International Journal of Technology and Engineering System (IJTES)
Vol 8. No.1 – Jan-March 2016 Pp.12-16

available at : www.ijcns.com
ISSN: 0976-1345

A TECHNICAL OVERVIEW OF VARIOUS HOMOMORPHIC ENCRYPTION TECHNIQUES FOR A SECURE CLOUD DATA STORAGE SYSTEM

S.Kalaivany
Research Scholar
Department of Computer Science
Vels University, Pallavaram,Chennai
kalaivany23@gmail.com

Dr.T.Nalini,
Professor
Department of Computer Science & Engineering
Bharath University ,Chennai 600 073
drnalinichidambaram@gmail.com

ABSTRACT

Data confidentiality is a major security threat in cloud storage system. To perform computation securely Homomorphic encryption methodology ensures the confidentiality of data by several partially, somewhat and fully homomorphic encryption techniques. This paper discusses the technical implementation of various homomorphic encryptions which enables the researchers to build a secure cloud storage system.

Keywords: *Cloud storage system, Fully Homomorphic Encryption, partially Homomorphic Encryption.*

1. INTRODUCTION

Homomorphic encryption is a form of encryption which allows computations on ciphertext.In modern communication system architectures Homomorphic encryption allows chaining of different services without. exposing the data. For example, a chain of different services from different companies could calculate 1) the tax 2) the currency exchange rate 3) shipping, on a transaction without exposing the unencrypted data to each of those services Thus Homomorphic encryptions are used in cloud computing environment for ensuring the confidentiality of data. In addition the homomorphic property of various cryptosystems can be used to create many other secure systems, for example secure voting systems, collision- resistant hash function, private information retrieval schemes etc

2. TECHNICAL OVERVIEW OF HOMOMORPHIC ENCRYPTION TECHNIQUES

There are several partially homomorphic, somewhat homomorphic and fully homomorphic encryption techniques available to perform computation securely in a cloud environment as stated bellow

2.1 Partially Homomorphic Cryptosystems.

In the following examples, the notation $\mathcal{E}(x)$ is used to denote the encryption of the message *x*.

2.1.1 UNPADDED RSA

If the RSA public key is modulus m and exponent e, then the encryption of a message x is given by $\mathcal{E}(x) = x^e \bmod m$. The homomorphic property is then

$$\mathcal{E}(x_1) \cdot \mathcal{E}(x_2) = x_1^e x_2^e \bmod m = (x_1 x_2)^e \bmod m = \mathcal{E}(x_1 \cdot x_2 \bmod m)$$

2.1.2 ELGAMAL

In the ElGamal cryptosystem, in a cyclic group G of order q with generator g, if the public key is (G, q, g, h), where $h = g^x$, and x is the secret key, then the encryption of a message m is $\mathcal{E}(m) = (g^r, m \cdot h^r)$, for some random $r \in \{0, \ldots, q-1\}$.The homomorphic property is then

$$\mathcal{E}(m_1) \cdot \mathcal{E}(m_2) = (g^{r1}, m_1 \cdot h^{r1})(g^{r2}, m_2 \cdot h^{r2})$$

$$= (g^{r1+r2}, (m_1 \cdot m_2)h^{r1+r2}) = \mathcal{E}(m_1 \cdot m_2).$$

2.1.3 GOLDWASSER–MICALI

In the Goldwasser–Micali cryptosystem, if the public key is the modulus *m* and quadratic non-residue *x*, then the encryption of a bit *b* is $\mathcal{E}(b) = x^b r^2 \bmod m$,forsome random $r \in \{0, \ldots, m-1\}$.The homomorphic property is then

$$\mathcal{E}(b_1) \cdot \mathcal{E}(b_2) = x^{b1} r_1^2 x^{b2} r_2^2 \bmod m = x^{b1+b2}(r$$

where $\oplus$ denotes addition modulo 2, (i.e. exclusive-or).

2.1.4 BENALOH

In the Benaloh cryptosystem, if the public key is the modulus *m* and the base *g* with a blocksize of *c*, then the encryption of a message *x* is $\mathcal{E}(x) = g^x r^c \bmod m$, for some random $r \in \{0, \ldots, m-1\}$. The homomorphic property is then

$$\mathcal{E}(x_1)\cdot\mathcal{E}(x_2) \bmod m = (g^{x1} r_1^c)(g^{x2} r_2^c) \bmod m = g^{x1+x2}(r_1 r_2)^c = \mathcal{E}(x_1 + x_2 \bmod m)$$

2.1.5 PAILLIER

In the Paillier cryptosystem, if the public key is the modulus *m* and the base *g*, then the encryption of a message *x* is $\mathcal{E}(x) = g^x r^m \bmod m^2$, for some random $r \in \{0, \ldots, m-1\}$. The homomorphic property is then

$$\mathcal{E}(x_1)\cdot\mathcal{E}(x_2) = (g^{x1} r_1^m)(g^{x2} r_2^m) \bmod m^2 = g^{x1+x2}(r_1 r_2)^m \bmod m^2 = \mathcal{E}(x_1 + x_2 \bmod m^2$$

2.2 Fully And Somewhat Homomorphic Cryptosystems

There are two types of homomorphic encryption: fully homomorphic encryption (FHE) and somewhat homomorphic encryption (SHE). Each type differs in the number of operations that can be performed on encrypted data. FHE allows for an unlimited, arbitrary number of computations (both addition and multiplication) to be

performed on encrypted data. SHE cryptosystems support a limited number of operations (i.e., any amount of addition, but only one multiplication) and are faster and more compact than FHE cryptosystems.

2.2.1 Bootstrapping And Lattices

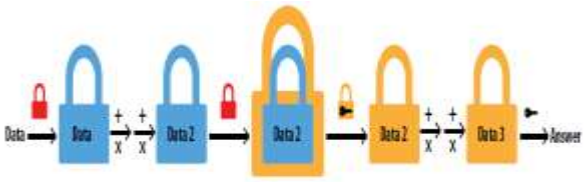
One of the hindrances limiting the feasibility of FHE is "noise." Noise refers to the distortion of ciphertexts (i.e., encoded text) that occurs after each operation (e.g., addition or multiplication) is performed. As more and more additions and multiplications are performed, the noise level becomes too high, and the resulting ciphertexts become indecipherable. Ciphertexts can be refreshed easily by decrypting them, but the idea behind homomorphic encryption is to not share the secret key required to do the decryption.

A process called bootstrapping is used to overcome this noise problem in SHE solutions. Bootstrapping modifies an SHE solution so it can homomorphically run its own decryption procedure by adding an encryption of the secret key to the public key is accomplished by using a sparse subset-sum problem (SSSP) or augmenting the public key with a large set of vectors so that a sparse subset of the vectors will add up to be the secret key.

The idea of bootstrapping calls for double encrypting the data and, as processes runs, removing a layer of encryption. Gentry's bootstrapping procedure adds another layer of encryption after a few computations using an encrypted key to unlock the inner layer of scrambling. This process "refreshes" the still-encrypted data and could allow for an infinite number of computations, effectively turning an SHE solution into an FHE solution.

2.3 SYSTEM ARCHITECTURE

Bootstrapping method modifies an SHE solution to homomorphically run its own decryption procedure by adding an encryption of the secret key to the public key



2.4 RECENT TRENDS

Advanced Research Projects Agency (DARPA) and the Intelligence Advanced Research Projects Activity (IARPA), issued Broad Agency Announcements (BAAs) for a solution that could perform computations on encrypted data (i.e., homomorphic encryption).In April 2011, DARPA awarded approximately $5 million to Galois, Inc. to be the research integrator for the Programming Computation on Encrypted Data (PROCEED) program. In December 2010, IARPA issued a request for proposals for a program called Security And Privacy Assurance Research (SPAR). The goal of the both programs is to make it feasible to execute programs on encrypted data without having to decrypt the data first. DARPA's stated goal was to reduce the computing time for an FHE solution by a factor of 10 million

2.5 CONCLUSION

Researchers worldwide are actively engaged in trying to perfect a practical FHE solution. Recent breakthroughs include a homomorphic encryption scheme from Fujitsu using batch encryption vice the bit- level encryption usually seen in FHE solutions. Researchers from the Massachusetts Institute of Technology, the University of Toronto, and

Microso_ Research created a three-part encryption scheme that uses homomorphic encryption as well as two other cryptographic techniques to obtain a fully functioning FHE solution.

REFERENCES

[1] Craig Stuntz (2010-03-18). "What is Homomorphic Encryption, and Why Should I Care?"

[2] Ron Rivest (2002-10-29). "Lecture Notes 15: Voting, Homomorphic Encryption".

[3] Daniele Micciancio (2010-03-01). "A First Glimpse of Cryptography's Holy Grail". Association for Computing Machinery. p. 96. Retrieved 2010-03-17.

[4] R. L. Rivest, L. Adleman, and M. L. Dertouzos. on data banks and privacy homomorphisms. In Foundations of Secure Computation, 1978

[5] D. Boneh, E. Goh, and K. Nissim. Evaluating 2-DNF Formulas on Ciphertexts. In Theory of Cryptography Conference, 2005.

[6] Y. Ishai and A. Paskin. Evaluating branching programs on encrypted data. In Theory of Cryptography Conference, 2007

[7] Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In the 41st ACM Symposium on Theory of Computing (STOC), 2009.

[8] Craig Gentry. "A Fully Homomorphic Encryption Scheme (Ph.D. thesis)" (PDF).

[9] Smart, Nigel P.; Vercauteren, Frederik. "Fully homomorphic encryption with relatively small key and ciphertext sizes". PKC 2010 (Springer).

[10] Smart, Nigel P.; Vercauteren, Frederik (2014). "Fully Homomorphic SIMD Operations". Designs, Codes and Cryptography (Springer) 71 (1): 57–81.

[11]Gentry, Craig; Halevi, Shai. "Implementing Gentry's fully-homomorphic encryption scheme". EUROCRYPT 2011 (Springer).

[12] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. Fully Homomorphic Encryption without Bootstrapping. In ITCS 2012

[13] C. Gentry, S. Halevi, and N. P. Smart. Better Bootstrapping in Fully Homomorphic Encryption. In PKC 2012 (SpringeR)

[14] Shai Halevi; Victor Shoup. "HElib: An Implementation of homomorphic encryption". Retrieved 31 December 2014.

[15] Ducas, Léo; Micciancio, Daniele. "FHE Bootstrapping in less than a second". Cryptology ePrint archive. Retrieved 2 January 2015.

[16]J. Gentry C, Halevi S. "Implementing Gentry's fullyhomomorphic encryption scheme." Cryptology ePrint Archive. 2011. Available at: http://eprint.iacr.org/2010/520

[17] Fujitsu Laboratories Ltd. "Fujitsu develops world's first homomorphic encryption technology that enables statistical
calculations and biometric authentication" [press release].Aug 2013. Available at: http://www.fujitsu.com/global/news/pr/archives/month/2013/20130828-01.html.

[18] Kalaivany.S and Dr.T.Nalini," An Investigation on the Issues in Cloud Data Storage System with Secure Data Forwarding", International Journal of Computing, Communication and Information Security, Volume 6, Issue: 3, ISSN: 0976-1349, pp. 106-117, July-Sep 2014.

[19] Kalaivany.S and Dr.T.Nalini,"A new re-encryption scheme with improvised delegation mechanism and homomorphic encryption", International Journal of Applied Engineering

Research ISSN 0973-4562 Volume 10, Number 14
(2015) pp 34485-34489.