

Two-Layer Encryption based on Paillier and ElGamal Cryptosystem for Privacy Violation

Anjan K Koundinya

Department of CSE, BMS Institute of Technology and Management, Bangalore.
Email: anjank-cse@bmsit.in

Gautham SK

Department of CSE, BMS Institute of Technology and Management Bangalore
Email: 1by19scs02@bmsit.in

Received: 21 April 2021; Revised: 13 May 2021; Accepted: 20 May 2021; Published: 08 June 2021

Abstract: Our life nowadays relies much on technologies and online services net banking, e-voting and so on. So, there is a necessity to secure the data that is transmitted through the internet. However, while performing decryption, it sometimes led to privacy violation so there is need to operate on users encrypted data without knowing the original plaintext.

This paper represents the implementation of two-layer cryptosystem using paillier and elgamal algorithm both following asymmetric encryption. It is mainly focusing the challenges of privacy protection and secure utilization of information, where homomorph encryption is gaining attention. Additive homomorphism is used in paillier cryptosystem which is used in fields like secure biometrics and electronic voting. Elgamal ensures that paillier encrypted data is secured that ensures two-layer encryption.

Index Terms: Pailliers cryptosystem, additive homomorphic encryption, elgamal cryptosystem, two-layer encryption, privacy violation, data security.

1. Introduction

Cryptography is scientific technique that is used in information security. Cryptography is derived from a Greek word know as kryptos, which means hidden things [1]. It involves varies techniques that hide any kind of information in a storage unit or to transmit the information. The cryptography is related to process where a normal readable text called the plain text is scrambled to an unreadable text called cipher text, this process is called encryption and the process of reversing it is called decryption and the people who work on these techniques are called cryptographers [2]. The objective of cryptography is to provide [3-5]:

- 1) Confidentiality
- 2) Authentication
- 3) Integrity
- 4) Non-Repudation

Symmetric cryptosystem like DES [6], use the same secret key for both encryption and decryption of plain text, which means that the sender and receiver should have the same secret key. This leads to two challenges; one is to how to securely transmit the secret key and second is how to manage a large number of secret keys. If we consider a scenario where 60 people are communicating with each other and each person must have secret key and along with that 59 secret keys of others.

But in the case of asymmetric cryptosystem like Elgamal cryptosystem [7], different keys are used for encryption and decryption. The encrypting key i.e., the public key of both sender and receiver is sent publicly and the user send message with receiver's public key. The receiver decrypts the ciphertext using the private key of the corresponding receiver. asymmetric cryptosystem solves the problems of symmetric cryptosystem.

There is need to secure the data's that are shared while using online service which can be ensured by encryption and while decrypting it should not lead to privacy violation. This can be avoided if the operation is performed in the users encrypted data without knowing the original plaintext.

The problem of privacy violation can be resolved using homomorphic encryption (HE), which supports mathematical operations on the ciphertext and while decrypting the result is similar to the computation that is performed in the plaintext.

The recent analysis as lead to suggestion that the paillier cryptosystem which is based on HE, leaks privacy information and subject leads to compromise. This brought up concern about the cryptosystem. This concern led to the use of tools that would resolve the problem. But instead of using these tools its better to thicken the encrypted data that was generated by paillier cryptosystem, which in turn will enhance the security. This concept led to two-layer encryption using two different HE techniques with also ensures the homomorphic properties.

A. Contributions

To resolve the problem of privacy violation, paillier cryptography is implemented and to ensure the two-layer encryption elgamal cryptosystem is enabled. Both the cryptosystem is implemented using python. We will also be analyzing the homomorphic property of paillier's cryptosystem and also analysis the runtime and key generation time of both the algorithms

B. Organization

The following paper is as follows. Section II summarizes the related work. Section III describes the proposed system. Section IV describes the result and analysis. Finally, Section V concludes the paper.

2. Related Work

Pascal Paillier's [8] homomorphic encryption system follows certain properties:

1. It is based on public key cryptosystem i.e.; encryption can be done by any sender who knows the receivers public key but the decryption can only be done by its corresponding private key which is kept secret.
2. Probabilistic property, which means that the attacker can never find out whether the two-cipher text belongs to the same plaintext.
3. It contains additive homomorphic properties [9].

The random value selected for encryption in pailliers cryptosystem is for semantic security [10]. It ensures that the data from the ciphertext cannot help the attacker to differentiate the two messages M_1 and M_2 and guess which one was encrypted. Semantic security is very useful in application like e-voting. Paillier cryptosystem is popular with e-voting system and huge number of voters also prefers paillier cryptosystem [11]. Boneh-Goh-Nissim [12] is a support homomorphic algorithm that is much faster and compact compared to other fully homomorphic encryption technique. The ElGamal cryptosystem [13], was developed in 1985, it is based on discrete logarithm problem for finite field.

3. Proposed Cryptosystem

The proposed system is a combination of two cryptosystem namely, Paillier and ElGamal. Both the algorithm is implemented using python. Both are based on public key scheme. The idea to implement a two-layer encryption system. The cryptosystem will first encrypt the message using paillier algorithm and the encrypted message is again encrypted using elgamal algorithm which produce a most secure data. And in the receiver's side, the encrypted data is decrypted by elgamal algorithm using receivers private key which gives paillier's cypher text, the receiver will operate on the cipher text to ensure privacy which is due to the homomorphic property of paillier.

The main functions used are as follows:

- $gcd(a, b)$: computes the greatest common divisor of the two-number a and b .
- $lcm(a, b)$: computes the least common multiple which helps to generate the random number g .
- $gen_key()$: Generate large random number.
- $power(a,b,c)$: computes modular exponentiation.
- $encrypt()$: encrypts the plain text to cipher text.
- $decrypt()$: decrypts the cypher text to plain text.

The algorithm of the two cryptosystem is described below:

A. Pailliers Homomorphic cryptosystem

The additive homomorphic encryption system which consists of three algorithms: Key generation, encryption and decryption. Described as follows:

1) Key Generation

1. Choose two prime numbers p and q , where p and q should be of same length and should be different.
2. Calculate n , $n = p \cdot q$ and $\lambda = \text{lcm}(p-1, q-1)$.
3. Select a random integer g , where g belongs to Z_n^{*2}
4. check whether n divides the order of g , this can be ensured by $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$, where $L(u) = u-1/n$.
5. Assign public key as (n, g) .
6. Assign private key as (λ, μ) .

2) Encryption

1. m is the message that needs to encrypted, where m belongs to Z_n .
2. Select a random value r , where r belongs Z_n^* .
3. Calculate the ciphertext as

$$c = g^m \cdot r^n \bmod n^2 \tag{1}$$

3) Decryption

1. c is the ciphertext that needs to decrypted, where c belongs to Z_n^{*2} .
2. Compute the message: $m = L(c^\lambda \bmod n^2) \cdot \mu \bmod n$.

B. ElGamal Cryptosystem

The algorithm describes as follows:

1. Consider P as a large prime number.
2. Consider g as a primitive element, where g belongs to Z_p .
3. Consider x_i as a secret key of the user i (u_i).
4. Consider r as a random number.
5. Assign $p_i = g^{x_i} \bmod P$, as the public key of u_i , where P , g and p_i are public information. And x_i and r are private information.
6. When u_i wants a sent a message m to another user u_j , u_i generates a random number r and encrypt the message m as follows:

$$b = g^r \bmod P, \\ c = m \cdot p_i^r \bmod P.$$

7. u_i sends (b, c) to u_j . Using this u_j decrypt c as follows:

$$m = c \cdot (b^{x_j})^{-1} \bmod P$$

4. Results and Analysis

In order to prove the effectiveness of paillier cryptosystem and its homomorphic properties fer tests are performed which are cipher uniqueness test, deciphering test, deciphering test with different plaintext, homomorphic test, runtime and key generation time of both the cryptosystem. For testing a 16-bit length value of p and q (prime numbers) will be taken, where $p = 56711$ and $q = 77477$.

1) Cipher Uniqueness Test

Table 1. Result of cipher uniqueness test

Sl.no	Plaintext	Random Number	Ciphertext
1	9	57342	6482410849035749
2	9	64389	8475285035861743
3	9	52906	6395629462029423
4	25	27843	9864520108324623
5	25	74437	8462958298322048

Based on the above table 1, the uniqueness of the ciphertext depends on the random value. The random value generates different ciphertext even though the plain text is similar.

1.a) Deciphering Test

The testing is done by the same values of p and q, when these prime numbers are multiplied, we obtain n = 4393798147.

Table 2. Result of Deciphering Test.

Sl.no	Ciphertext	Decrypted Text	Result
1	6482410849035749	9	True
2	8475285035861743	9	True
3	6395629462029423	9	True
4	9864520108324623	25	True
5	8462958298322048	25	True

The above table 2 proves that the encryption process is performed successfully.

2) Deciphering Test with Different Plaintext

Table 3. Result of deciphering test with different plaintext

Sl.no	Plaintext	Ciphertext	Decrypted text	Result
1	25000	3743986204862975	25000	True
2	3293588147	8503756297662847	3293588147	True
3	4393798147	8230342920952394	0	False
4	3908524362 325	2387588275712003	24	False

From the above table 3, we prove that the decryption result will be true if the plaintext value m is less than n, and if m is larger than n or m >= n the decryption result will be false.

3) Homomorphic Test

In this we will be testing the homomorphic property, the homomorphic function used is:

$$D (E (m_1, r_1). E (m_2, r_2) \text{ mod } n^2) = m_1 + m_2 \text{ mod } n$$

Table 4. Result of homomorphic test

Sl.no	M ₁ + M ₂	Cipher Text m ₁ m ₂ mod n ²	Decryption Result	Result
1	25 + 50	3658403675921648	75	True
2	35687226 + 6598325	5748923549871943	42285551	True
3	4393798144 + 1023	7593648234671976	708	False

The above table 4 proves that the homomorphic property is followed for messages lesser than the value of n but produce false result if the message value is greater than the value of n.

4) Runtime and Key generation time

Table 5. Runtime of Paillier and ElGamal

Sl.no	Runtime ElGamal	Runtime of Paillier	Input Length
1	0.003497	0.000673	20
2	0.003899	0.000989	40
3	0.004571	0.001034	60
4	0.004781	0.001389	80
5	0.005014	0.001857	100

Table 6. Key generation of Paillier and ElGamal

Sl.no	Total time key generation in ElGamal	Total time key generation in Paillier	Input Length
1	0.000998	0.000993	20
2	0.001995	0.001049	40
3	0.003579	0.001554	60
4	0.002002	0.002770	80
5	0.002396	0.002789	100

The above table 5 and table 6 shows the runtime and key generation of pailliers and elgamal cryptosystem. The length prime numbers p and q is 50.

Table 7. Runtime of Paillier and ElGamal

Sl.no	Total time key generation in ElGamal	Total time key generation in Paillier	Input Length
1	0.001408	0.000373	20
2	0.001875	0.000549	40
3	0.002678	0.000854	60
4	0.002998	0.000985	80
5	0.003469	0.001284	100

Table 8. Key generation of Paillier and ElGamal

Sl.no	Runtime of ElGamal	Runtime of Paillier	Input Length
1	0.003497	0.000673	20
2	0.003899	0.000989	40
3	0.004571	0.001034	60
4	0.004781	0.001389	80
5	0.005014	0.001857	100

The above table 7 and table 8 shows the runtime and key generation of pailliers and elgamal cryptosystem. The chosen the prime numbers p and q length is 90.

When we compare the runtime and key generation of both the algorithm, we can notice that the when the length of the prime number increases the runtime and key generation time decreases, which means that encryption and decryption time decreases with the increase in the length of prime number.

5. Conclusion

The recent analysis suggests that the paillier method leaks privacy information and also leads the subject to compromise, so instead adding tools that does not inherit the problem of the paillier method, it's better to thicken the encrypted text with other homomorphic encryption system. In this paper, we have implemented a two-layer cryptosystem using Paillier and Elgamal algorithm to protect against privacy violation. The implementation was done using python. The result and analysis section of the paper, have shown that the cryptosystem have undergone with different inputs in order to prove the homomorphic properties of both the algorithms i.e., paillier and elgamal cryptosystem. The cryptosystem was given with different lengths of input, in order to perform analysis on the runtime and key-generation and also came up with the conclusion that as the length of prime number increases with respect to the length of the input, the cryptosystem gives a better runtime and key generation time.

References

- [1] Alfred J. Menezes and Paul C. van Oorschot and Scott A. Vanstone: "Handbook of Applied Cryptography", pp. 1 - 2, August 1996
- [2] Mohammed, Abdalbasit & Varol, Nurhayat. (2019). A Review Paper on Cryptography. 1-6. 10.1109/ISDFS.2019.8757514.
- [3] Stallings, William. (2003). Cryptography and Network Security: Principles And Practices.
- [4] Sobti, Rajeev & Ganesan, Geetha. (2012). Cryptographic Hash Functions: A Review. International Journal of Computer Science Issues, ISSN (Online): 1694-0814. Vol 9. 461 - 479.
- [5] Khalifa, Othman & Islam, Md & Khan, Sheroz & Shebani, M.S.. (2004). Communications cryptography. 220 - 223. 10.1109/RFM.2004.1411111.
- [6] U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, "Data Encryption Standard".
- [7] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985, doi: 10.1109/TIT.1985.1057074.
- [8] Paillier P. (1999) Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In: Stern J. (eds) Advances in Cryptology — EUROCRYPT '99. EUROCRYPT 1999. Lecture Notes in Computer Science, vol 1592. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48910-X_16.
- [9] Suwandi, Rifki & Nasution, Surya & Azmi, Fairuz. (2018). Secure E-voting System by Utilizing Homomorphic Properties of the Encryption Algorithm. Telkonnika (Telecommunication Computing Electronics and Control). 16. 862-867. 10.12928/TELKOMNIKA.v16i2.8420.
- [10] Catalano, Dario & Gennaro, Rosario & Howgrave-Graham, Nick. (2001). The Bit Security of Paillier's Encryption Scheme and Its Applications.. 229-243.
- [11] Balasubramanian, K. and Jayanthi, M. (2016) A Homomorphic Crypto System for Electronic Election Schemes. *Circuits and Systems*, 7, 3193-3203. doi: 10.4236/cs.2016.710272.
- [12] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. 2005. Evaluating 2-DNF formulas on ciphertexts. In *Proceedings of the Second international conference on Theory of Cryptography* (TCC'05). Springer-Verlag, Berlin, Heidelberg, 325–341. DOI:https://doi.org/10.1007/978-3-540-30576-7_18.
- [13] ElGamal T. (1985) A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In: Blakley G.R., Chaum D. (eds) *Advances in Cryptology. CRYPTO 1984. Lecture Notes in Computer Science*, vol 196. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39568-7_2

Authors' Profiles



Gautham SK received the BTech degree from Kerala Technical University (KTU), in 2019. He is currently a MTech scholar in BMSIT&M, Bengaluru, India. His research interest includes authentication, physical layer security, machine learning and deep learning.



Dr. Anjan K Koundinya has received his B.E (CSE), M.Tech (CSE), and Ph.D degree from Visveswariah Technological University (VTU), Belagavi, India. He has been awarded Best Performer PG 2010, First Rank Holder (M. Tech CSE 2010) and recipient of Best Ph.D Thesis Award by BITES, Karnataka for the academic year 2016-17. He has served in industry and academia in various capacities for more than a decade. He is currently working as Associate Professor and PG Coordinator in Dept. of CSE, BMSIT&M, Bengaluru.

How to cite this paper: Anjan K Koundinya, Gautham SK, " Two-Layer Encryption based on Paillier and ElGamal Cryptosystem for Privacy Violation", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.3, pp. 9-15, 2021.DOI: 10.5815/ijwmt.2021.03.02