ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal 8 (2019), no.3, 555–559
(Special issue on ICRAPAM)
ISSN 1857-8365 printed version
ISSN 1857-8438 electronic version

APPLICATION OF HX RING THEORY IN HOMOMORPHIC ENCRYPTION

R. Muthuraj[1] , N. Ramila Gandhi[2]

[1]PG and Research Department of Mathematics,

H.H.The Rajah's College, Pudhukottai,Affiliated to Bharathidasan University, Tiruchirappalli,

Tamilnadu, India.E-mail: rmr1973@yahoo.co.in

[2]Department of Mathematics,PSNA College of Engineering and Technology, Dindigul, Research

Scholar, PG and Research Department of Mathematics,

H.H.The Rajah's College, Pudhukottai,Affiliated to Bharathidasan

University,Tiruchirappalli, Tamilnadu, India.E-mail:satrami@yahoo.com

Abstract: In abstract algebra, homomorphism is a structure preserving map between two algebraic structures. In homomorphic cryptosystem the user can perform operations on the encrypted data without decrypting the data and get the same result as performed on the original data.In this paper we introduce HX homomorphic encryption techniques.

Keywords: HX ring , homomorphism ,encryption, decryption, RSA algorithm.

AMS Subject Classification (2010): 20N25, 03E72, 03F055, 06F35, 03G25.

1. Introduction

Ring theory has been used in cryptography and many other computer tasks. The inclusion of ring theory in digital images, it is achieved by considering the image like a matrix in which the elements belong to finite cyclic ring Zn. Therefore the use of ring theory could be a good structure when one desires to juxtapose images due to the digital images present cyclical properties correlated with the pixel values. This property will allow to increase or decrease the difference among and will make possible to find the edges in the analysed images. The original message is called the plain text. The coded version is called the cipher text. The process of changing plaintext into cipher text is called coding or encryption. The process of changing cipher text back into plaintext is called decoding or decryption. Encryption is the transmutation of information into a cryptographic encoding that cannot be read without key. Encryption stratagem is additively homomorphic if there is a coherent estimable operator * on cipher texts such that $c_0 * c_1$is a valid cipher text that decrypts to the sum $m_0 + m_1$. If such operator * exists then the encryption and decryption functions are homomorphism, hence

the name homomorphic encryption. By running a sequence of mathematical operations, called an algorithm, on the binary data that contains an image, encryption software changes the values of the numbers in a foreseeable way. An image encrypted using homomorphic encryption scheme and can be accessed by deliberated persons by decrypting it using homomorphic decryption scheme. Homomorphic cryptosystem has been widely used all over the public cloud. There are two homomorphic characteristics one is additive homomorphic property of the Paillier algorithm and the other is multiplicative homomorphic property of RSA algorithm. A homomorphic cryptosystem has the property that when any specific algebraic operation is accomplished on the data input before encryption, the resulting encryption is same as if an algebraic operation is executed on the data input after encryption. In 1978 Rivest-Shamir-Adleman (RSA) [9] first researched the design of a homomorphic encryption scheme which is the suitable public key crypto system. In that paper he noted that addition to the algebraic system of the user, we shall need another algebraic system of to be used by the computer system. Encoding and decoding shall then mean mapping elements from one to another or vice versa, respectively. In order for the system to be able to operate on the (encoded) data base without decrypting it, the decoding function should be a homomorphism. In 1999[7] Pascal Paillier, created an algorithm for public key cryptography. This algorithm is an additivehomomorphic cryptosystem. A remarkable feature of Paillier cryptosystem is its homomorphic properties along with it non-deterministic encryption. In 1988, Professor Li Hong Xing [4] proposed the concept of HX ring and derived some of its properties. In HX ring theory we have discussed so many properties under homomorphism. Discussing the same techniques under HX ring theory will yield a better result.

2. RSA algorithm

2.1 Key generation algorithm

Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted. This algorithm takes security parameter as an input and produces secret key as output.

2.2 Encryption and decryption algorithm(RSA)

Read the input image. Select two distinct big prime numbers p and q which are used for calculating private key and public key. (When the value of prime numbers become smaller, the output result become poor, hence we have to select large prime numbers). Calculate $n = p.q$, $\varphi(n)=(p-1)(q-1)$, φ is Euler's totient function. Choose an integer 'e' such that $1<e<\varphi(n)$, $\gcd(e, \varphi(n)) =1$. Encrypted image is $C = E(PT) =M^e \bmod n$. Decryption algorithm is a deterministic algorithm which takes cipher text, secret key as an input and produces a plaintext as an output. $M =D(CT)= C^d \bmod n$.

2.3 Key space analysis

Key space analysis is a conception which governs the range of number of bits need to be used for a secret key. Key with more number of bits results in depletion of execution speed and a key with less number of bits will make attacks easier for prowlers. In order to provide more security, key space should be less than 2^{100}.

3. Homomorphism of HX ring

Definition 3.1 **HX ring**

Let R be a ring. In $2^R - \{\phi\}$, a non-empty set $\Re \subset 2^R - \{\phi\}$ with two binary operations ' + ' and '$\cdot$' is said to be a HX ring on R if $\Re$ is a ring with respect to the algebraic operation defined by

i. $A + B = \{a + b / a \in A \text{ and } b \in B\}$, which its null element is denoted by Q , and the negative element of A is denoted by – A.

ii. $AB = \{ab / a \in A \text{ and } b \in B\}$

iii. A (B + C) = AB + AC and (B + C) A = BA + CA.

That is, let $\Re$ be a nonempty subset of $P_0(R)$ such that $\Re$ forms a ring under the operations (i) and (ii).

Example 3.2 Let C^0 be the set of all nonzero complex numbers. The operations "⊕" and "⊗" of C^0 are defined as follows , $a \oplus b = ab$ and $a \otimes b = |a|^{\ln|b|}$ for all $a,b \in C^0$. Then $(C^0, \oplus, \otimes)$ forms a ring.
Let $I = (1, \infty)$ and $H = \{1, -1, i, -i\}$ then $\Re = \{a \oplus I / a \in H\}$ is an HX ring on $(C^0, \oplus, \otimes)$.

Definition 3.3 **HX Ring homomorphism**

A mapping f from a HX ring $\Re_1$ to a HX ring $\Re_2$ is said to be a homomorphism if for any $A, B \in \Re_1$,

i. $f(A+B) = f(A) + f(B)$
ii. $f(AB) = f(A) \cdot f(B)$.

Definition 3.4 **Homomorphic encryption**

Any encryption algorithm E( ) is said to be homomorphic if, given E(A) and E(B), one can obtain $E(A \oplus B)$ without decrypting E(A) and E(B). $E(A \oplus B) = E(A) \otimes E(B)$ where ⊕ and ⊗ can be addition or multiplication. A decryption D( ) is said to be homomorphic if $D(E(A) \otimes E(B)) = D(E(A \oplus B))$ and $D(E(A) \otimes E(B)) = A \oplus B$.

Paillier support homomorphic operation of addition modulo n over the plaintext. RSA supports homomorphic operation of multiplication modulo n.

HX Homomorphic encryption

Assume that plaintexts forms a HX ring (P ,+, .) and cipher texts forms a HX ring (C, + , .) then the encryption algorithm E is a map from a HX ring P to a HX ring C. That is, E: PC is either a secret key or a public key. For all A and B in P and if $E(A) \oplus E(B) = E(A \otimes B)$ the encryption scheme is homomorphic.

Example of homomorphic encryption and decryption(RSA)

Fig.1 illustrates an example of the proposed homomorphic encryption method using RSA algorithm. $C_1$and C_2 are encrypted images of the original images M_1 and M_2. C_1XC_2 is a valid encryption of M_1, M_2. The purpose of the proposed method is to safely share a secret image where pixels were grouped to reduce the load of encryption at each step. Therefore, basic mathematical homomorphic multiplication process is applied. Incremental multiplication of each encrypted image with another encrypted image results in a new encrypted image, which is sent into the homomorphic multiplication process till the secret encrypted image is input to give the final encrypted image. The decryption process is nothing but the reverse process of encryption. Since RSA is multiplicative homomorphic, the operations are changed to multiplication. Let p=23, q=13,e=5,d=53, $M_1(1,1) = 146$; $M_2(1,1) = 178$; $C_1(1,1) = 269$; $C_2(1,1) = 159$;$C_1 XC_2(1,1) = 42771$

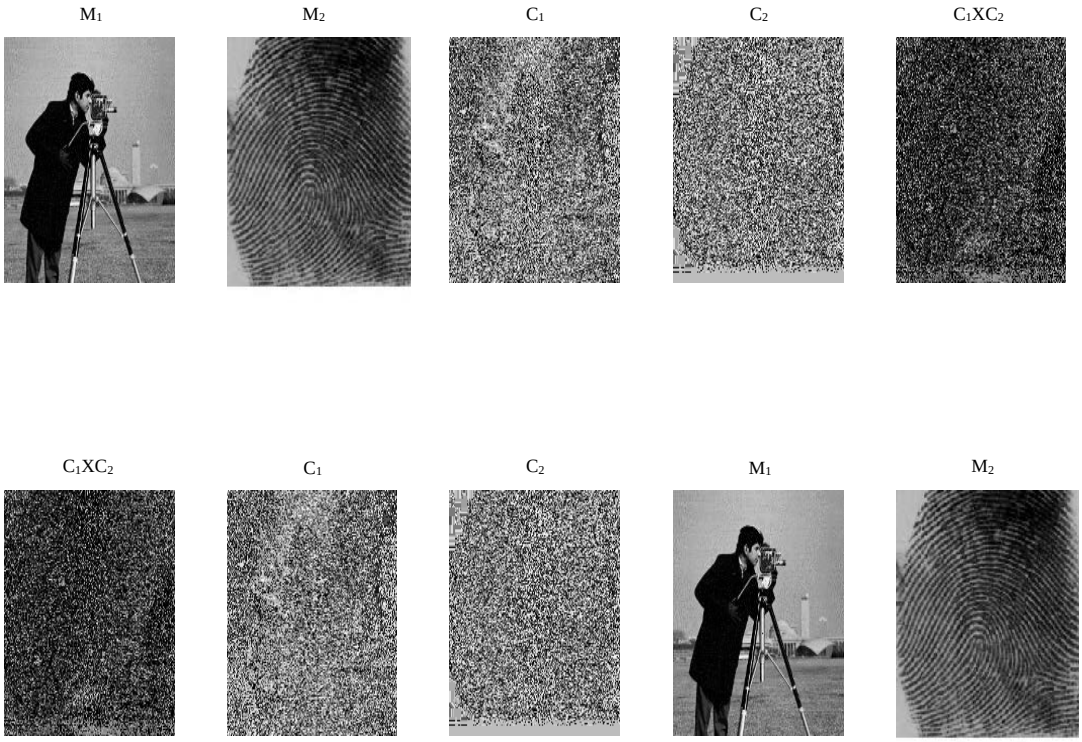

Fig.1

Overview of proposed method

Fig. 2 and Fig. 3 describes the purpose of the proposed scheme to securely share a secret image. If the number of rows and columns are not even by inserting arrow or column we will make into even. In order to form sets from each row first let us divide the elements(pixels) by number two. Since the number of elements in the row are even we will get i/2 number of sets(i- number of pixels in each row). Using maximum operation we compare the pixel values within the set and the maximum value obtained is transferred to another matrix and placed in its position and the minimum values were omitted. This will reduce the processing time and save the storage space. In this process a set is considered as an element. At the receiving end multiplicative homomorphic property is applied (during the extraction process).

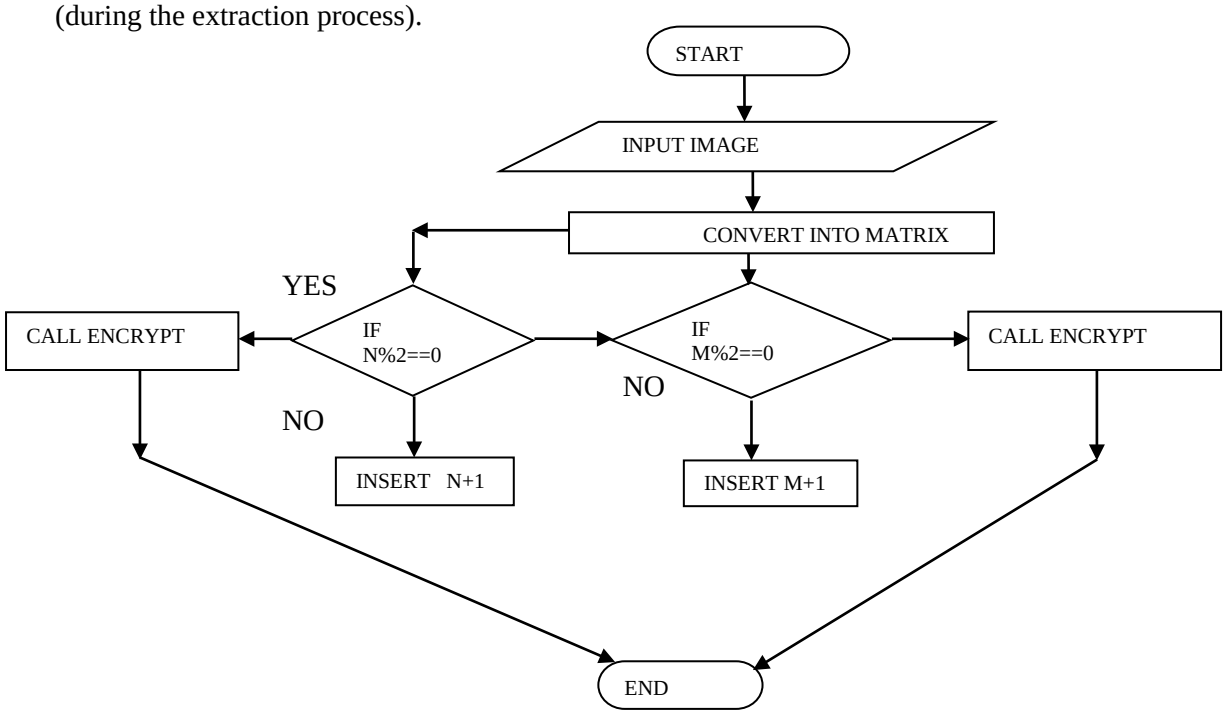

Fig. 2

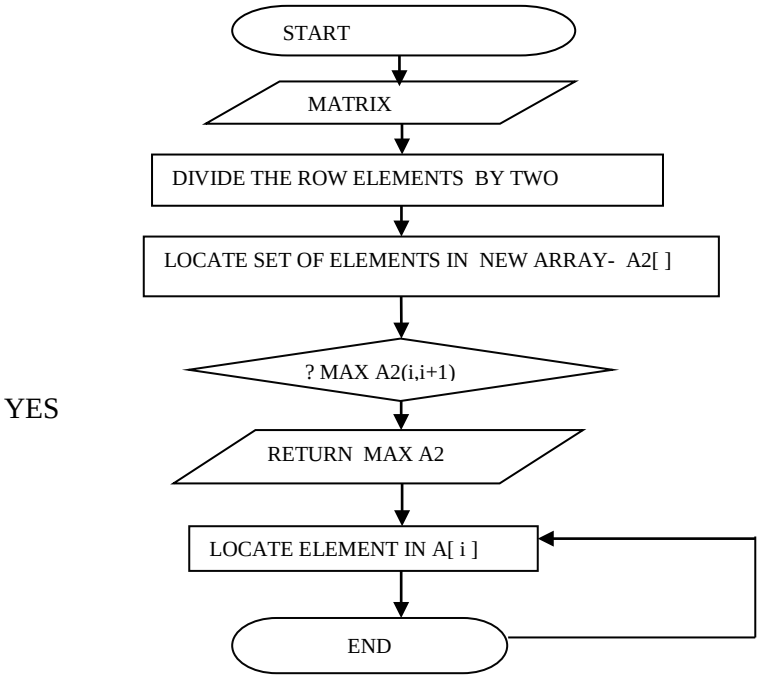

Fig. 3

4.Conclusion:

In this paper we proposed a method for sharing a secret image by multiplicative homomorphic property of RSA cryptosystem using the concept of HX ring theory. By grouping the elements in a row we can reduce the calculation time during encryption process and hence we can save storage space. At the same time decrypting the cipher text also takes considerably lesser time.

Acknowledgement:

I would like to thank my colleagues of P.S.N.A. college of engineering & Tech., for their valuable suggestions during the planning and development of this work. I am grateful to all of those with whom I have had the pleasure to work during this work.

References

[1] David J.Wu, Fully homomorphic encryption, Cryptography's Holy Grail.

[2] Dima Grigoriev,Ilia Ponomarenko,Homomorphic public-key cryptosystems over groups and rings, 2003, pp.1-15.

[3] Dinesh Kumar.G, Dontoju Pranay Teja, Sykam Sreekar Reddy, Saikala Devi.N, An efficient watermarking Technique for Biometric images,Science direct,Procedia Computer science 115(2017), pp. 423-430.

[4] Li Hong Xing, HX ring, BUSEFAL,34(1),pp. 3-8 ,(1988).

[5] Muthuraj.R, Ramila Gandhi.N, "Homomorphism on fuzzy HX ring", International Journal of Advanced Research in Engg., Tech.,& Sciences, Volume 3, Issue 7, July 2016, pp. 46-54.

[6] Naveed Islam, William Puech, Khizar Hayat, Robert Brouzer, Application of homomorphism to secure image sharing, Optic communication(2011), pp.1-18.

[7] Paillier.P.,Public-key cryptoystem baed on composite degree residuosity classe, In Eurocrypt,1999.

[8] R.L. Rivest, "RSA chips (past/present/future)," Ezlrocrypt'84, pp. 159-165.

[9] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Comm. ACM, vol. 21, pp. 12G126,1978.

[10] Ronald L. Rivest ,Len Adleman ,Michael L. Dertouzos, On data banks and Privacy homomorphisms, In foundations of secure computation4 , 11(1978),pp. 169-180.

[11] Xun Yi,Russell Paulet, Elisa Bertino,Homomorphic Encryption and Applications , Springer Briefs in Computer Science, 2014.

[12] Yasel Garces, Esley Torres,Osvaldo Pereira,Roberto Rodriguez, Application of the ring theory in the segmentation of digital images,Institute of Cybernatics, Mathematics and Phy, ,24 Nov 2014,pp.1-12.