Fully Homomorphic Encryption Scheme with Probabilistic Encryption Based on Euler's Theorem and Application in Cloud Computing

Vinod Kumar, Rajendra Kumar, Santosh Kumar Pandey and Mansaf Alam

Abstract Homomorphic encryption is an encryption scheme that allows different operations on encrypted data and produces the same result as well that the operations performed on the plaintext. Homomorphic encryption can be used to enhance the security measure of un-trusted systems which manipulates and stores sensitive data. Therefore, homomorphic encryption can be used in cloud computing environment for ensuring the confidentiality of processed data. In this paper, we propose a fully Homomorphic Encryption Scheme with probabilistic encryption for better security in cloud computing.

Keywords Homomorphism · Cloud computing · Fully homomorphic encryption · Security

1 Introduction

Cloud computing enables sharing of services and focuses on maximizing the effectiveness of the shared resources. In the Cloud computing the user data place their data in the cloud, and any computation on the stored data will be performed on the cloud. The Cloud computing has privacy issues because the service provider can access, alter or even delete the data intentionally. Some of the cloud service providers share the information with third parties to provide the effective services. The

V. Kumar
Department of I.T, Centre for Development of Advanced Computing Noida, Noida, India

R. Kumar · M. Alam (✉)
Department of Computer Science, Jamia Millia Islamia, New Delhi, India
e-mail: malam2@jmi.ac.in

S.K. Pandey
Department of Electronics and Information Technology, Ministry of Communication and Information Technology, New Delhi, India

V.B. Aggarwal et al. (eds.), *Big Data Analytics*, Advances in Intelligent Systems and Computing 654, https://doi.org/10.1007/978-981-10-6620-7_58

third party can also access the user private data and modifies the information to make it beneficial to himself. Therefore, security is major thing over the cloud. To protect the private information from cloud service provider or third party—encryption is needed. But it is not enough to protect the computation done on the cloud because to perform computation, decryption of stored data is needed on the cloud.

To protect such computation on the cloud, we need an encryption scheme that enables us to perform the computation of encrypted data. The Fully Homomorphic encryption is the technique that can be used to perform computation on encrypted data [1]. Homomorphic encryption is the encryption scheme that allows to perform some computations on message without decrypting the message [2]. Therefore, using Fully Homomorphic scheme we can perform any computations on the cloud stored data without any obstruction by cloud provider [3].

Here, we propose an Euler's Theorem-Based Fully Homomorphic Encryption Scheme with probabilistic Encryption to solve the issues of third-party control and data security of Cloud computing.

The Remaining part of the paper is organized as follows. Section 2 describes the related work. Section 3 provides the details of proposed scheme and proof of correctness of scheme. Section 4 presents a working example. Finally, Sect. 5 describes concluding remarks of contributions.

2 Related Work

In 1978, the concept of Homomorphic encryption introduced by Ronald Rivest, Leonard Adleman, and Michael Dertouzos. In 1982, Shafi Goldwasser and Silvio Micali invented an additive Homomorphic encryption that can encrypt only single bit. In 1999 Pa Paillier also given an additive Homomorphic encryption. In 2005, a security system that can compute only one multiplication and an unlimited number of additions proposed by Dan Boneh, et al. In 2009, the first fully Homomorphic encryption system that computes an arbitrary number of additions and multiplications proposed by Gentry and Halevi [4], Gentry [5]. Gentry [3] also proposed ideal lattices hardness based a fully homomorphic encryption in 2009. In 2010, A Fully homomorphic encryption scheme based on integers given by Van Dijk et al. [6]. In 2012, Xiang Guangli, Cui Zhuxiao proposed Fermat's Little Theorem Based, Algebra Homomorphic Encryption Scheme that works for rational number [7].

3 Fully Homomorphic Encryption with Probabilistic Encryption

Our proposed scheme is fully homomorphic scheme with probabilistic Encryption, which supports both additive and multiplicative homomorphism property. It is also based on Euler's theorem that can be thought of as a generalization of Fermat's little theorem. The Fermat theorem uses prime modulus, and the modulus in Euler's theorem is an integer. Two versions of Euler theorem are as follows:

1. If a and n are co-prime, then $a^{\varnothing(n)} \equiv 1 (\mathrm{mod}\, n)$.
2. It removes the condition that a and n should be co-prime. If $n = p \times q, a < n$, and k an integer, then $a^{k \times \varnothing(n)+1} \equiv a (\mathrm{mod}\, n)$.

The Euler's theorem sometimes is helpful for quickly finding a solution to some exponentiations. The proposed Homomorphic encryption scheme consists three phases which are as follows:

- Key generation
- Message Encryption
- Message Decryption

Phase-I: Key Generation

1. Select two prime numbers p and q
2. Calculate $n = p \times q$ and $\varnothing(n)$
3. Select another prime number z such that $\gcd(n, z) = 1$
4. Calculate $x = n \times z$

Phase-II: Messages Encryption

1. Messages addition $(M_1 + M_2)$ and multiplication $(M_1 * M_2)$ should be less than $< n.$, therefore, M_1 & M_2 will always be less than n
2. Select two random integer k_1 and k_2 for probabilistic encryption
3. $C_1 = M^{k_1 \times \varnothing(n)+1} \bmod x$ and $C_2 = M^{k_2 \times \varnothing(n)+1} \bmod x$
   Here, C_1 and C_2 are cipher texts
4. Evaluate result C_3 after performing operations on cipher texts C_1 and C_2

Phase-III: Message Decryption

1. $M = C_3 \bmod n$, Where C_3 is cipher text after performing operations on C_1 and C_2, n is private key and M is plain text

Proof of Correctness of scheme

$$\begin{aligned} C &= M^{k\times\varnothing(n)+1} \bmod x \\ D &= C \bmod n \\ &= \left(M^{k\times\varnothing(n)+1} \bmod x\right) \bmod n \\ &= \left(M^{k\times\varnothing(n)+1} \bmod n\right) \bmod x \end{aligned}$$

Now by second version of Euler's theorem, we know that $\left(a^{k\times\varnothing(n)+1}\right) \equiv a(\bmod n)$

$= (M) \bmod x = M, M < x$ *(Hence proved)*

Homomorphism

For message M_1 and M_2, we have the corresponding cipher texts as C_1 and C_2, and random integer's k_1 and k_2 used for deciphering, respectively. The multiplicative and additive Homomorphic property and their proof are presented below.

Multiplicative homomorphism

Multiplicative homomorphism property is stated as:

$$M_1 \times M_2 = \mathrm{DEC}[\mathrm{ENC}(M_1) \times \mathrm{ENC}(M_2)]$$

DEC represents Decryption function, and ENC represents Encryption function.

Proof

$$\begin{aligned} C_1 &= \left(M_1^{k_1\times\varnothing(n)+1} \bmod x\right), \\ C_2 &= \left(M_2^{k_2\times\varnothing(n)+1} \bmod x\right) \\ C_1 \times C_2 &= \left(M_1^{k_1\times\varnothing(n)+1} \bmod x\right) \times \left(M_2^{k_2\times\varnothing(n)+1} \bmod x\right) \\ D(C_1 \times C_2) &= (C_1 \times C_2) \bmod n \\ &= \left[\left(M_1^{k_1\times\varnothing(n)+1} \bmod x\right) \times \left(M_2^{k_2\times\varnothing(n)+1} \bmod x\right)\right] \bmod n \\ &= \left[\left(M_1^{k_1\times\varnothing(n)+1} \bmod x\right) \bmod n \times \left(M_2^{k_2\times\varnothing(n)+1} \bmod x\right) \bmod n\right] \\ &= \left[\left(M_1^{k_1\times\varnothing(n)+1} \bmod n\right) \bmod x \times \left(M_2^{k_2\times\varnothing(n)+1} \bmod n\right) \bmod x\right] \end{aligned}$$

Now, we know that $\left(a^{k\times\varnothing(n)+1}\right) \equiv a(\bmod n)$ so

$$= [(M_1 \bmod x) \times (M_2 \bmod x)] = M_1 \times M_2$$

Additive Homomorphism:

Additive homomorphism property is stated as:

$$M_1 + M_2 = \mathrm{DEC}[\mathrm{ENC}(M_1) + \mathrm{ENC}(M_2)]$$

Proof

$$\begin{aligned}
C_1 &= \left(M_1^{k_1 \times \varnothing(n)+1} \bmod x\right), \\
C_2 &= \left(M_2^{k_2 \times \varnothing(n)+1} \bmod x\right) \\
C_1 + C_2 &= \left(M_1^{k_1 \times \varnothing(n)+1} \bmod x\right) + \left(M_2^{k_2 \times \varnothing(n)+1} \bmod x\right) \\
D(C_1 + C_2) &= (C_1 + C_2) \bmod n \\
&= \left[\left(M_1^{k_1 \times \varnothing(n)+1} \bmod x\right) + \left(M_2^{k_2 \times \varnothing(n)+1} \bmod x\right)\right] \bmod n \\
&= \left[\left(M_1^{k_1 \times \varnothing(n)+1} \bmod x\right) \bmod n + \left(M_2^{k_2 \times \varnothing(n)+1} \bmod x\right) \bmod n\right] \\
&= \left[\left(M_1^{k_1 \times \varnothing(n)+1} \bmod n\right) \bmod x + \left(M_2^{k_2 \times \varnothing(n)+1} \bmod n\right) \bmod x\right]
\end{aligned}$$

Now we know that $\left(a^{k \times \varnothing(n)+1}\right) \equiv a(\bmod n)$ so

$$= [(M_1) \bmod x + (M_2) \bmod x] = M_1 + M_2$$

4 Working Example

Example Let we take two prime number p = 5 and q = 7, then

$$n = p \times q \rightarrow n = 5 \times 7 \rightarrow n = 35$$

Now calculate $\varnothing$(n) according to the Euler Totient function, $\varnothing(35) = 24$,
Now select a prime number z such that gcd(n, z) = 1
Let z = 31, and calculate gcd(35, 31) = 1,
Now, calculate $x = n \times z \rightarrow x = 35 \times 31 \rightarrow x = 1085$
Now take two random integer k_1 = 3 and k_2 = 2, and two messages $m_1 = 2$ and $m_2 = 4$, such that $(m_1 + m_2)$ and $(m_1 * m_2)$ less than n
Now $c_1 = {m_1}^{k_1 \times \varnothing(n)+1} \bmod x$

$$c_1 = 2^{3 \times \varnothing(35)+1} \bmod 1085 \rightarrow c_1 = 2^{3 \times 24+1} \bmod 1085 \rightarrow c_1 = 597$$

And $c_2 = m_2{}^{k_2 \times \varnothing(n)+1} \bmod x$

$$c_2 = 4^{2\times\varnothing(35)+1} \bmod 1085 \rightarrow c_2 = 4^{2\times 24+1} \bmod 1085 \rightarrow c_2 = 39$$

Additive Homomorphism:

Let the addition of two encrypted messages is c_3 then

$$c_3 = c_1 + c_2 \rightarrow c_3 = 597 + 39 \rightarrow c_3 = 636$$

Now decryption of this message is m_3 then

$m_3 = c_3 \bmod n \rightarrow m_3 = 636 \bmod 35 \rightarrow m_3 = 6$, this is equal to $m_1 + m_2$ (i.e., 2 + 4 = 6)

Multiplicative homomorphism:

Let the multiplication of two encrypted messages is c_4 then

$$c_4 = c_1 \times c_2 \rightarrow c_4 = 597 \times 39 \rightarrow c_4 = 23,283$$

Now let the decryption of this message is m_4 then

$m_4 = c_4 \bmod n \rightarrow m_4 = 23{,}283 \bmod 35 \rightarrow m_4 = 8$, this is equal to $m_1 \times m_2$ (i.e. $2 \times 4 = 8$).

5 Conclusion

In this paper, a Fully Homomorphic encryption scheme was applied to Cloud computing with different computations on cipher text without decryption. The Homomorphic encryption schemes are used in secure electronic voting, searching over encrypted data, securing biometric information etc. The operations on small numbers are supported by Fully Homomorphic encryption scheme till now. In future, we can develop a fully Homomorphic encryption scheme that support a large number of circuits.

References

1. Chen, L., Gao, C.M.: Public key homomorphism based on modified ElGamal in real domain. In: 2008 International Conference on Computer Science and Software Engineering. IEEE Computer Society, Wuhan, Hubei, China, pp. 802–805 (2008)

2. Smart, N.P., Vercauteren, F.: Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Public Key Cryptography—PKC'10, vol. 6056 of Lecture Notes in Computer Science, pp. 420–443. Springer, 2010
3. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Symposium on the Theory of Computing (STOC), pp. 169–178 (2009)
4. Gentry, C., Halevi, S.: Implementing gentry's fully-homomorphic encryption scheme. Adv. Cryptol EUROCRYPT 2011, pp. 129–148 (2011)
5. Gentry, C.: A fully homomorphic encryption scheme. PhD thesis, submitted to the department of computer science and the committee on graduate Stanford University, September (2009)
6. Van Dijk, M., Gentry, C., et al.: Fully homomorphic encryption over the integers. In: Advances in Cryptology EUROCRYPT 2010
7. Xiang, G., Cui, Z.: The algebra homomorphic encryption scheme based on Fermat's little theorem. In: International Conference on Communication Systems and Network Technologies (CSNT), pp. 978–981, 11–13 May 2012 (2012)
8. Goldwasser, S., Micali, S.: 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), pp. 365–377, New York, NY, USA (1982)
9. Okamoto, T., Uchiyama, S.: A new public-key cryptosystem as secure as factoring. In: Advances in Cryptology (EUROCRYPT '98), vol. 1403 of Lecture Notes in Computer Science, pp. 308–318. Springer, New York (1998)
10. Van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V.: Fully homomorphic encryption over the integers. In: Advances in Cryptology EUROCRYPT 2010, p. 24-4 (2010)
11. Yu, Y., Leiwo, J., Premkumar, B.: A study on the security of privacy homomorphism‖, Nanyang Technological University, School of Computer Engineering. In: Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06), IEEE (2006)