceil \in (z-1, z], \lceil z \rceil \in (z-\frac{1}{2}, z+\frac{1}{2}]$.For a real number z and an integer p,we use $[z]_p$ or $r_p(z)$ to denote z mod p,$q_p(z)$ to denote the quotient of z/p.The progressive symbols used in this paper, using $\tilde{O}(\cdot)$ said the same order of infinity, with $\omega(\cdot)$ said the high order of infinity.

In this paper, some Greek letters is used to represent the parameters, the following is the Greek letter in this article meaning:

λ:Safety parameters;

γ:The bit-length of the public key, to thwart various lattice-based attacks on the underlying AGCD, the bit-length of the public key is $\omega(\eta^2 \log \lambda)$;

η:The bit-length of the secret key, to support homomorphism for deep enough circuits, the bit-length of the secret key is $\rho.\Theta(\lambda \log^2 \lambda)$;

ρ:The bit-length of the noise, to protect against brute-force attacks on the noise, the bit-length of the noise is $\omega(\log \lambda)$;

τ:The number of public key, should satisfy $\tau \geq \gamma + \omega(\log \lambda)$;

ρ' :The second noise parameter, should satisfy $\rho' = \rho + \omega(\log \lambda)$;

In order to satisfy the above constraint conditions, the parameters are selected as shown in table 1.

Table 1 parameter selection of the encryption scheme

ρ	ρ'	η	γ	τ
λ	2λ	$\tilde{O}(\lambda^2)$	$\tilde{O}(\lambda^5)$	$\gamma+\lambda$

Definition 1 (Augmented Decryption Circuits). Let $\varepsilon = (\mathbf{Keygen, Enc, Dec}$,Evaluate) be a homomorphic encryption scheme and it's decryption circuit is D_ε, whose input is the private key and cipher text, the output is clear. Let a set of input and output are homomorphic encryption scheme ε and set the circuit space Γ. There is a circuit composed of a plurality of decryption circuits, and there is a gate circuit g connected to the decryption circuit, said circuit is g-extended decryption circuit. If the circuit $g \in \Gamma$, these decryption circuits and the extended decryption circuit are denoted as $D_\varepsilon(\Gamma)$.

Definition 2 (Boots trappable Encryption). Let $\varepsilon = (\mathbf{Keygen, Enc, Dec}$,Evaluate) be a homomorphic encryption scheme. Let $D_\varepsilon(\Gamma)$ be the decryption and extended decryption circuit, and the set of circuits that can be evaluated by scheme ε. If $D_\varepsilon(\Gamma) \subset C_\varepsilon$, then the encryption scheme ε is bootstrapped.

Definition 3 (Error-Free AGCD). For a random η bits integer p, a non-square random $2^{\lambda^2}-\mathbf{rough}$ integer $q_0 \in [0, 2^\gamma/p)$,let $x_0 = q_0.p$.Meet $D_{\gamma,\rho}$ of multiple samples is difficult to recover p.

The Design of Fully Homomorphic Encryption Scheme with a Smaller Public key

According to the ideas of constructing Gentry, Somewhat homomorphism to construct one can support a limited addition, multiplication improved encryption scheme, analysis of the correctness of this method, and proved its safety; Compression of the decryption algorithm. It reduces its computational complexity; Then the scheme has been bootstrapped, thus obtained the homomorphic scheme.

Design of Improved Somewhat Encryption Scheme. In this scheme, the public key elements form from linear to two times, namely $x_{i,j} = x_{i,0}.x_{j,1} \bmod x_0$,which β is the new beta parameters and $1 \leq i, j \leq \beta$. So the original need to store $\tau = \beta^2$ integers, this article only need to sort e 2β integers. Similarly, the key elements of $x_{i,b}(1 \leq i \leq \beta, b \in \{0,1\})$ is changed from the difference between a random number $\chi_{i,b}$ and an integer $\delta_{i,b}$ to represent. So the original γ bits integer to be stored, we only need to store the magnitude and $\delta_{i,b}$ can be quite an integer. At the same time, modulo 2 in DGHV scheme is changed to modulo 2^k. So that the original encryption can only be 1 bit, this program can encrypt k bits each time. The selected parameters of the scheme is shown in table 2.

Table 2 parameter selection of Somewhat encryption scheme

ρ	ρ'	η	γ	α	β
λ	4λ	$\tilde{O}(\lambda^2)$	$\tilde{O}(\lambda^5)$	λ	$\tilde{O}(\lambda^2)$

1）Key Generation Algorithm $\mathbf{Keygen}(1^{\lambda})$

Key Generation Algorithm $\mathbf{Keygen}(1^{\lambda})$ is described as follows.

a)Randomly generated a prime p and it's length is η bits, which $p \in [2^{\eta-1}, 2^{\eta})$。Let $x_0 = q_0 . p$,which $q_0 \in [0, 2^{\gamma}/p)$ is less than 2^{λ^2} and does not contain prime factors.

b)We initialize a pseudo random number generator f_1 with the random seed se_1,produce a set of integer $\chi_{i,b} \in [0, x_0)$ with $f_1(se_1)$,when $1 \le i \le \beta$, $b \in \{0,1\}$.

c)Calculates the public key offset $\delta_{i,b} = [\chi_{i,b}]_p + \xi_{i,b} . p - 2^k, r_{i,b}, 1 \le i \le \beta, b \in \{0,1\}$,when $r_{i,b} \leftarrow \mathbb{Z} \cap (-2^{\rho}, 2^{\rho})$, $\xi_{i,b} \leftarrow \mathbb{Z} \cap (0, 2^{\lambda+\eta}/p)$.

Let the public key pk=$< x_0, xe_1, (\delta_{i,b})_{1 \le i \le \beta, b \in \{0,1\}} >$ and private key sk=p.

2)Encryption Algorithm $\mathrm{Encrypt}(pk, m \in \{0,1\}^k)$

a)Recover the set of integers $\chi_{i,b} \in [0, x_0)$ with $f_1(se_1)$,when $1 \le i \le \beta$,$b \in \{0,1\}$,and then calculate the secondary public key parameter $x'_{i,0} = \chi_{i,0} - \delta_{i,0}, x'_{j,1} = \chi_{i,1} - \delta_{i,1}$.

b)Generate a random $\tau = \beta^2$ scale integer vector $b = (b_{i,j})$,when $1 \le i,j \le \beta, b_{i,j} \in [0, 2^{\alpha})$.

c)Choose a random integer $r \leftarrow (-2^{\rho'}, 2^{\rho'})$ and integer set $S \subset \{1,2,\dots,\beta\}$.

Calculates and outputs the cipher text

$$c = \left[m + 2^k r + 2^k \sum_{i,j \in S} b_{i,j} . x'_{i,0} . x'_{j,1} \right]_{x_0}$$

3）Ciphertext processing $\mathbf{Evaluate}(pk, C, c_1, \dots c_t)$

Given a t-input computational circuit C, input t cipher texts, pass the input cipher text through the additive gate and multiplication gate of circuit C (perform the homomorphic addition and multiplication on integers) ,and return the resulting integer.

4）Decryption algorithm Decrypt (sk,c)

Given a cipher text C, Output m given by $m \leftarrow (c \bmod p) \bmod 2^k$.

The Correctness Analysis of the Improved Scheme. Definition 6[4] (Permitted Circuit)Any absolute value is less than $\tau^i . 2^{i(\rho'+2)} (i \ge 1)$ as integer input value, if the output circuit C_ε absolute values in the $n = \lceil \log_2(\lambda+1) \rceil$ under the premise of up to $2^{i(\eta-3-n)}$,is a collection of C_ε circuit said the operation circuit.

Theorem 1 The Somewhat scheme in this paper can correct the homomorphic decryption for the circuit C_ε.

Proof: If the encryption algorithm $\mathrm{Encrypt}(pk, m \in \{0,1\}^k)$ to obtain the ciphertext c, that is

$$c = \left[m + 2^k r + 2^k \sum_{i,j \in S} b_{i,j} . x'_{i,0} . x'_{j,1} \right]_{x_0}$$

For all$1 \le i \le \beta, b \in \{0,1\}$, there is

$x_{i,b} = \chi_{i,b} - \delta_{i,b}, \chi_{i,b} \in [0, x_0), \delta_{i,b} = [\chi_{i,b}]_p + p . \xi_{i,b} - r_{i,b}, \xi_{i,b} \leftarrow \mathbb{Z} \cap [0, 2^{\lambda+\eta}/p)$

and $|r| < 2^{\rho'}, r_{i,b} \leftarrow \mathbb{Z} \cap (-2^{\rho}, 2^{\rho}), b_{ij} \in [0, 2^{\alpha}), S \subset \{1,2,\dots,\beta\}$,we have

$$c = [m + 2^k . r + 2^k \sum_{i,j \in S} b_{i,j} . (p . (q_p(\chi_{i,0}) - \xi_{i,0}) + r_{i,0}) . (p . (q_p(\chi_{i,1}) - \xi_{i,1}) + r_{i,1})] \bmod x_0$$

$$c \bmod p = \left[m + 2^k r + 2^k \sum_{i,j \in S} b_{i,j} . r_{i,0} . r_{j,1} \right]_p$$

Since $\rho' = 2\rho + a + \omega(\log\lambda)$,there is

$|c \bmod p| \le 2^{\rho'+k} + 2^k . \tau . 2^{2\rho+\alpha} \le \tau . 2^{\rho'+k+1} \le \tau^{k-1} . 2^{(k-1)(\rho'+2)}$

If the number of inputs is t, the operable circuit is denoted by $C \in C_\varepsilon$, the circuit operating on the integer is denoted by C^*, and $c_i \leftarrow \mathrm{Encrypt}(pk, m_i)$,it is the case that

$c \bmod p = C^*(c_1, c_2, \dots, c_t) \bmod p = C^*(c_1 \bmod p, c_2 \bmod p, \dots, c_t \bmod p) \bmod p$

By definition 2

$$|C^*(c_1 \bmod p, c_2 \bmod p, \ldots, c_t \bmod p)| \le (2^{\eta-4})^{k-1} \le (p/8)^{k-1}$$
$$C^*(c_1 \bmod p, c_2 \bmod p, \ldots, c_t \bmod p) \bmod p = C^*(c_1 \bmod p, c_2 \bmod p, \ldots, c_t \bmod p)$$
$$c \bmod p = C^*(c_1 \bmod p, c_2 \bmod p, \ldots, c_t \bmod p)$$
$$[c \bmod p]_{2^k} = [C^*(c_1 \bmod p, c_2 \bmod p, \ldots, c_t \bmod p)]_{2^k}$$
$$= C^*([c_1 \bmod p]_{2^k}, [c_2 \bmod p]_{2^k}, \ldots, [c_t \bmod p]_{2^k})$$

That is $[c \bmod p]_{2^k} = C(c_1, c_2, \ldots, c_t)$。

So, the program is correct.

The Security Analysis Of The Improved Scheme. The security of the scheme is reduced to the approximate maximum common divisor problem.

Theorem 2 The above scheme takes λ as the security parameter and $\rho,\rho',\eta,\gamma,\tau=\beta^2$ as the parameter polynomial. If any attacker A breaks the algorithm with the dominant ε, there is a probability of an algorithm B which is not less $\varepsilon/2$ through $x_{i,b} = p.q_{i,b} + 2^k.r_{i,b}(1 \le i \le \beta, b \in \{0,1\})$ to find p, that algorithm B can not less than ε / 2 probability of solving the approximate maximum common factor problem.

Any attack on this scheme can be converted to the approximate GCD problem, if the attacker A wanted to break through this scheme, it must be through $x_{i,b} = pq_{i,b} + 2^k r_{i,b}(1 \le i \le \beta, b \in \{0,1\})$ for P, but at present the approximate GCD problem is not solvable, so this scheme is semantically secure.

An fully homomorphic Encryption Scheme with a Smaller Public Key

First of all, the introduction of three new additional parameters κ, θ and Θ, which $\kappa = \gamma + 2 + \lceil \log_2(\theta+1) \rceil, \theta = \lambda$ and $\Theta = \tilde{O}(\lambda^3)$, specific programs are as follows:

1) KeyGen: by using the method of Somewhat encryption algorithm to generate the private key sk^* and the public key pk^*. Let $x_p \leftarrow \lfloor 2^\kappa/p \rfloor$ be a random vector with a weight of $\sqrt{\theta}$ and a length of $\sqrt{\Theta}$ .For $s = (s_1, s_2, \ldots, s_{\sqrt{\Theta}}), s' = (s'_1, s'_2, \ldots, s'_{\sqrt{\Theta}})$,they meet $s_0 = s'_0 = 1$; In each s_i and s'_i, there is at most one nonzero bit, where $k\lfloor B \rfloor \le i \le (k+1)\lfloor B \rfloor, B = \Theta/\theta, k \in [0, \sqrt{\theta})$;Tick set $S = \{(i_1, i_2): s_{i,i_1}.s'_{i,i_2} = 1\}$contains only θ elements.

Initializes a random seed se_2 for random number generator f_2, using $f_2(se_2)$ generation integer $u_i \in \mathbb{Z} \cap [0, 2^{\kappa+1})$, where $2 \le i \le \Theta$ and get the value of u_i by $\sum_{i \in S} u_i = x_p (\bmod 2^{\kappa+1})$.Meanwhile, let $y_i = u_i/2^\kappa$,then the vector $y = (y_1, y_2, \ldots, y_\Theta)$ and y_i are positive values of κ bits precision less than 2. This collection to meet $1/p = \left[\sum_{i=1}^{\sqrt{\Theta}} s_i.s'_i.y_i + \Delta_p\right]_{2^k}, |\Delta_p| < 2^{-\kappa}$. (1)

Output private key $sk = (s, s')$ and public key $pk = (pk^*, se_2, y_1)$.Proof of equation (1) is as follows:

$$\left[\sum_{i=1}^{\sqrt{\Theta}} s_i.s'_i.y_i + \Delta_p\right]_{2^k} = \left[\sum_{i=1}^{\sqrt{\Theta}} y_i + \Delta_p\right]_{2^k} = \left[\sum_{i=1}^{\sqrt{\Theta}} u_i/2^\kappa + \Delta_p\right]_{2^k} =$$
$$\left[\lfloor 2^\kappa/p \rfloor/2^\kappa + \Delta_p\right]_{2^k} = 1/p - \Delta_p + \Delta_p = 1/p$$

2） $Encrypt(pk, m \in \{0,1\}^k)$:generate a random $\tau = \beta^2$ scale integer vector $b = (b_{ij})$,where $1 \le i,j \le \beta, b_{i,j} \in [0, 2^\alpha)$ and $b' = (b_{ij}), 1 \le i,j \le \beta, b_{i,j} \in [0, 2^\alpha]$.As mentioned earlier, calculate the cipher text $c^* = \left[m + 2^k r + 2^k \sum_{i,j \in S} b_{i,j}.x'_{i,0}.x'_{j,1}\right]_{x_0}$.For all $i \in \{1,2,\ldots,\Theta\}$,let $z_i = [c^*.y_i]_{2^k}$ and retain the decimal point after the $n = \lceil \log\theta \rceil + 3$ effective number, set vactor $z = < z_1, z_2, \ldots, z_\Theta >$ and output expansion cipher text $c' = (c^*, z)$.

3) $Decrypt(sk, c')$.The decryption process is $m \leftarrow \left[c^* - \sum_{i \in S} s_i.s'_i.z_i\right]_{2^k}$.

The Correctness Analysis Of Compression And Decryption Algorithm. In theorem 1, it is proved that the Somewhat scheme is correct for calculating the set of C_e,and it is proved that the scheme is correct for the set $C(P_e)$ of the gate.

Theorem 2 Shows that the proposed scheme can decrypt the right gate set $C(P_e)$ with proper

homomorphism.

Proof: If the scheme after decompression is still able to decrypt correctly, then there must be $\left\lfloor \sum_{i=1}^{\sqrt{\Theta}-1} s_i s_i' z_i \right\rceil \bmod(2^k) = \lfloor c^*/p \rceil$.

From the proof of equation (1),we know that the original equals $\lfloor c^*/p \rceil - \lfloor c^*.\Delta p \rceil (\bmod 2^k)$.

Since z_i can be represented by $[c^*.y_i]_{2^k}$ and retains the decimal point $n = \lceil \log\theta \rceil + 3$n significant digits, so $\varepsilon_i = z_i - [c^*.y_i]_{2^k}$,where $\varepsilon_i < 2^{-(n+1)} \le 1/16\theta$. Then,

$$\left[c^*/p - \left\lfloor \sum_{i=1}^{\sqrt{\Theta}-1} s_i s_i' z_i \right\rceil\right]_{2^k} = \left[c^*/p - \sum_{i=1}^{\sqrt{\Theta}-1} s_i s_i' [c^*.y_i]_{2^k} + \sum_{i=1}^{\sqrt{\Theta}-1} s_i s_i' \varepsilon_i\right]_{2^k} =$$

$$\left| \left[c^*.\Delta_p + \sum_{i=1}^{\sqrt{\Theta}-1} s_i s_i' \varepsilon_i\right]_{2^k} \right| \le |c^*.\Delta_p| + \left| \sum_{i=1}^{\sqrt{\Theta}-1} s_i s_i' \varepsilon_i \right| \le$$

$$2^{\frac{\gamma(\eta-4)}{\rho'+2}}.2^{-k} + \theta.\frac{1}{16\theta} \le 2^{k-4}.2^{-k} + \frac{1}{16} \le \frac{1}{8}$$

So， $\left\lfloor \sum_{i=1}^{\sqrt{\Theta}-1} s_i s_i' z_i \right\rceil \bmod(2^k) = \lfloor c^*/p \rceil$ set up, theorem proves.

Bootstrappable. According to the method in [4],in order to reduce the complexity of the decryption algorithm, the decryption algorithm is divided into three steps:

Step 1 Computes $a_i = s_i.z_i$,where $i = 1,2,\ldots,\Theta$.

Step 2 Produced by Step 1 in a Θ number of $\{a_i\}_{i=1}^{\Theta}$,get $n+1$ rational numbers $\{w_j\}_{j=1}^{n}$.The precision of each w_j is no more than n bits and satisfies $\sum_j w_j \ (\bmod 2^k)$.

Step 3 Calculate and output $c^* - (\sum_j w_j) mod 2^k$.

The efficiency Analysis of the Improved Scheme. The difficulty of this scheme is based on the error-free AGCD problem and the SSSP problem. First, we constructed a somewhat homomorphic encryption scheme, the public and private key size number are $\tilde{O}(\lambda^{10})$ and $\tilde{O}(\lambda^2)$, and by change the mode 2 to mode 2^k, the improved scheme can encrypt the k bits plaintext at one time. As shown in Table 3 and table 4, we compare the scheme of this paper with the original DGHV scheme and the scheme of literature [7] from the aspects of public key size, private key size and the difficulty of the problem.

Table 3 the comparison of Somewhat homomorphic encryption schemes

Scheme	Encrypted plaintext bits	Public key size	Private key size	Based on the difficult issues
DGHV scheme	1 bit	$\tilde{O}(\lambda^{10})$	$\tilde{O}(\lambda^2)$	Error-Free AGCD
Reference[7] scheme	k bits	$\tilde{O}(\lambda^7)$	$\tilde{O}(\lambda^2)$	Error-Free AGCD
My scheme	k bits	$\tilde{O}(\lambda^4)$	$\tilde{O}(\lambda^2)$	Error-Free AGCD

Table 4 the comparison of Fully homomorphic encryption schemes

Scheme	Encrypted plaintext bits	Public key size	Private key size	Based on the difficult issues
DGHV scheme	1 bit	$\tilde{O}(\lambda^{13})$	$\tilde{O}(\lambda^7)$	Error-Free AGCD,SSSP
Reference[7] scheme	k bits	$\tilde{O}(\lambda^7)$	$\tilde{O}(\lambda^2)$	Error-Free AGCD,SSSP
My scheme	k bits	$\tilde{O}(\lambda^4)$	$\tilde{O}(\lambda^2)$	Error-Free AGCD,SSSP

Conclusion

Based on the original DGHV scheme, this paper uses the method of document[8] to change the mode 2 operation in the original scheme into a modular 2^k operation, and then constructs an efficient fully homomorphic encryption scheme. And use the method of literature [5] reduces the number of public key, using the method of literature [6] reduces the length of the public key, and public key size by $\tilde{O}(\lambda^{10})$ reduced to $\tilde{O}(\lambda^4)$. The scheme can encrypt k bits at one time, so the scheme has shorter public key size and higher efficiency than the original DGHV scheme.

Acknowledgement

In this paper,the research was sponsored by the National Natural Science Foundation of China(Proje ct No.) and Scientific Research Project of Hebei Province (Project No.).

References

[1] Rivest R, Adleman L, Dertouzos M. On data banks and privacy homomorphisms [J]. Foundation of Secure Computation, 1978: 160-171.

[2] Gentry C. Fully homomorphic encryption using ideal lattices [C]//Proc of the 41st Annual ACM Symposium on Theory of Computing. 2009: 169-178.

[3] GENTRY C.A fully homomorphic encryption scheme [D]. Stanford:Stanford University, 2009.

[4] Van Dijkm G, Halevis. Fully homomorphic encryption over the integers[C]//Advances in Cryptology-EUROCRYPT. Berlin: Springer, 2010: 118-130.

[5] Cronj S, Mandala N. Fully homomorphic encryption over the integers with shorter public keys[C]//Advances in Cryptology-CRYPTO. Berlin: Springer,2011: 94-145.

[6] CORON J S,NACCACHE D,TIBOUCHI M. Public key compression and modulus switching for fully homomorphic encryption over the integers [C] //Advances in Cryptology-EUROCRYPT. Berlin: Springer,2012: 446-464.

[7] LIN Ru-lei, WANG Jian, DU He. Improved fully homomorphic encryption over integers[J]. Application Research of Computers, 2013, 30(5): 113-122.

[8] Li Zichen,Zhang Fengjuan,Wang Peidong.Highly efficient fully homomorphic encryption scheme with shorter public keys[J]. Application Research of Computers, 2017,02:1-4.

[9] Dai Hongyan,Ding Yong,Lv Haifeng,Gao Wen.Faster FHE scheme over integers[J]. Application Research of Computers, 2015,11:3448-3451+3455.

[10] LUO B C, LIU Q, MA Y, et al. Batch fully homomorphic encryption over integers with shorter public keys[J]. Application Research of Computers, 2014, 31(4): 1180–1184.

[11] XIONG W J, WEI Y Z, WANG H Y. An improved fully homomorphic encryption scheme over the integers[J]. Journal of Cryptologic Research, 2016, 3(1): 67–78.