VOL. 10, NO. 12, JULY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ANALYSIS OF HOMOMORPHIC CRYPTO SYSTEMS

K. Brindha and S. Sudha
School of Information Technology and Engineering, VIT University, Vellore Campus, Vellore, India
E-Mail: brindha.k@vit.ac.in, sudha.s@vit.ac.in

ABSTRACT

Homomorphic encryption technique does some changes manipulation to be done on the encrypted data without decrypting the encrypted data. The decryption of encrypted data is the same as if some changes done on the original data. There are some partial homomorphic encryption schemes used for some practical applications like electronic voting, e-cashing, multiparty computation and secret sharing etc., but they allow only certain specific computation on encrypted text. We describe how refreshing cipher text and Squashed decryption to play role on arbitrary computation on encrypted text in the fully homomorphic crypto system. In this paper based on the strengths and weaknesses of the existing homomorphic system we are doing the comparison of it.

Keywords: homomorphic encryption, computation, electronic voting e-cashing, refreshing cipher text, squashed decryption.

1. INTRODUCTION

Data security and secure communication are of great importance in growing digital and network communication. The security can be achieved by the use of cryptographic primitives [2]. Many of the cryptographic algorithms guarantee data confidentiality and privacy on data storage and retrieval. In case if any modification or computation on public storage required its creates complexity and violates security [3]. This can be solved by the homomorphic crypto system which performs operation on encrypted data that is reflected on the original data. It is an important feature in modern communication systems [4]. This important feature can be used for various applications secure voting, secret sharing scheme, commitment scheme, collision-resident hash functions, threshold scheme, anonymity, multiparty computation, privacy, private information retrieval scheme and finger printing.

The organization of the paper is as follows. Section 2 describes the homomorphic crypto systems. Section 3 discusses the various crypto system which uses homomorphic property. Section 4 gives the analysis of homomorphic systems and security aspects specified in Section 5 and finally we conclude the paper.

2. HOMOMORPHIC CRYPTO SYSTEM

It allows specific mathematical operation to be performed on cipher text without exposing the contents of the plain text. Consider two plaintexts M1 and M2 and their corresponding cipher texts EM1 and EM2. A homomorphic crypto system permits meaningful operation of M1 ° M2 from EM1 and EM2 without exposing M1 or M2 [1]. This crypto system mainly involves four algorithms such as key generation, Encryption, Decryption and Evaluation.

Figure-1. Homomorphic crypto system.

Key generation (μ)

It takes input security parameter μ and generates pair of keys are public and private key (Pu, Pr).

Encryption (Pu, M)

The given plaintext M is encrypted by public key and generates cipher text EM.

Evaluation (Pu, C, EM)

The evaluation performed on a set of encrypted text such that decrypting the result of the evaluation is same as the result of evaluation on the original data.

The cipher text evaluated based on the homomorphic property (additive or multiplicative) of crypto system. It takes input parameter public key Pu, a circuit C with s inputs and set of EM of cipher text EM_1, EM_2……, EMs. The given cipher text EM is decrypted by private key and generates plaintext M.

$$D_{Pr}(Eval_{Pu}(C,EM_1,EM_2,EM_3,\ldots\ldots\ldots..EM_s))=C(M_1,M_2$$

3. EXISTING HOMOMORPHIC CRYPTO SYSTEM

Based on the property of homomorphism, the crypto system classified into partially, somewhat and fully homomorphic crypto system.

3.1. Partially homomorphic crypto system

If the system performs any one of the mathematical operation such as addition, subtraction, multiplication, division and comparison on encrypted data then the crypto system is said to be the partially homomorphic crypto system. It can be additive or multiplicative crypto system based on the operation. We have discuss about some of the partially homomorphic crypto system.

3.1.1. Goldwasser - Micali scheme

The Goldwasser and Micali (GM) crypto system is the first probabilistic public encryption system which is probably secure [5]. The security of this crypto system is based on quadratic residuosity problem. In this scheme sender A encrypting individual plaintext bit as either random quadratic residues or non residue modulo N. The receiver B decrypts the message by testing the quadratic residuosity of the encrypted values using factorization of modulo N. GM scheme involves probabilistic key generation and encryption and deterministic decryption [7].

Key generation

Pick two large distinct prime numbers p and q.

Compute n = p * q.

Select $x \in Z_n$ such that x is non quadratic residue and Jacobi symbol x/n is 1.

Sender A's public key is (n, x) and private key is (p, q).

Encryption

Represent the given message M as a string of binary of length L.

$M = M_1, M_2 \ldots\ldots M_l$

for I = 1 to L

{

Select any $y \in Zn$ at random

If Mi = 1 then set EMi $\leftarrow y^2 \bmod n$,

else set EMi $\leftarrow x^2 \bmod n$.

}

Send Em -> $Em_1Em_2 \ldots .Em_l$ to receiver

Decryption

To recover the plain text M from EM, Sender A do the following

for I = 1 to L

{

Calculate legendre symbol ci = EMi/ p

If ci = 1 then set EMi $\leftarrow$0,

else set EMi $\leftarrow$1.

}

The decrypted message is $M_1M_2 \ldots\ldots M_l$

Security of Goldwasser - Micali scheme

The GM system has additive homomorphic property i.e.

$$E(b_1) * E(b_2) = y\, b_1 r_1^2\, yyb_2\, r_2^2 = y\,(b_1+b_2)\,(r_1 r_2)^2 = E$$

The security of this crypto system is based on quadratic residuosity hard problem. Hence this scheme is semantically secure.

3.1.2. Benaloh scheme

It is an advancement of the Goldwasser micali scheme. In this scheme block of data can be encrypted at once whereas in GM scheme each bit is encrypted individually [8]. This scheme involves key generation, message encryption and message decryption.

Key generation

Select two distinct large prime numbers P and Q.

Consider block size as R.

Compute N = P * Q.

Check R divides P-1.

Check R and P-1/R are co-prime.

Check R and Q-1 are co-prime.

Select $x \in Z^*_n$.

Sender public and private keys are (x, R, N) and (P, Q)

Message encryption

Select $U \in Z^*_n$.

Choose M is an element in Z_r.

Compute $E_r(M) = x^M U^R \bmod N$

Message decryption

Using private key, check whether m = 0

If R is small, decrypt the message using exhaustive search.

Security of Benaloh scheme

The Benaloh system has additive homomorphic property i.e. $E_r(M_1) * E_r(M_2) = (x^{M1}U_1^R)\,(x^{M2}U_2^R) = Er(M1 + M2)$. The security of this system based on higher residuosity problem. Given block size R, Modulus N and Cipertext Er(M), where factorization of N is unknown it is infeasible to determine plaintext [9].

3.1.3 Paillier scheme

It is one of the probabilistic asymmetric crypto systems. The system has additive homomorphic property. The system is based on arithmetic in the ring of integers modulo N^2 [10]. The cryptosystem is based on decisional composite residuosity assumption (DCRA) i.e. Given N (product of two large prime numbers P and Q) and an

integer Z, it is hard to find whether Z is an n^{th} residue modulo N^2 or not [11].

Key generation

Select two distinct large prime numbers P and Q.
Compute Euler's Totient ϕ(N) = (P-1) (Q-1).
Compute Carmichacel's function λ (N) = LCM (P-1, Q-1).
Pick random integer $x \in Z^*_{n^2}$.
Compute modular multiplicative inverse $\mu = (L (g^{\lambda} \bmod N2))^{-1} \bmod n$
Compute L (U) = U-1 / N.
Public and private keys are (N, P, Q) and (N, ϕ (N)).

Encryption

Consider message $M \in Z_n$.
Select random $R \in Z_n^*$
Compute Cipher text $E(M) = x^M R^N \bmod N^2$

Decryption

Consider E (M) be the message to decrypt, where $E(M) \in Z^*_{n^2}$.
Compute plaintext $M = L (E (M)^{\lambda} \bmod N^2) * \mu \bmod N$.

Security of Paillier scheme

The system provides semantic security against chosen plaintext attacks. The security of the system is based on decisional composite residuosity assumption. It has additive homomorphic primitive i.e. The product of two encrypted texts will decrypt to the sum of their corresponding original texts. $D(E(M_1R_1)* E(M_2R_2) \bmod N^2) = M_1 + M_2 \bmod N^2$ [12].

3.1.4. Damgard Jurik scheme

This probabilistic cryptosystem managed to generalize the paillier crypto system to higher moduli to enable more application [13]. It has additive homomorphic primitive.

Key generation

Select two distinct large prime numbers P and Q.
Compute Euler's Totient ϕ(N) = (P-1) (Q-1).
Compute Carmichacel's function λ (N) = LCM (P-1, Q-1).
Pick random integer $x \in Z^*_{n^{s+1}}$.

Using the CRT (Chinese Remainder Theorem) select r such that $r \bmod n \in Z^*_n$ and $r = 0 \bmod \lambda$.
The public and private keys are (N, x) and r.

Encryption

Consider message $M \in Z^*_{n^s}$.
Pick random $R \in Z^*_{n^{s+1}}$.
Compute Cipher text $E(M) = x^M R^{Ns} \bmod N^{s+1}$.

Decryption

Consider $E(M) = x^M R^{Ns} \bmod N^{s+1}$.
Compute $E(M)^r \bmod N^{s+1}$.
Let $E(M)^r = (1+N)^M \bmod N^{s+1}$.

Apply recursively paillier system to get the original message.

Security of Damgard Jurik scheme

The security of this system based on decisional composite residuosity assumption similar to paillier system. It has additive homomorphic primitive. This system is semantically secure if it is hard to decide if two given elements are in the same coset.

3.1.5. Okamoto and Uchiyama scheme

It is one of the probabilistic encryption schemes. This scheme provides efficient solution for discrete logarithm problem solved in polynomial time over specific group. It is semantically secure under subgroup assumption [14]. In this system modulus N is of the form p^2q.

Key generation

Consider two large distinct prime numbers P and Q.
Compute $N = P^2 * Q$.
Let $g \in Z^*_n$ such that $g \neq 1 \bmod P^2$.
Compute $h = g^N \bmod N$.
Public and private keys are (N,g,h) and (P,Q).

Message encryption

Consider $M \in Z_n$.
Pick $r \in Z_n$.
Compute $E(M) = g^M h^r \bmod N$.

Message decryption

Let L(x) = x-1 / P.
Compute plaintext $M = (L (E (M)^{P-1} \bmod P^2) / (g^{P-1} \bmod P^2) \bmod n$

Security of Okamoto and Uchiyama scheme

The security of this system based on factorization of modulus N. The system is semantic security under P subgroup assumption; hence it is difficult to determine an element $x \in Z_n$.

3.1.6. Unpadded RSA Scheme

The system is multiplicative homomorphic primitive. i.e. The multiplication of two cipher texts is equal to the multiplication of original messages. Consider two plaintext messages M_1, M_2 and the corresponding encrypted messages are M_1^e, M_2^e [15]. $E(M_1)*E(M_2) = M_1^e M_2^e \bmod N = (M_1*M_2)^e \bmod N = E(M_1 * M_2)$.
$D ((M_1*M_2)^e \bmod N = M_1 * M_2 \bmod N$

The security of this system is based on integer factorization problem. Chosen cipher text attack is possible due to this multiplicative property.

3.1.7. El Gammal scheme

It is one of the probabilistic public key crypto systems. The system is multiplicative homomorphic primitive. Practically it used to encrypt the secret key of symmetric crypto system.

Decrypting the multiplication of two cipher texts is equal to the multiplication of original messages [16]. The public and private key of this system are (g, h, q) and x. Consider two plaintext messages M_1, M_2 with nonces k1, k2 and the corresponding encrypted messages are

$E(M_1, k_1) = (y_1, y_2) = (g^{k1} \bmod q, M_1 h^{k1} \bmod q)$

$E(M_2, k_2) = (y_3, y_4) = (g^{k2} \bmod q, M_1 h^{k2} \bmod q)$

Multiplying the two encrypted message yield

$E(M_1, k_1) * E(M_2, k_2) = (y_1, y_2) * (y_3, y_4) = (g^{k1+k2}, M1M2\ h^{k1+k2})$

$D(E(M_1, k_1) * E(M_2, k_2)) = M_1 * M_2$

3.2. Somewhat homomorphic system

The crypto system considered to be somewhat homomorphic system if it deals with limited number of addition and multiplication on encrypted data.

3.2.1. Boneh-Goh -Nissim scheme

It is the first crypto system which allows both additions and multiplications with constant size encrypted data. It operates in two groups G1 and G2. The order of group G1 and G2 are p and q. The groups G1 and G2 possess a polynomial time bilinear map [18].

e: G1 * G2 -> G2 such that G = e(g, g) generates G

Bilinearity implies that $\forall u,v \in G1$ and $\forall a,b \in Z$, $e(u^a, v^b) = e(u, v)^{ab}$.

Key generation

Consider p, qs are two distinct primer number order of group G1 and G2.

Compute n = p * q.

Select randomly $u \in G1$.

Compute $h = u^q$.

Public and private keys are (n, G1, G2,g, h).

Encryption

Consider message M.

Select randomly $r \in Z_n$.

Compute $E(M) = g^M h^r$.

Decryption

Compute $M = \log_g^p (E(M)^p)$.

Security of Boneh-Goh-Nissim

This system semantically secure under subgroup decision problem. It exploits additive homomorphism and its one time multiplicative homomorphic property [17].

3.3. Fully Homomorphic cryptosystem

The crypto system considered fully homomorphic system if it deals with arbitrary addition and multiplication on encrypted data.

3.3.1. Gentry's scheme

In somewhat homomorphic scheme the limited number of multiplication and addition can be performed on the encrypted data [22]. The noise is created during each encryption, which goes on increasing, when we perform homomorphic operations on the encrypted data and it sometimes it becomes difficult to get the correct decryption of the encrypted data. To make the system to be fully homomorphic Gentry develop the two techniques 1. Cipher text refresh procedure and 2.Squashed decryption procedure.

Cipher text refresh procedure

The general idea is to refresh a cipher text, given a cipher text E(M) for some original text M, compute a cipher text E(M)' such that the size of the noise in E(M)'is lower than the size of the noise in E(M). Refreshing a cipher text is operation of recrypt the cipher text and encrypts the secret key. The new cipher text E(M)' encrypts the same message, but it maintains smaller noise.

E (M)' = Recrypt (Encrypt (Pr), Encrypt (E (M)).

D (E (Pr), E (M)') = D (Pr, E (M)).

Squashed decryption

The decryption procedure uses a sparse subset of values that adds up to the private key instead of original private key. Decrypt the expanded cipher text with new private key produce the original data.

Gentry's scheme over system of integers [19] involves key generation, encryption and decryption process

Key generation

Select a random odd integer P.

Encryption

Consider bit $M \in \{0, 1\}$.

Let M' = M mod 2 (ie M' is odd if M = 1 and M' is even if M = 0.)

Select a random no Q.

Compute E (M) = M' + P*Q, Where M' is the noise associated with the plaintext.

Decryption

Let E (M') = E (M) mod P, Where E (M') ∈ {-P/2, P/2}.

Compute M = E (M') mod 2, Where E (M') is noise.

4. COMPARISON OF HOMOMORPHIC CRYPTOSYSTEMS

We are comparing the existing homomoprhic systems with main key parameters homomorphic property, strength and weakness of the cryptosystem.

Table-1. Comparison of Homomorphic Crypto systems.

S. No.	Name of the Crypto system	Category of Homomorphic Crypto system	Homomorphic property	Strength of the system	Weakness of the system
1	Goldwasser Micali Scheme	Partially homomorphic crypto system	Additive	Probabilistic algorithm. It prevents an Intruder from recognizing intercepted message by comparing known cipher text. It is based on quadratic residuosity hard problem. The system is semantically secure	Size of cipher text is large. It follows bit by bit encryption
2	Benaloh crypto system	Partially homomorphic crypto system	Additive	It is based on higher residuosity hard problem. The system is semantically secure. Given Er(M),R and N, where the factorization is unknown, it is infeasible to determine plaintext.	Wrong choice of public key leads to ambiguous decryption of cipher text.
3	Paillier Scheme	Partially homomorphic crypto system	Additive	The cryptosystem is based on decisional composite residuosity assumption (DCRA). It is used in many application such as electronic voting, electronic cash etc. Self blinding property.	The semantic security cannot protect against adaptive chosen cipher text attack.
4	Damgard Jurik Scheme	Partially homomorphic crypto system	Additive	The security of this system based on decisional composite residuosity assumption	The plain text space is Zn^{s} and the cipher text space is Zn^{s+1}. Hence the ratio of bandwidthblock size is ½.
5	Okamoto and Uchiyama Scheme	Partially homomorphic crypto system	Additive	The security of this system based on quadratic residuosity problem.	Chosen cipher text attack is possible.
6	Unpadded RSA cryptosystem	Partially homomorphic crypto system	Multiplicative	Integer factorization problem.	Chosen cipher text attack is possible
7	Elgamal crypto system	Partially homomorphic crypto system	Multiplicative	Discrete log problem Secured against chosen cipher text.	Cipher text length is double the size of plain text. Encryption consume more time.
8	Boneh-Goh –Nissim Scheme	Somewhat homomorphic cryptosystem	Additive and onetime multiplicative	Security of the crypto system is based on sub group decision problem.	It is feasible to decrypt the value, once the factorization of n is known.
9	Gentry's Scheme	Fully Homomorphic Crypto system	Arbitray Addition and Multiplication	Security of the crypto system based on sparse subset sum problem (SSSP) & Bounded distance decoding (BDD) problem. Computation time depends on number of operations on encrypted data.	The key generation process is slow. The system is impractical for various applications because increasing security level lead to increase of cipher text size and computation time.

5. SECURITY ASPECTS

The security of any encryption scheme can be evaluated based on available computational resources. Shannon introduced the notion of unconditional security / perfect secrecy for any encryption scheme does not give information about the key or original text with the knowledge cipher text. The security of any public key crypto system based on hardness of mathematical problem [20]. These mathematical problems are well defined and are difficult to solve in general, but these problems can be solved easily one knows the algorithm and secret key. Hence the security of the crypto system depends on the intractability of mathematical structure. If the knowledge of the encrypted text does not give any information about the original text and key, then the homomorphic crypto systems are considered to be semantically secure. Consider in formal manner C = f(M), even though the adversary probability to guess cipher text and function, it is very difficult to know the plain text. The re-randomizable property of homomorphic system provides polynomial security. The system is protected against indistinguishable chosen plain text attacks.

6. CONCLUSIONS

Homomorphic system provides user can evaluate f (M) from an encrypted data M, but user should not be able to know any other information about message M. Partially homomorphic system used in many applications such as protection of mobile agents, multiparty computation, secret sharing, threshold scheme, electronic voting, Oblivious transfer, e-cashing and Watermarking and fingerprinting schemes but there is lot of improvements and analysis needed for fully homomorphic systems. Our main focus is to design a simple homomorphic crypto system with less complexity which is used to practical applications.

REFERENCES

Nitin Jain, Saibal K.Pal and Dhananjay K.Upadhyay. 2012. Implementation and analysis of Homomorphic Encryption Schemes. International Journal on Cryptography and Information Security. 2(2): 27-44.

Menezes A., Van Orschot P. and Vanstone S. 1997. Handbook of Applied Cryptography. CRC Press.

Van Tilborg H., Ed. 2005. Encyclopedia of Cryptography and Security, Springer, New York, NY, USA.

Rivest R., Adleman L. and Dertouzos M. 1978. On data banks and privacy homomorphisms. Foundations of Secure Computation, Academic Press. 169-177.

Goldwasser S and Micali S. 1984. Probabilistic encryption. In Journal of Computer and System Sciences. 28(2): 270-299.

Rivest R., Shamir A. and Adleman L. 2002. A method for obtaining digital signatures and public-key cryptosystems. In Communications of the ACM. 21(2): 120-126.

Goldwasser S. and Micali S. 1982. Probabilistic encryption and how to play mental poker keeping secret all partial information. In Proceedings of the 14th ACM Symposium on the Theory of Computing (STOC '82), New York, NY, USA. 365-377.

Benaloh J. 1988. Verifiable secret-ballot elections. Ph.D. thesis, Yale University, Department of Computer Science, New Haven, Conn, USA.

Laurent Fousse, Pascal, Lafourcade and Mohamed Alnuaimi. Benaloh's Dense Probabilistic Encryption Revisited. Progress in Cryptology - AFRICACRYPT (2011). 4th International Conference on Cryptology in Africa, Dakar, Senegal, July 5-7, Proceedings, Lecture notes in Computer science, Springer. 6737: 348-362.

Paillier P. 1999. Public-key cryptosystems based on composite degree residuosity classes. Inadvances in Cryptology (EUROCRYPT '99), Vol. 1592 of Lecture Notes in Computer Science, Springer, New York, NY, USA. 223-238.

Ivan Damgard, Mads Jurik and Jesper Buus Nielsen. 2010. A Generalization of Paillier's Public-Key System with Applications to Electronic Voting. International Journal of Information Security. 9(6): 371-385.

P.Y.A. Ryan. 2008. Prêt à Voter with Paillier encryption. Mathematical and Computer Modelling. 48(9-10): 1646-1662.

Damgard and M. Jurik. 2001. A generalization, a simplification and some applications of Pailliers probabilistic public-key system. In: 4th International Workshop on Practice and Theory in Public-Key Cryptography, Vol. 1992 of Lecture Notes in Computer Science, Springer, New York, NY, USA, 119-136.

Okamoto T and Uchiyama S. 1998. A new public-key cryptosystem as secure as factoring. In Advances in Cryptology (EUROCRYPT '98), Vol. 1403 of Lecture Notes in Computer Science, Springer, New York, NY, USA. 308-318.

Rivest R, Shamir A and Adleman L. 2002. A method for obtaining digital signatures and public-key cryptosystems. In Communications of the ACM. 21(2): 120-126.

The Basis of ElGamal Encryption Algorithm. URL: http://www.cprogramdev.com/75562.

Boneh D., Goh E. and Nissim K. 2005. Evaluating 2-DNF Formulas on Ciphertexts. In Proceedings of Theory of Cryptography (TCC) '05, LNCS 3378, 325-341.

Salil P. Vadhan. 2007. Theory of Cryptography. 4th Theory of Cryptography Conference, TCC. pp. 562-563.

Zhenfei Zhang, Thomas Plantard, Willy Susilo. 2012. On the CCA-1 Security of Somewhat Homomorphic Encryption over the Integers. Information Security Practice and Experience 8th International Conference, ISPEC 2012, Hangzhou, China, April 9-12, 2012. Proceedings, Lecture notes in Computer Science. Vol. 7232.

Jaydip Sen. 2013. Theory and Practice of Cryptography and Network Security Protocols and Technologies. INTECH Publishers, Croatia. 133-164.

Brickell E and Yacobi Y. 1987. On privacy homomorphisms. Advances in Cryptology (EUROCRYPT ’87), volume 304 of Lecture Notes in Computer Science, Springer, New York, USA. pp. 117-126.

Rappe D. 2004. Homomorphic Cryptosystems and their Applications, Ph.D. thesis, University of Dortmund, Dortmund, Germany.