Asian Journal of Research in Computer Science

6(3): 12-17, 2020; Article no.AJRCOS.61783
ISSN: 2581-8260

Security Evaluation of Pailiar Homormophic Encryption Scheme

Daniel Asiedu[1*] and Abdul-Mumin Salifu[1]

[1]Department of Computer Science, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana.

Authors' contributions

This work is as a result of MSc theses carried by author DA supervised by author AMS. Author DA had a thorough discussion with author AMS to come out with the idea. Author DA did the theoretical analysis of the study area and validated by author AMS. Author AMS wrote the abstract and the conclusion of the paper. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2020/v6i330159
Editor(s):
(1) Dr. Hasibun Naher, BRAC University, Bangladesh.
(2) Dr. Xiao-Guang Lyu, Huaihai Institute of Technology, China.
Reviewers:
(1) Varun Shukla, Dr. A. P. J. Abdul Kalam Technical University (APJAKTU), India.
(2) Suman De, SAP Labs India Pvt. Ltd, India.
(3) Zeena N. Al-kateeb, University of Mosul, Iraq.
(4) Bhavana Narain, MATS University, India.
(5) Sayyada Fahmeeda Sultana, PDA College of Engineering, India.
Complete Peer review History: http://www.sdiarticle4.com/review-history/61783

Short Research Article

Received 12 August 2020
Accepted 17 October 2020
Published 06 November 2020

ABSTRACT

In modern days of information security, much attention is drifted towards achieving the major security triad of privacy, authentication and availability. Pailiar homormophic encryption is one of the most widely area of pubic key encryption schemes researchers are exploring to enhance information security. In this paper, we presented an overview of the Pailiar cryptosystem. We further evaluated the security vulnerabilities in the cryptosystem. This was achieved through mathematical theorems and inductions. This is to present some open issues for further research to propose and implement a more robust security system based on the Pailiar homormophic encryption scheme.

Keywords: Homormophic encryption; RSA; security; cryptography.

E-mail: asalifu@cktutas.edu.gh;

1. INTRODUCTUON

Recently, much research has been diverted towards information security (cryptography) due to the increasing rate of electronic data. Apparently, diverse form of cryptographic schemes is being applied in order to achieve the essential electronic data properties of privacy, anonymity, accuracy, verifiability, integrity and robustness. The Paillier cryptosystem based on computations over multiplicative subgroup $Z^*_{n^2}$, where n is an RSA modulus (composite residuosity class problem) has received much of the research interest due to possessing some important properties useful in such areas. This scheme has some very useful properties, due to its homomorphic nature.

Using Paillier cryptosystem, modern aims of cryptography for providing information security such as Data integrity, Data privacy and Data authentication in various computational settings are achieved. Cryptographic systems with additive homomorphisms of which Paillier cryptosystem is based are useful for a lot of cryptological protocols like electronic voting, multi-party computation, Digital signature, Zero-knowledge proofs, Watermarking and fingerprinting schemes and Lottery protocols.

2. RELATED WORKS

In [1], Paillier, proposes a new probabilistic asymmetric algorithm for public key cryptography based on computation over $Z^*_{n^2}$, n being RSA modulus. The scheme is based on the assumption that computing n-th residue classes is considered to be computational difficult. The scheme can be similarly traced to the earlier cryptographic algorithm proposed by Okamoto and Uchiyama [2], whereby the group $Z^*_{p^2 q}$ is used, where p and q are large primes. It is also believed that the first threshold scheme proposed by Fouque, et al. [3] was a version of Pascal Paillier's original scheme. Damgard, et al. [4], in their paper titled "A Generalization of Paillier's Public-Key System with Applications to Electronic Voting" proposed useful application of the Paillier's scheme in the area of Electronic Voting. Jurik [5], in his thesis titled "Paillier's original scheme. Extensions to the Paillier Cryptosystem with Applications to Cryptological Protocols" proposed some useful length-flexibility. This is based on the ability to extend the plaintext space at encryption time rather than at key generation time, when the public key is chosen which was only available for symmetric ciphers in literature. Sakurai and Takagi [6,7,8], analyzed M-Paillier cryptosystem proposed by Choi et al and one-wayness of it was proven as intractable as factoring the modulus n.

3. PAILLIAR CRYPTOSYSTEM OVERVIEW

Parameters: prime numbers p, q

n = pq
λ = lcm (p−1,q−1)
g, with $g \in Z^*_{n^2}$ and the order of g is a multiple of n
Public key: n, g
Private key: p, q, λ

Encryption: plaintext m < n. Select a random r < n such that $r \in Z^*_{n.}$ cipher text $c = g^m r^n \mod n^2$

Decryption: ciphertext $c < n^2$. Plaintext $m = L (c^{\lambda} \mod n^2) / L(g^{\lambda} \mod n^2) \mod n$

3.1 Theoretical Overview Pailliar Cryptosystem

Key Generation

1. Pick two large prime numbers p and q, randomly and independently, such that gcd (pq,(p−1)(q−1))=1. If not, start again. This property is asserted if both primes are of equal length.
2. Compute n=pq, λ = lcm (p−1,q−1), where lcm stands for the least common multiple.
3. Select random integer g where g belong to $Z^*_{n^2}$.
4. Calculate the modular multiplicative inverse $\mu = (L (g\lambda \mod n^2))^{-1} \mod n$. If μ does not exist, start again from step 1.
5. The public key is (n, g). For encryption.
6. The private key is λ. For decryption. [9,10,11]

Encryption

Compute ciphertext $c = g^m r^n \mod n^2$. Select a random r < n such that $r \in Z^*_{n.,}$ m < n.

Decryption

Compute plaintext $m = L (c^{\lambda} \mod n^2) / L (g^{\lambda} \mod n^2) \mod n$. Ciphertext $c < n^2$.

4. EVALUATION OF THE PAILLIAR SCHEME

The security of the pailliar scheme is based on

Problem 1: Factorization of n, that's multiplication of two large prime numbers (equivalent to RSA modulus)

Problem 2: Deciding n-th composite residuosity. That is: $z = y^n \bmod n^2$

Our focus here is how we can recover the original message (m) without solving Problem 1 and Problem 2 above.

4.1 Choice of the Least and the Highest Value/Number of R ∈ Z^*_N

The first attack is on the choice of the least and the highest value/number of $r \in Z^*_n$ as random number for semantic security (r).

Example 1:

Let p=3, q=5 then
$n=15$, $n^2 = 225$

The generator g, in most general form is given by

$g = (1 + \alpha.n)\ \beta^n, \quad \alpha, \beta \in Z_n^*$
If α=1 and β=1 then g=16
Random number r < n such that $r \in Z^*_n$.

If we consider the Table 1 above, we have the message we will be transmitting on the first row starting from 0 to 14.

We have all the possible values of $r \in Z^*_n$ on the first column, starting from 1, 2, 4 ……, 14 in that order.

The gray area of Table 1 indicates the resulting cipher text.

Analysis One: when we choose the least value of $r \in Z^*_n$ (which is 1) as our random number for semantic security.

There is something unique (pattern) about the cipher text generated for all the messages, 0 – 14, m < n when analysis one is true. Careful examination of the Table 1 above when r=1 shows that the cipher text has a constant increasing growth (addition) by the value of n (n=15) for all m < n (all the possible cipher text). This is because the least value of $r \in Z^*_n$ is chosen as the random number for semantic security.

How to recover the original message when analysis one is asserted:

Firstly, take the least and the highest message value that belongs to m < n. That is 0 and 14 considering the example (Table 1) above.

Secondly, encrypt them (0 and 14), which gives 1 and 211 as the cipher text respectively. It means that 1 is the first valid cipher text if we are to transmit all the messages (0 – 14) and also 211 is the last valid cipher text if we are to transmit all the messages (0 – 14).

Once we get the first and the last valid ciphers, the remaining cipher text which will occur between them is just adding the value of n (15) to the remaining ciphers starting from the first valid cipher text. That is if we are to transmit the next message which is 1 in the Table above, we simply add n (15) to the value of the first valid cipher text which is one (1) resulting 16 as the next cipher text in that order.

Table 1. The results of computing example 1 with its valid cipher text

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	m
		1	16	31	46	61	76	91	106	121	136	151	166	181	196	211	g^m
1	1	1	16	31	46	61	76	91	106	121	136	151	166	181	196	211	
2	143	143	38	158	53	173	68	188	83	203	98	218	113	8	128	23	
4	199	199	34	94	154	214	49	109	169	4	64	124	184	19	79	139	
7	118	118	88	58	28	223	193	163	133	103	73	43	13	208	178	148	
8	107	107	137	167	197	2	32	62	92	122	152	182	212	17	47	77	
11	26	26	191	131	71	11	176	116	56	221	161	101	41	206	146	86	
13	82	82	187	67	172	52	157	37	142	22	127	7	112	217	97	202	
14	224	224	209	194	179	164	149	134	119	104	89	74	59	44	29	14	
r	r^n																

Results of random values of r<n

Lastly, in recovering the message, subtract the first valid cipher text (1) from the cipher text you want to recover the original message and divide the result by n (15).

Example: let's say we want to transmit 7, 8, and 10. You will get 106, 121 and 151 respectively as cipher text (note that r=1).

Taking 106,

106 – 1 = 105
105/n = 105/15 = 7 (which is the original message)

Taking 121,

121 – 1 = 120
120/n = 120/15 = 8 (which is the original message)

Taking 151,

151 – 1 = 150
150/n = 150/15 = 10 (which is the original message)

Note: one (1) here is the first valid cipher text indicated above.

Analysis Two: when we choose the highest value of $r \in Z^*_n$ (which is 14) as our random number for semantic security.

There is also something unique (pattern) about the cipher text generated for all the messages, 0 – 14, m < n when analysis two is true. Careful examination of the Table 1 when r=14 shows that the cipher text has a constant decreased (subtraction) by the value of n (n=15) for all m < n (all the possible cipher text). This is because the highest value of $r \in Z^*_n$ is chosen as the random number for semantic security.

How to recover the original message when analysis two is asserted:

Firstly, take the least and the highest message value that belongs to m < n likewise. That is 0 and 14 considering the example (Table 1) above.

Secondly, encrypt them (0 and 14), which gives 224 and 14 as the cipher text respectively. It means that 224 is the first valid cipher text if we are to transmit all the messages (0 – 14) and also 14 is the last valid cipher text if we are to transmit all the messages (0 – 14).

Once we get the first and last possible cipher's, the remaining cipher text which will occur between them is just subtracting the value of n (15) from the remaining ciphers starting from the first valid cipher text. That is if we are to transmit the next message which is 1 in the Table 1, we simply subtract n (15) from the value of the first valid cipher text which is 224 resulting 209 as the next cipher text in that order.

Lastly, in recovering the message, subtract the cipher text you want to recover the original message from the first valid cipher text (224) and divide the result by n (15).

Example: let's say we want to transmit 7, 8, and 10. You will get 119, 104 and 74 respectively as cipher text (note that r=14).

Taking 119,

224 – 119 = 105
105/n = 105/15 = 7 (which is the original message)

Taking 104,

224 – 104 = 120
120/n = 120/15 = 8 (which is the original message)

Taking 151,

224 – 74 = 150
150/n = 150/15 = 10 (which is the original message)

Note: 224 here is the first valid cipher text indicated above.

4.2 Mathematics of the Encryption Scheme

The second attack is on the mathematics of the encryption scheme, $g^m r^n \bmod n^2$.

When we consider the Table 1 for multiplicative subgroup $Z^*_{15}{}^2$ ($Z^*_n{}^2$), the $g^m \bmod n^2$ part of the cipher Text is a matter of increasing the cipher text by the value of n starting from the least cipher text which is one (1) up to the highest which is 211 for all the message space m < n. What makes the difference is the value of random semantic security append to g^m, that is $g^m.r^n$.

Any cipher text you pick from the multiplicative subgroup $Z^*_{15^2}$, apart from cipher text resulting from r=1 and r=14 (the least and the highest value of r) can be traced to the original message by solving the equation below:

$$g^m r^n \equiv c \bmod n^2 \quad (1)$$

Where:

g^m is the cipher text without random semantic security value r^n is the random semantic security valuec is the cipher text you trying to recover the original message.

From Eq.1, we can have:

$$r^n \equiv (g^m)^{-1}.c \bmod n^2 \quad (2)$$

Where $r^n \in r < Z^*_n$

By solving Eq.2, you can extract the random semantic security part of the cipher text (c).

This idea is based on the fact that any cipher text you pick from the multiplicative subgroup is just a combination of g^m and $r^n \bmod n^2$

Illustration:

Let consider all the g^m ($g^m \bmod n^2$) values in the Table 1. That is, 1, 16, 31, 46, 61, 76 …, 211. Note also that all the cipher text generated within the multiplicative subgroup are coprime to 225 ($Z^*_{15^2}$).

Let also consider all the r^n ($r^n \bmod n^2$) values in the Table 1. That is, 1, 143, 199, 118, 107… 224.

We will now pick a random cipher text from the multiplicative subgroup $Z^*_{15^2}$, which is 94. This cipher text (94) we have selected consist of g^m part and r^n part.

We will now test the cipher we selected (94) against the values of g^m ($g^m \bmod n^2$) using Eq.2 until we get the first valid result belonging to r^n ($r^n \bmod n^2$).

From Eq.2

When $g^m = 1$,
$r^n \equiv (1)^{-1}.94 \bmod 225$
$(1)^{-1}.94 \bmod 225$
$94 \notin r^n$
When When $g^m = 16$,
$r^n \equiv (16)^{-1}.94 \bmod 225$
$16^{-1}.94 \bmod 225$
$34 \notin r^n$
When $g^m = 31$,
$r^n \equiv (31)^{-1}.94 \bmod 225$
$31^{-1}.94 \bmod 225$
$199 \in r^n$

When $g^m = 31$, we now have $r^n = 199$ which is part of $r^n \bmod n^2$, $r \in Z^*_n$. This result implies that the cipher text 94, was simply a multiplication of $g^m = 31$ and $r^n = 199$ all mod n^2. Now to get the message m, we compute:

$g^m \equiv 31 \bmod n^2$
$16^m \equiv 31 \bmod 225$
m=2

The same method can be repeated for all the cipher text within the multiplicative subgroup to recover the original message.

4.3 The Third Attack is on the Repetition of the Message (M)

The third attack is on the repetition of the message (m) value as the cipher text for transmission.

The system does not have any unique cipher representation for the highest message belonging to m < n for transmission when highest random semantic security value $r \in Z^*_n$ is chosen other than the message itself. In other words, it would always produce a cipher text equal to the original message.

Illustration:

Let's consider the Table 1, if we decide to transmit 14, which is the highest message of m < n and r (highest random semantic security value) = 14, it will produce the cipher text: $16^{14}.14^{15}$ mod 225 =14 which is the same as the message we are transmitting.

Another example:

Let p=7, q=11 n=77, n^2 =5929, g=78, r=76

Here the message m for transmission is 76 (highest in m < n) and the highest value of $r \in Z^*_n$ is 76. The cipher text (c) then will be:

$C= 78^{76}.76^{77} \bmod 5929$

C= 76 equal to the message we are transmitting. It must be noted here that, this findings are valid for all g (generator) = n +1

5. CONCLUSION

The overview of Pailiar homormophic encryption scheme is presented. The security vulnerabilities of the scheme are shown using mathematical theorems and inductions. The results shows that the pailiar homormophic encryption is not robust and vulnerable to various attacks.

Based on this problem, future work will pivot on finding a new secured cryptosystem that can enhance the security of Pailiar homormophic encryption.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Paillier P. Public-Key Cryptosystems based on Composite Degree Residue Classes, Advances in Cryptology - EUROCRYPT '99, LNCS. Springer Verlag. 1999;1592:223-238.
2. Okamoto T, Uchiyama S. A New Public-Key Cryptosystem as Secure as Factoring, Advances in Cryptology - EUROCRYPT '98, LNCS. Springer Verlag. 1998;1403:308-318.
3. Fouque P-A, Poupard G, Stern J. Sharing Decryption in the Context of Voting or Lotteries, Financial Cryptography (2000), LNCS. Springer Verla. 2001;1962:90-104.
4. Damgard I, Jurik M, Nielsen JB. A Generalization of Paillier's Public-Key System with Applications to Electronic Voting, to appear in special issue on Financial Cryptography, International Journal on Information Security (IJIS). Springer Verlag.
5. Mads J. Jurik. Extensions to the Paillier Cryptosystem with Applications to Cryptological Protocols. PhD thesis. 2003;xii+117.
6. Sakurai K, Takagi T. (2002) On the Security of a Modified Paillier Public-Key Primitive. In: Batten L, Seberry J. (eds) Information Security and Privacy. ACISP. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg. 2002;2384. Available:https://doi.org/10.1007/3-540-45450-0_33
7. Catalano D, Gennaro R, Howgraw-Graham N. The bit security of Paillier's encryption scheme and its applications. Eurocrypt 2001, LNCS 2045. 2001;229-243.
8. Shukla V, Chaturvedi A, Srivastava N. Nanotechnology and cryptographic protocols: Issues and possible solutions, Nanomaterials and Energy. 2019;8(1):1-6. DOI:https://doi.org/10.1680/jnaen.18.00006
9. Acar A, Aksu H, Uluagac AS, Conti M. A survey on homomorphic encryption schemes: Theory and implementation. ACM Comput. Surv. 2018;51:1–35.
10. Dowlin N, Gilad-Bachrach R, Laine K, Lauter K, Naehrig M, Wernsing J. Manual for using homomorphic encryption for bioinformatics. Proc. IEEE. 2017;105:552–567.
11. El Makkaoui K, Ezzati A, Beni-Hssane A, et al. Fast Cloud–Paillier homomorphic schemes for protecting confidentiality of sensitive data in cloud computing. J Ambient Intell Human Comput. 2020;11:2205–2214. Available:https://doi.org/10.1007/s12652-019-01366-3

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/61783