Konuralp Journal of Mathematics
Volume 4 No. 1 pp. 122–129 (2016) ©KJM

A SYMMETRIC KEY FULLY HOMOMORPHIC ENCRYPTION SCHEME USING GENERAL CHINESE REMAINDER THEOREM

EMİN AYGÜN AND ERKAM LÜY

Abstract. The Fully Homomorphic Encryption (FHE) was an open problem up to 2009. In 2009, Gentry solved the problem. After Gentry's solution, a lot of work have made on FHE. In 2012, Xiao et al suggested a new FHE scheme with symmetric keys. They proved that security of their scheme depends on large integer factorization. In their scheme, they used $2m$ prime numbers in keygen algorithm and they used Chinese Remainder Theorem (CRT) in encryption algorithm. In 2014, Vaudenay et al broken this scheme. In this paper we present a new FHE scheme with symmetric keys which is a little different from Xiao et al scheme. We extend the approach with using General Chinese Remainder Theorem (GCRT). With using GCRT, we obtained a new FHE scheme and also we achieved to avoid choosing $2m$ prime/mutually prime numbers. Our scheme works with random numbers.

1. Introduction

The privacy homomorphism idea was introduced in 1978 by Rivest, Adleman and Dertouzos in [1]. In 1982, S. Goldwasser and S. Micali made Goldwasser-Micali cryptosistem [3], and a generalization of this system which is called Pailler cryptosystem [4] presented in 1999. Some cryptosystems homomorphic according to a single operation. RSA and El-Gamal (known cryptosystems) are homomorphic according to multiplication [2]. Pailler cryptosystem is homomorphic according to addition.

None of the mentioned cryptosystems above does not provide the feature of being homomorphic for both two operations. They are homomorphic for just one operation. Only addition or only multiplication.

It is very well known that making any arbitrary operation on encrypted data is very important for privacy. Up to 2009, when Gentry suggested first FHE Scheme [5], this was an open problem. After Gentry's solution, many cryptographers made a lot of study on it for doing it more practice and more secure.

Date: January 1, 2013 and, in revised form, February 2, 2013.
2010 *Mathematics Subject Classification.* 11T71,94A60,68P25.
Key words and phrases. Fully Homomorphic Encryption, Large Integer Factorization, General Chinese Remainder Theorem.

In 2011 Vaikuntanathan, in his article [6], asked some questions like can be build any FHE scheme whose security based on problems in number theory? What can be said about factorization and DLP?

Dealing with this subject a study conducted in 2012, authors built a FHE scheme [7]. They proved that security of their scheme is based on factorization problem. Also they used CRT and matrices type $4x4$. After that this study was developed by C. P. Gupta and Iti Sharma [8] and [9]. In 2014, Vaudenay and Vizar broken schemes [7], [8] and [9] in their study [12].

In this paper we present a new scheme with using GCRT. Our scheme is fully homomorphic, symmetric and main idea of our scheme is same with [7].

Main difference of our scheme is that we achieve FHE with random numbers which used in keygen algorithm. Our idea was avoiding from choosing $2m$ prime / mutually prime numbers. In this paper we showed how we achieved this.

Note that security of our scheme is depend on large integer factorization problem too. But attack in [12] can break our scheme too. But there is a big difference in our scheme. We use GCRT first time in cryptography and we achieved FHE with random numbers.

Rest of paper designed as follows: in section 2 we gave CRT, GCRT and scheme in [7]. In section 3 we introduce our scheme. Section 4 contains proof and homomorphism of our scheme. We showed differences between [7] and our scheme in section 5. In section 6 there is a simple example of our scheme and section 7 contains security and conclusions.

2. CRT, GCRT and Scheme suggested in [7]

Chinese Remainder Theorem Suppose the positive integers $m_1, m_2, m_3, ..., m_k$ are coprime in pairs, that is $(m_i, m_j) = 1$ for all i, j where $i \neq j$, then the set of congruences $x \equiv c_i (mod\ m_i)$ for $i = 1, 2, ..., k$ has a unique common solution modulo m where $m = m_1.m_2.m_3...m_k$ [10].

General Chinese Remainder Theorem A necessary and sufficient condition that the system of congruences $x \equiv c_i (mod\ m_i)$ for $i = 1, 2, ..., k$ be solvable is that for every pair of indices i, j between 1 and k inclusive, $(m_i, m_j)|(c_i - c_j)$. The solution, if exists, is unique modulo the least common multiple of $m_1, m_2, m_3, ..., m_k$ [11].

Scheme suggested in [7]

Keygen

(1) Choose $2m$ prime numbers p_i and q_i , for $1 \leq i \leq m$. This extended to $2m$ odd numbers which are mutually prime in [8] and [9].
(2) Let $f_i = p_i.q_i$ and $N = \prod_{i=1}^{m} f_i$.
(3) Pick an invertible matrix $k \in M_4(Z_N)$.
(4) Public key is $\{N\}$ and secret key is $\{k, f_i\}$.

Encryption

(1) Choose a random value $r \in Z_N$.
(2) Choose plaintext $x \in Z_N$.
(3) Construct a matrix $X_{m.3}$ such that each row has only one element equal to x, and other two equal to r.

(4) Using Chinese Remainder Theorem, let a, b, c be solution to the set of simultaneous congruences $a = a_i \ mod \ f_i$, $b = b_i \ mod \ f_i$, $c = c_i \ mod \ f_i$, for $1 \leq i \leq m$.
(5) Compute k's inverse as $k^{-1} \in M_4(Z_N)$
(6) Ciphertext is $C = (k^{-1}.diag(x, a, b, c).k) \ (mod \ N)$.

Decryption

(1) Given ciphertext C and key k, the decryption algorithm computes the plaintext $x = (k.C.k^{-1})_{11} \ (mod \ N)$.

3. Our Scheme with GCRT

The algorithm is as follows:

Keygen

(1) Choose randomly $2m$ numbers p_i and q_i , for $1 \leq i \leq m$.
Remark 1: It is very important that p_i and q_i are not prime and not mutually prime.
(2) Let $f_i = p_i.q_i$ and $N = \prod_{i=1}^{m} f_i$.
(3) Evaluate $(f_1, f_2, ..., f_m) = a$.
Remark 2: If m value is bigger, then the probability of being $a > 1$ is quite small but even if $a = 1$ then our scheme reduces to original one. Also if $a > 1$ then we generalize the original one. So for small values of m, our scheme is more useful.
(4) Compute $\frac{N}{a} = N_1$.
(5) Pick an invertible matrix $k \in M_4(Z_{N_1})$.
(6) Public key is $\{N_1\}$ and secret key is $\{k, f_i\}$.

Encryption

(1) Take the keys.
(2) Determine your plaintext as $x \in Z_{N_1}$.
(3) Compute k's inverse as $k^{-1} \in M_4(Z_{N_1})$.
(4) Evaluate $(f_1, f_i) = b_j$, for $2 \leq i \leq m$ and $1 \leq j \leq m-1$.
Remark 3: It is enough that only evaluate $(f_1, f_i) = b_j$ for $2 \leq i \leq m$ and $1 \leq j \leq m-1$ because the matrix which construct in step 6's type is $m.3$ and in step 7 we use this matrix's coloumns for GCRT. So if $m \geq 3$ we will have same element as previous rows because of we will take only one x plaintext each row. In the $m.$ row other two element will be equal to r. So if this element both x or r it will be same with one of previous elements. So property of GCRT, differnces of mod values will absolutely divide the differences of x and r because $x - x = 0$ and $r - r = 0$ and every value can divide 0. So evaluate $(f_1, f_i) = b_j$ is enough for applicate GCRT.
(5) Chose a r like that seperately for every j, $b_j | x - r$, $r \neq x$ and $r \in Z_{N_1}$. If does not provide this condition, chose again.
Remark 4: For applicate GCRT we must chose like above. If we don't chose like above, differences of mod values will not divide the values which is front the mod.
Remark 5: Also we can easily show that there is at least a certain r such that which provides the above conditions.
Let

$$\begin{aligned}(f_1, f_2) &= b_1\\ (f_1, f_3) &= b_2\\ (f_1, f_4) &= b_3\\ &\vdots\\ (f_1, f_m) &= b_{m-1}\end{aligned}$$

so we are looking for a r such that

$$\begin{aligned}b_1 &\mid x - r\\ b_2 &\mid x - r\\ b_3 &\mid x - r\\ &\vdots\\ b_{m-1} &\mid x - r\end{aligned}$$

if $b_1|x - r$ than $r \equiv x(mod\ b_1)$ and with same idea if $b_2|x - r$ than $r \equiv x(mod\ b_2)$, ... and if $b_{m-1}|x - r$ than $r \equiv x(mod\ b_{m-1})$.

So because of $x - x = 0$ and every number can divide 0 than from GCRT there must be a solution. So we guarantee a value of r.

(6) Construct a matrix $X_{m.3}$ such that each row has only one element equal to x, and other two equal to r.
(7) Using General Chinese Remainder Theorem, let a, b, c be solution to the set of simultaneous congruences $a = a_i\ mod\ f_i$, $b = b_i\ mod\ f_i$, $c = c_i\ mod\ f_i$, for $1 \leq i \leq m$.
(8) Ciphertext is $C = (k^{-1}.diag(x, a, b, c).k)\ (mod\ N_1)$.

Decryption

(1) Given ciphertext C and key k, the decryption algorithm compute the plaintext $x = (k.C.k^{-1})_{11}\ (mod\ N_1)$.

4. Proof and Homomorphism of Our Scheme

Theorem 4.1. *The encryption scheme is correct.*

Proof. $((k^{-1})^{-1}(k^{-1}diag(x, a, b, c)k)k^{-1})_{11} = diag(x, a, b, c)_{11} = x$

□

Theorem 4.2. *The multiplication and addition algorithms are correct.*

Proof. Let $E(x, k)$ and $E(y, k)$ represent chiphertext of respectively plaintext x and y under the key k.

First we show that addition is correct.

$$\begin{aligned}E(x, k) + E(y, k) &= [k^{-1}.diag(x, a, b, c).k] + [k^{-1}.diag(y, d, e, f).k]\\ &= k^{-1}.(diag(x, a, b, c) + diag(y, d, e, f)).k\\ &= k^{-1}.(diag(x + y, a + d, b + e, c + f)).k\\ &= E(x + y, k)\end{aligned}$$

So scheme is additional homomorphic. Secondly we show that multiplication is correct.

$$\begin{aligned} E(x,k).E(y,k) &= [k^{-1}.diag(x,a,b,c).k].[k^{-1}.diag(y,d,e,f).k] \\ &= k^{-1}.(diag(x,a,b,c).diag(y,d,e,f)).k \\ &= k^{-1}.(diag(x.y,a.d,b.e,c.f)).k \\ &= E(x.y,k) \end{aligned}$$

So scheme is multiplicational homomorphic. Thus scheme is fully homomorphic. □

Note that above two theorems are taken from [7]. Also in our encryption scheme we use matrix like in [7]. So this two theorems are valid for our scheme.

5. Differences between Xiao et al.'s scheme and our scheme

Xiao et al.'s Scheme	**Our Scheme**
Keygen	**Keygen**
$2m$ prime	$2m$ random
f_i values must be different	f_i values can be same
	Compute $(f_1, f_2, ..., f_m) = a$
	Compute $\frac{N}{a} = N_1$
Pick an inversible matrix $k \in M_4(Z_N)$	Pick an inversible matrix $k \in M_4(Z_{N_1})$
Public Key $\{N\}$ and Secret Key $\{k, f_i\}$	Public Key $\{N_1\}$ and Secret Key $\{k, f_i\}$
Encryption	**Encryption**
Take Public and Secret Key	Take Public and Secret Key
Determine plaintext in *mod* N	Determine plaintext in *mod* N_1
Compute k^{-1} matrix in *mod* N	Compute k^{-1} matrix in *mod* N_1
	Evaluate $(f_1, f_i) = b_j$, for $2 \leq i \leq m$ and $1 \leq j \leq m-1$
Chose a random r	Chose a r like that seperately for every j, $b_j \vert x - r$, $r \neq x$ and $r \in Z_{N_1}$. If does not provide this condition, chose again.
Construct a matrix $X_{m.3}$ such that each row has only one element equal to x, and other two equal to r.	Construct a matrix $X_{m.3}$ such that each row has only one element equal to x, and other two equal to r.
Solve congrances with Using CRT	Solve congrances with Using GCRT
Ciphertext is $C = (k^{-1}.diag(x,a,b,c).k)$ $(mod\ N)$	Ciphertext is $C = (k^{-1}.diag(x,a,b,c).k)$ $(mod\ N_1)$
Decryption	**Decryption**
Compute $x = (k.C.k^{-1})_{11}$ $(mod\ N)$	Compute $x = (k.C.k^{-1})_{11}$ $(mod\ N_1)$

6. Example of Our Scheme

A simple example of our scheme is following:

Keygen

(1) Let $m = 2$ and consider p_i and q_i values $p = (3, 8)$, $q = (6, 10)$.

(2) $f_1 = 3.6 = 18$ and $f_2 = 8.10 = 80$ so that $N = f_1.f_2 = 18.80 = 1440$.
(3) Compute $(f_1, f_2) = a = (18, 80) = 2$.
(4) Compute $\frac{N}{a} = N_1$ is $\frac{1440}{2} = 720$.
(5) We randomly chose the key $k = \begin{pmatrix} 17 & 44 & 25 & 126 \\ 91 & 121 & 84 & 85 \\ 85 & 71 & 119 & 25 \\ 0 & 85 & 57 & 44 \end{pmatrix}$ matrix $(mod 720)$.
(6) Public key is $\{N_1 = 720\}$ and secret key is $\{k, f_1 = 18, f_2 = 80\}$.

Encryption:

(1) Take the keys $\{N_1, k, f_1, f_2\}$.
(2) Determine plaintext as $x = 42 \in Z_{720}$.
(3) Compute k's inverse matrix $k^{-1} = \begin{pmatrix} 605 & 181 & 329 & 120 \\ 146 & 123 & 449 & 611 \\ 146 & 253 & 403 & 566 \\ 347 & 711 & 296 & 1 \end{pmatrix}$ $(mod 720)$.
(4) Compute $(f_1, f_2) = (b_j) = (18, 80) = 2$.
(5) To be $r \in Z_{720}$, $r \neq x = 42$ and $2|42 - r \longrightarrow 42 - r = 2k \longrightarrow r = 42 - 2k$ for $k = -25$ $r = 92$ chosen.
(6) For $m = 2$ so we construct $m.3 = 2.3$ type $X = \begin{pmatrix} 92 & 42 & 92 \\ 92 & 92 & 42 \end{pmatrix}$ matrix.
(7) This gives us the linear congruences as follows:
a) $a \equiv 92(mod\ 18)$
$a \equiv 92(mod\ 80)$
b) $b \equiv 42(mod\ 18)$
$b \equiv 92(mod\ 80)$
c) $c \equiv 92(mod\ 18)$
$c \equiv 42(mod\ 80)$
If we solve the congruences with using GCRT, solutions are $a \equiv 92(mod\ 720)$, $b \equiv 492(mod\ 720)$, $c \equiv 362(mod\ 720)$.
Encryption proceeds as :
(8) $C = (k^{-1}.diag(x, a, b, c).k) = \begin{pmatrix} 2 & 440 & 150 & 500 \\ 300 & 142 & 390 & 80 \\ 140 & 180 & 492 & 520 \\ 90 & 110 & 600 & 352 \end{pmatrix}$ $(mod 720)$.

Decryption:

(1) Is done as: $x = (k.C.k^{-1})_{11} = \begin{pmatrix} 42 & 0 & 0 & 0 \\ 0 & 92 & 0 & 0 \\ 0 & 0 & 492 & 0 \\ 0 & 0 & 0 & 362 \end{pmatrix} = 42$ $(mod 720)$.

For example of homomorphism of our scheme; if we encrypt $x_2 = 5 \in Z_{720}$ plaintext

we obtain this chiphertext: $C_2 = \begin{pmatrix} 93 & 40 & 570 & 700 \\ 564 & 1 & 474 & 400 \\ 484 & 108 & 707 & 440 \\ 198 & 226 & 264 & 655 \end{pmatrix}$ $(mod\ 720)$.

So $C_1 + C_2 = \begin{pmatrix} 95 & 480 & 0 & 480 \\ 144 & 143 & 144 & 480 \\ 624 & 288 & 479 & 240 \\ 288 & 336 & 144 & 287 \end{pmatrix}$ $(mod\ 720)$

and decryption of $C_1 + C_2$ is $\begin{pmatrix} 47 & 0 & 0 & 0 \\ 0 & 95 & 0 & 0 \\ 0 & 0 & 335 & 0 \\ 0 & 0 & 0 & 527 \end{pmatrix}$ $(mod\ 720)$.

Really addition of x_1 and x_2 is 47.

So our scheme is additional homomorphic.

With same idea $C_1.C_2 = \begin{pmatrix} 186 & 120 & 630 & 660 \\ 108 & 342 & 198 & 480 \\ 588 & 36 & 84 & 600 \\ 666 & 462 & 648 & 360 \end{pmatrix}$ $(mod\ 720)$

and decryption of $C_1.C_2$ is $\begin{pmatrix} 210 & 0 & 0 & 0 \\ 0 & 276 & 0 & 0 \\ 0 & 0 & 516 & 0 \\ 0 & 0 & 0 & 690 \end{pmatrix}$ $(mod\ 720)$.

Really multiplication of x_1 and x_2 is 210.

So our scheme is multiplicational homomorphic. So our scheme is fully homomorphic.

7. Security and Conclusion

In [7] authors proved that the security of their scheme based on factorization problem. Security assumptions of our scheme is same with this scheme. Additionally D. Vizar and S. Vaudenay have broken this scheme in 2014. They broken the scheme with a known plaintext key-recovery attack. Also they can break our scheme with same attack.

But difference of our scheme is that our scheme allows using random numbers in keygen algorithm and we use first time GCRT.

As a conclusion of this paper, we extended the study on [7]. We designed a new FHE scheme which uses GCRT and allows using random numbers in keygen algorithm.

References

[1] R. Rivest, L. Adleman and M. L. Dertouzos, *On data banks and privacy homomorphisms* Foundations of Secure Computation, 169-170, 1978.

[2] A. Silverberg, *Fully Homomorphc Encrypton for Mathematcans* sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750- 13-2-0054. 2013.

[3] S. Goldwasser and S. Micali, *Probabilistic encryption and how to play mental poker keeping secret all partial information* in proceedings of the 14th ACM Symposium on Theory of Computing, 365-377, 1982.

[4] P. Pailler, *Public-Key Cryptosystems Based on Composite degree Residuosity Classes* in Advances in Cryptology, EUROCRYPT, 223-238, 1999.

[5] C. Gentry, *A Fully Homomorphc Encrypton Scheme* phd thesis, Stanford University, 2009.

[6] V. Vaikuntanathan, *Computing Blindfolded: New Developments in Fully Homomorphic Encryption* 52nd Annual Symposium on Foundations of Computer Science,5-16, 2011.

[7] L. Xiao, O. Bastani and I-Ling Yen, *An Efficent Homomorphic Encryption Protocol for Multi-User Systems* iacr.org, 2012.

[8] C. P. Gupta and I. Sharma, *Fully Homomorphic Encryption Scheme with Symmetric Keys* Master of Technology in Department of Computer Science & Engineering, Rajasthan Technical University, Kota, August - 2013.
[9] C. P. Gupta and I. Sharma, *A Fully Homomorphic Encryption scheme with Symmetric Keys with Application to Private Data Processing in Clouds, Network of the Future (NOF)* Fourth International Conference on the Digital Object Identifier: 10.1109/NOF.2013.6724526, Page(s): 1 - 4 IEEE CONFERENCE PUBLICATIONS, 2013.
[10] H. E. Rose, *A Course n Number Theory* School of Mathematics , niversity of Bristol,1988.
[11] W. J. Leveque, *Topics in Number Theory* Addison-Wesley Publishing Company, University of Michigan, 35-35, 1965.
[12] D. Vizar and S. Vaudenay, *Cryptanalysis of Chosen Symmetric Homomorphic Schemes* EPFL CH-1015 Lausanne, Switzerland, 2014.

Erciyes University, Faculty of Science, Department of Mathematics, Kayseri 38200
E-mail address: eaygun@erciyes.edu.tr

Erciyes University, Faculty of Science, Department of Mathematics, Kayseri 38200
E-mail address: erkamluy@erciyes.edu.tr