Improved Fully Homomorphic Encryption Algorithm for Cloud Storage

Renyuan Hu*, Longjun Zhang and Yongzhen Qin
Engineering University of CAPF, Xi'an 710086, China
*Corresponding author

***Abstract*—Fully homomorphic encryption has important applications in cloud storage, the cipher text retrieval and other aspects. In order to get a better fully homomorphic encryption scheme for cloud storage, an improved fully homomorphic encryption (FHE) scheme based on DGHV scheme is proposed by analyzing and comparing the existing research situation of fully homomorphic encryption scheme. On the premise of guarantying scheme's safety, the amount of single encrypted data is increased to 3 bit. Arguably, improving the single encrypted data volume at the same time, the public key, suitable for cloud storage platform, has smaller size, and reduces the computational complexity.**

Keywords-fully homomorphic encryption; cloud storage; cipher text retrieval

I. INTRODUCTION

With the continuous promotion of cloud computing technology, the storage and management of information data has become one of the hottest topics in cloud computing field. As one of the effective methods to solve the problem of information data storage and management, the cloud storage technology is developed from the parallel storage, distributed storage and grid storage, but as such a new merging technology, it is still not complete matured in each aspects at all, especially the security aspect. To use the outsourced storage service [1] of the cloud computing, the user's data will inevitably be uploaded to the cloud end. How to protect the security of user's data under the situation that the users shall lose the absolute ownership and control of their data, which shall be the biggest practical problem the cloud storage should face to. With such basis, it may also need further exploration and improvement on the data encryption technique to realize the cipher text computing and search function accordingly.

In 1970s Rivest et al.[2] proposed the FHE problem, hoping to carry out the add, subtract, multiply and divide operation on the cipher text through the character of full homomorphism and under the situation that not encrypting the cipher text, and the operated result after decryption shall also be in consistent with the operated result with matching plain text. After that, both domestic and foreign scholars have made plenty of researches on the homomorphic encryption accordingly, but many of resulted homomorphic encryption schemes did not meet the requirement of the full homomorphism encryption. Until 2009 the researcher of IBM Gentry made the great breakthrough in this field and proposed the full homomorphic encryption scheme based on the ideal grid[3] and gave the further in-depth discussion on the homomorphic encryption in his doctoral dissertation[4] accordingly. The two articles have lightened the way forward for the research field of full homomorphic encryption, and also provided such a technology with feasibility for realizing the cipher text retrieval.

Currently the majority of domestic research findings on the full homomorphic encryption technique related to the integers still stopped at the level of improved scheme that proposed based on existing scheme foundations. For example, based on the literature [3], Dianhua Tang et al.[5] have made the improvement accordingly and it got the advantages in the smaller public key dimension and higher computing efficiency etc in comparison with the literature [3]. Rulei Lin et al [6] encrypted the 2bit plain text at once and changed the mode 2 operation into mode 4 operation, which further improved the efficiency and made the analysis on the security of such scheme. There's another way for the research on full homomorphic encryption technique that is based on the problem of LWE difficulty, but it shall also need further research and analysis on whether it can be used for cloud storage accordingly.

This paper mainly analyzes the property and character of the cloud storage, by combining with the relative domestic improvement thoughts and improved the full homomorphic encryption scheme on the integers mentioned in literature [7], increasing the single encrypted data volume from 1bit to 3bit, and constructing the full homomorphic encryption scheme by using the full homomorphic encryption thought of Gentry, then shortening the public key dimension greatly by using the technology mentioned in literature [7],resulting in higher efficiency accordingly.

II. THEORETICAL FOUNDATION

A. The Principle of Homomorphic Encryption

The homomorphism is such a fundamental concept of modern algebra theory.

To suppose that the encryption function is EK and decryption function is DK, the arithmetic operation is α and the plain text is M (m_0,m_1,…,m_i), the formula is α (DK (M (m_0,m_1,…,m_i)))= D (α(M (m_0,m_1,…,m_i)))

FHE encryption scheme shall include four algorithms as followed:

The key part (Key) : According to the given parameter γ, it generates the private key *sk* and public key *pk*;

Encrypted part (Enc) :To get the encrypted text c by using public key *pk* to encrypt the plain text;

Decrypted part (Dec):The plain text m shall be obtained after decrypting the encrypted text with private key.

Encrypted text operation algorithm (Evaluate): To output the circuits C which has t input and public keys *pk*, and the encrypted text c matched with the plain text. To express it through formula, the output shall be Evaluate (*pk*, C, c).

B. DGHV Fully Homomorphic Encryption

The specific DGHV scheme [7]can be:

- To create a Somewhat encryption scheme

To generate the encryption key: to select p as the encryption key, where p should meet the condition as: p is such a big prime number, and $p \in [2\eta-1, 2\eta)$;

Encryption part: the 1bit plain text $m \in \{0,1\}$, after encryption on m there's encrypted text c=m+pq+2r, to randomly generate q and r during encryption. Among them, q is a quite large integer that is larger than p so far, r is quite a smaller integer and $2r < p/2$;

Decrypted part: the decryption process is the plain text m =(c mod p)mod2.

- To structure the somewhat scheme in asymmetric public key scheme

For q is opened for public, so if it takes pq as public key directly, then it should be quite easy to calculate the private key p, then supposing such a set {xi, xi=pqi+2ri}, to form the subset S by selecting any items from the set, to take the sum of the elements in the subset as public key sum (s)= the formula can be expressed as: c=m+2r+sum (s). Then the public key with random property could effectively guarantee that the encrypted text cannot be decrypted.

- To constantly refresh the encrypted text by using the compressed decryption technique, so as to control the increase of noise.

From the decryption algorithm it can be seen that, while encrypted text is located among c mod p (p/2, p/2), it can get the plain text through decryption. If it exceeds such range, then it cannot be restored in plain text accordingly. Before each operation, the "fresh" encrypted text is encrypted for one time, so that the noise of encrypted text under operation can be controlled within a certain range, thus the target to eliminate the noise can be achieved. So the new encrypted text after each operation could be decrypted successfully.

III. The Improved Full Homomorphic Encryption Scheme Based on the Integers

A. The Principle of Improved Scheme

A full homomorphic encryption scheme based on the integers that can encrypt 3bit encrypted text at once was proposed, through the study and analysis in literature [7]. It has a larger single encryption data volume and even smaller public key dimension.

First the symbols used in this paper should be instructed as following:

λ: the security parameter;

ρ: Length of noise, in order to strike against the violent attack, the length of noise shall be taken as $\rho=\omega(\log \lambda)$;

η: the binary length of private key, it should meet $\eta \geq \rho\ \Theta(\lambda \log 2\lambda)$;

Γ: the binary length of public key, it should meet $\gamma=\omega(\eta 2\log\lambda)$;

τ: the number of public keys, $\tau \geq \gamma + \omega(\log \lambda)$, in this paper it totally needs 2 public keys.

There $\omega()$ is the infinitely large quantity in higher order.

B. The Full Homomorphic Encryption Scheme

1) To structure partially homomorphic Somewhat scheme

To change the mode 2 operation into 2^3 operations, it can encrypt the information with 3bit plain text in one time.

- KeyGen(λ): the encrypted key p generated by the security parameter λ in η bits and the encrypted key sk=p.
- Encrypt(sk, m): to encrypt the $m \in \{000,001,010,\ldots,111\}$ then get $c=m+23r+pq$, where r is the random integer in size of ρ bits and q is the random integer in size of γ bits during the encryption process.
- Decrypt (sk, c):m=(c mod p) mod23

The value of c mod p shall be the noise volume, only when $|\ m+2^3r\ | < p/2$, the noise c mod $p=m+2^3r$. Then it can restore the plain text in validity. Following is the validation on the homomorphism of the scheme:

$$c_1=m_1+2^3r_1+pq_1$$

$$c_2=m_2+2^3r_2+pq_2$$

$$c_1+c_2$$

$$=[(m_1+2^3r_1)+(m_2+2^3r_2)]+p(q_1+q_2)$$

$$=(m_1+m_2)+2^3(r_1+r_2)+p(q_1+q_2)$$

$$c_1c_2$$

$$=(m_1+2^3r_1)(m_2+2^3r_2)+p[(m_1+2^3r_1)q_2$$

$$+(m_2+2^3r_2)q_1+pq_1q_2]$$

$$=m_1m_2+2^3(m_2r_1+m_1r_2+2^3r_1r_2)$$

$$+p\ (m_1q_2+m_2q_1+2^3r_1q_2+2^3r_2q_1+pq_1q_2)$$

$$[(c_1+c_2)\ mod\ p]mod2^3$$

$$=[m_1+m_2+2^3(r_1+r_2)]mod2^3=m_1+m_2$$

$$(\text{when}\ |\ (m_1+m_2)+2^3(r_1+r_2)\ |\ <p/2)$$

$$[(c_1*c_2)mod\ p]mod2^3$$

$$=[m_1m_2+2^3(m_2r_1+2^3r_1r_2+m_1r_2)]mod2^3=m_1m_2$$

$$(\text{when}\ |\ (m_1m_2+2^3(m_2r_1+m_1r_2+2^3r_1r_2))\ |\ <p/2)$$

From the formulas we can obtain that, the structured symmetric encryption scheme can both meet the additive

homomorphism and the subtraction homomorphism. But the noise of the scheme may continuously "expand" along with the operation numbers. However the noise is larger than p/2, the above equation will not be established at all, And it cannot decrypt the valid plain text. Meanwhile it can be seen from above formula that, the noise presents the linear growth in additive homomorphic operation, and in multiply homomorphic operation it shows the geometric growth then.

2) Transform in the public key encryption system

It may need to add a set of "0" encrypted text as public key, the specific method is given below:

- KeyGen(λ):The private key p in η bits generated randomly during the encryption process, let x0=pq0, and x0 is the odd number and meet the condition that rp(x0) can be divided completely by 23 . And there b={0,1},1≤i≤,xi,b=pqi,b+23ri,b then pk=<x0,x1,0,x1,1,x2,0,x2,1,…, ,>.
- Encrypt(pk, m): τ-dimension vector b=<bi,j>(1≤i,j≤,bi,j∈{0,1}), Q is the fixed large prime number that generated randomly during encryption process,(and the digits of p shall be larger than the digits of Q) the plain text m∈{000,001,010,…,111}, the encrypted text c shall be: c=(m+23r+p+23Qbi,jxi,0xj,1)mod x0
- Decrypt(sk, c): the plain text used for decryption on encrypted text m=(c mod p)mod23, during the encryption process, mod on x0 is to lower the size of encrypted text.

3) Compress the decryption circuit, to realize the full homomorphic encryption scheme

According to the procedure in literature [7], to compress the decryption circuit by utilizing the bootstrap property of the scheme, some private key information is added into the public keys. By pre-handling the encrypted text with the part of private key information keeps the "freshness" of the encrypted text, achieving the full homomorphism accordingly; after the pretreatment it can greatly accelerate the decryption speed and reduce the complexity of the operations.

C. The Safety Analysis on the Improved Scheme.

The safety of such scheme is based on partially approximate greatest common divisor (GCD), which is similar with the DGHV scheme. Its safety grade has reached the IND-CPA security. which was proved in literature [7]. Till now the problem of the greatest common divisor still cannot be solved, so this scheme shall meet with the safety requirement. At the same time, by introducing the sparse subset and problem into the compressed decryption algorithm in this paper, it further guarantees the safety of the algorithm mentioned in this paper.

D. The Comparison between the Improved Scheme and DGHV Scheme

The full homomorphic encryption scheme based on the integers that proposed by Dijk et al shall be the first full homomorphic encryption scheme based on the integers, and the improved Somewhat homomorphic encryption scheme that with quite small public key size is also based on the integers too. Then the comparison is made between the improved scheme and the DGHV scheme in aspects of safety and efficiency etc. The indices used to measure the safety property are mainly the safety grade of the scheme, the difficult problem hypothesis based on etc; and the indices influencing the efficiency of the scheme shall be the size of private/public key, the complexity of the encryption/decryption algorithm, the throughput capacity of the algorithm etc. As shown in Table I:

TABLE I. THE COMPARISON BETWEEN DGHV SCHEME AND IMPROVED SCHEME

Scheme name	DGHV scheme	Improved scheme
Safety grade	IND-CPA	IND-CPA
Continuity	good	good
Difficulty-based problem	The problem of approximate greatest common divisor, sparse subset and problem	The problem of partially approximate greatest common divisor, sparse subset and problem
Size of public key	$\tilde{O}(\lambda^{10})$	$\tilde{O}(\lambda^{7})$
Size of private key	$\tilde{O}(\lambda^{2})$	$\tilde{O}(\lambda^{2})$
The data volume can be encrypted in one time	1bit	3bit

From the comparison in Table I it can be easily found that, the improved scheme remained the advantage of the full homomorphic encryption scheme based on the integers in the aspect of difficulty-based problem, and its safety grade also reaches the IND-CPA standard. For the sufficiency aspect, it lowered the size of public key and increased the data volume that can be encrypted in one time and reduced the complexity of encryption/ decryption process and accelerated the encryption speed, which will greatly improve the ability of the algorithm on data processing.

IV. The Application of Improved Scheme on the Cloud Storage Platform

After using the improved full homomorphic encryption scheme to encrypt the data in the cloud storage environment, with the premise of the data safety guarantee during the transmission and storage process, it can realize the retrieval on the encrypted text without decryption, in comparison with traditional encryption methods, which can greatly shorten the encryption/decryption process, reduce the computing complexity and improve the efficiency accordingly. And the improved scheme shall also have the good continuity, lower computing complexity and higher efficiency characters, improve the information retrieval speed of the cloud storage platform, the application of the improved scheme in the cloud storage environment is shown in Figure I and II:

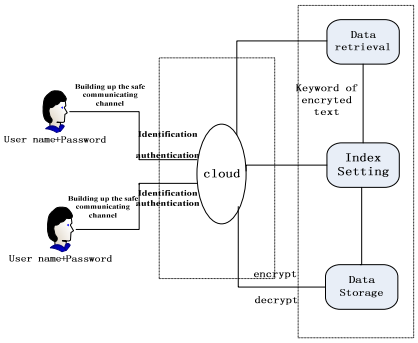

FIGURE I. CLOUD STORAGE PLATFORM

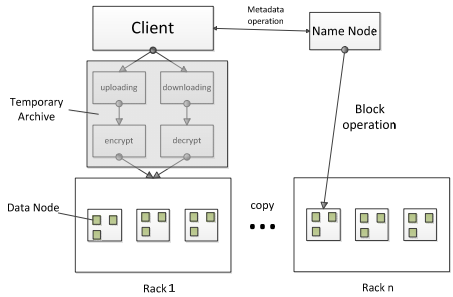

FIGURE II. THE DHFS DISTRIBUTED FILE SYSTEM

Through the identification authentication on the cloud server, the users can set up the safety communicating channel with the cloud storage platform, to guarantee the safety of data transmission process. The client end at cloud storage platform shall upload/ download the data to a temporary space in the local hard disk of the server that HDFS may locate in, then to encrypt/ decrypt the data accordingly, to carry out the copying, segmenting operation on the data and store them into the matching data nodes. While the users propose to make retrieval operation on the data, the client end shall set up the index and generate the key word for retrieval of the encrypted text, through MapReduce technology to make retrieval on the encrypted text. Once it got the result, they shall be decrypted by the data encryption decryption engine and then transmitted from the client end to the user end.

V. CONCLUSION

Through study and analysis on domestic and foreign results related to full homomorphic encryption technique, this paper proposed such a full homomorphic encryption algorithm depending on the basis of current domestic study results, but this method may also have certain gap in comparison with the efficiency of traditional encryption scheme in the aspects of public key size, computing complexity etc after the improvement. So it may still need further study continuously in such field, to reduce computing complexity, improve computing efficiency and enhance the safety accordingly.

ACKNOWLEDGMENT

This work is supported in part by National Natural Science Foundation of China (No. 61402529) and National Natural Science Foundation of Shaanxi Province, China (No. 2015JQ6266).

REFERENCES

[1] Fan Liu, Ming Yang. Ciphertext policy attribute based encryption scheme for cloud storage [J]. Application Research of Computers,2012,4(29):1452-1456.

[2] RIVEST R L,ADLEMAN L,DERTOUZOS M L. On data banks and privacy homomorphisms [J]. Fou-ndations of Secure Computation,1978,4(11):169-180.

[3] Gentry C. Fully homomorphic encryption using ideal lattices[C]//STOC'09,2009:169-178.

[4] Gentry C.A fully homomorphic encryption scheme [D/OL]. Stanford University,2009.http://crypto.stanford.edu/craig.

[5] Dianhua Tang, Shixiong Zhu, Yunfei Cao. Faster fully homomorphic encryption scheme over integer[J]. Computer Engineering and Applications,2012,48(28):117-122.

[6] Rulei Lin, Jian Wang, He Du. Improved fully homomorphic encryption over integers[J]. Application Research of Computers,2013,5(30):1515-1519

[7] van Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [C] // Proceedings of EUROCRYPT 2010.Riviera, French: [s.n.],2010:24-43