Proposal of Two Enhanced Paillier Cryptosystems

Enas Tariq Khudir
Department of Computer Sciences
University of Technology

Abstract

This paper presents two enhanced Paillier cryptosystem. Firstly, this paper prove that the one-wayness of the two proposed enhanced Paillier cryptosystem is as intractable as factoring the modulus n, if the public key g can be generated only by the public modulus n. Secondly, this work prove that the oracle that can generate the public-key factors the modulus n. Thus the public keys cannot be generated without knowing the factoring of n. The Paillier cryptosystem can use the public key g = 1 + n, which is generated only from the public modulus n. Finally, discussion the relationship between the two proposed enhanced Paillier cryptosystem and the modified Paillier cryptosystem and the Okamoto-Uchiyama scheme.

أقتراح طريقتين محسنتين لتشفير Paillier

أيناس طارق خضير
قسم علوم الحاسبات
الجامعة التكنولوجية

الخلاصة

هذا البحث يقدم طريقتين محسنتين لتشفير Paillier. أولاً سنبرهن على ان الطريق الواحد للطريقتين المحسنتين لتشفير Paillier متوافقة مع التجزئة لعوامل n ، اذا كان المفتاح العام g يتولد فقط من القيمة العامة n. ثانياً هذا البحث يبرهن على امكانية توليد معاملات المفتاح العام n. هذه المفاتيح العامة لا تتولد الا من خلال معرفة معاملات n. تشفير Paillier يستخدم المفتاح العام g = n+ 1 الذي يتولد فقط من خلال n. أخيراً سيتم مناقشة العلاقة بين الطريقتين المحسنتين لتشفير Paillier وطريقة Paillier المطورة اصلاً وطريقة Okamoto-Uchiyama.

Keywords : Public-Key Cryptosystem, M-Paillier Cryptosystem, Paillier Cryptosystem, Okamoto-Uchiyama Scheme.

1- Introduction

Paillier proposed a probabilistic encryption scheme [1]. The Paillier cryptosystem encrypts a message m by E (m,r) = $g^m h^n$ mod n^2, where g,n is the public key and h is a random integer. The encryption function E (m,r) has a homomorphic property: E(m_1, r_1) E(m_2, r_2) = E($m_1 + m_2, r_1 r_2$).

The Paillier cryptosystem have been extended to various scheme.Damgard and Jurik proposed a scheme with moduli n^2(i > 2) that is useful for voting system [2]. Galbraith extended the Paillier cryptosystem to a scheme over elliptic curves [3]. Catalano al. proposed an efficient variant scheme that encrypts a message by r^e(1+mn) mod n^2, where e, n is the RSA public key and r is random integer in ((ZZ/nZZ)^x[4]. Because the encryption key e can be chosen small, the encryption speed of their scheme is much faster than that of the original scheme. Sakurai and Takagi investigated the security of their scheme [5]. Galindo et al. constructed their scheme over elliptic curves [6].

The decryption algorithm of the Paillier cryptosystem involves a modular inversion L $(g^{\lambda})^{-1}$ mod n, where n = pq and λ = lcm (p − 1, q − 1). Choi et al. proposed how to eliminate the inverse by modifying the generation of the key g [7]. They use a special public-key g that satisfies g^{λ} = 1 + n modn^2. The distribution of their keys is not the same as that of the original one. The reduced number-theoretic problems are different from the original scheme. However, they did not prove the one-wayness / semantic security for the distribution. Call their scheme as the modified Paillier cryptosystem (Enhanced-Paillier cryptosystem).

2- Paillier Cryptosystem

The public key of the Paillier cryptosystem is the RSA modulus n and an element g ϵ $(ZZ/n^2ZZ)^x$ whose order is divisible by n. The secret key is λ = lcm (p −1, q – 1), where p, q are the primes of n = pq. A message m ϵ {0, 1, ..., n − 1} is encrypted by c = $g^m h^n$ mod n^2 for a random integer h ϵ ZZ/n ZZ. Figure (1) illustrates Paillier cryptosystem.

Key Generation
n = pq, the RSA modulus λ = lcm (p − 1, q − 1) g ϵ ZZ/n^2ZZ s.t. n\ord_{n^2}(g) Public-key: (n, g), Secret key: λ
Encryption of m
m ϵ {0, 1, ..., n − 1}, a message h ϵ R ZZ/n ZZ c = $g^m h^n$ mod n^2, a ciphertext
Decryption of c
m = L(c^{λ} mod n^2)L(g^{λ} mod n^2)$^{-1}$ mod n

Figure 1: Paillier Cryptosystem

Paillier cryptosystem is a probabilistic encryption and has a homomorphic property. The ciphertext c is decrypted by m = L(c^{λ} mod n^2)L (g^{λ} mod n^2)$^{-1}$mod n using the secret key λ, where L(a mod n^2) = (a-1)/n for an integer a such that a = 1 mod n.

The key g is the element of $(ZZ/n^2ZZ)^x$ s.t. n\ord_{n^2}(g). In the group $(ZZ/n^2ZZ)^x$, there are (n−1)φ(n) elements whose order is divisible by n. The order of the group $(ZZ/nZZ)^x$ is nφ(n). The probability that a random element satisfies the key condition is 1 − 1/n and it is an overwhelming probability in the bit-length of the public modulus n. Therefore can use a random g of ZZ/n^2ZZ as the public key.

2-1 Security of the Paillier Cryptosystem

In order to discuss the security of the Paillier cryptosystem, define the following number theoretic problems. Denote by RSA_{moulus} and $G_{Paillier}$ the set of the RSA modulus n and the public key g of the Paillier cryptosystem, respectively.

Let c be an integer of $(ZZ/n^2ZZ)^x$. The n-th residuosity class of c with respect to g ϵ $G_{Paillier}$ is the unique integer x which satisfies c = $g^m h^n$ mod n^2 for an integer h ϵ ZZ/nZZ. We denote by $[[c]]_g$ the n-th residuosity class of c with respect to g.

The computational composite residuosity problem (C-CRP) is to compute the $[[c]]_g$ for given c ϵ $(ZZ/n^2ZZ)^x$, g ϵ $G_{Paillier}$, and n ϵ RSA_{moulus}. The decisional composite residuosity problem (D-CRP) is to decide whether x = $[[c]]_g$ holds for given x ϵ ZZ/n ZZ, c ϵ (ZZ/n2ZZ)×, g ϵ $G_{Paillier}$r, and n ϵ RSA_{moulus}. An algorithm that factors the modulus n can solve the C-CRP, but the opposite direction is unknown. There is a possibility that the C-CRP is solved without factoring the modulus n.

The problem of breaking the one-wayness of the Paillier cryptosystem is to find the integer m for given n ϵ RSA_{moulus}s, g ϵ $G_{Paillier}$, h ϵ ZZ/n ZZ, and c = $g^m h^n \bmod n^2$.

The one-wayness assumption of the Paillier cryptosystem is that for any probabilistic polynomial time algorithm $A^{ow}_{Paillier}$ the probability

$$Pr_{m \epsilon R} \text{ ZZ/nZZ } [n \leftarrow RSA_{moulus}, h \leftarrow R \text{ ZZ/nZZ}, g \leftarrow G_{Paillier}, c = g^m h^n \bmod n^2 : A^{ow}_{Paillier}(c) = m]$$

is negligible in log n. It is known that the one-wayness of the Paillier cryptosystem is as intractable as breaking the computational composite residuosity problem (C-CRP) [1].

A semantic security adversary $A^{SS}_{Paillier}$ against the Paillier cryptosystem consists of two stages: the find stage $A^{SS1}_{Paillier}$ and the guess stage $A^{SS2}_{Paillier}$. Algorithm $A^{SS1}_{Paillier}$ returns two messages m_0, $m_1$and a state information st from a public-key n. Let c be a cipher text of either m_0 or m_1. The $A^{SS1}_{Paillier}$ guesses whether the cipher text c is the encryption of m_b (b ϵ {0, 1}) for given (c, m_0, m_1, st) and outputs b. The semantic security of the Paillier cryptosystem is that for any probabilistic polynomial time algorithm $A^{SS}_{Paillier}$ the probability

$$2P_r [n \leftarrow RSA_{moulus}, (m_0, m_1, st) \leftarrow A^{SS1}_{Paillier}(e,n), b \leftarrow \{0, 1\}, h \leftarrow R \text{ ZZ/n ZZ}, g \leftarrow G_{Paillier}, c = g^m h^n \bmod n^2 : A^{SS2}_{Paillier}(c, m_0, m_1, st) = b] - 1$$

is negligible in log n. It is known that the semantic security of the Paillier cryptosystem is as intractable as breaking the decisional composite residuosity problem (D-CRP) [1]. The semantic security is often called as the indistiguishability. If a semantic security adversary is allowed to access the decryption oracle, the attack model is called chosen cipher text attack. A public cryptosystem that is semantically secure against the chosen cipher text attack is called an IND-CCA2 scheme [8]. The IND-CCA2 security has become one of the criteria for a general purpose public-key cryptosystem.

2-2 The Modified Paillier Cryptosystem

The main differences of the modified-Paillier cryptosystem from the original one are the choice of the key g and the decryption algorithm, figure (2) illustrate modified Paillier [17]. The public key g is chosen from the set

$$G_{modified-Paillier} = \{ g \epsilon (ZZ/n^2ZZ)^x \text{ s.t. } g^\lambda = 1 + n \bmod n^2 \}. \quad (1)$$

The set $G_{modified-Paillier}$ is a subset of all public keys g of the original Paillier cryptosystem, i.e., $G_{modified\ Paillier} \subset G_{Paillier}$.

Then the computation L ($g^\lambda \bmod n^2$) in the Paillier decryption is equal to 1, due to $g^\lambda \bmod n^2 = 1 + n$. We do not have to compute the inversion in the decryption process for any g ϵ $S_{modified-Paillier}$. Figure (2) illustrates the encryption and the decryption of the Modified Paillier cryptosystem.

Key Generation
n = pq, the RSA modulus λ = lcm (p − 1, q − 1) g ϵ ZZ/n^2ZZ s.t. $g^\lambda = 1 + n \bmod n^2$ Public-key: (n, g), Secret key: λ
Encryption of m
m ϵ {0, 1, ..., n − 1}, a message h ϵ R ZZ/n ZZ C= $(g^m h^n \bmod n^2)^s$, a ciphertext
Decryption of c
M = L($c^\lambda \bmod n^2$)

Figure 2: The Modified Paillier Cryptosystem

Generate the public key g as follows: Write the public-key g as the n-adic representation such that g = a + bn, where 0 ≤ a, b < n are unique. Because of $(a+bn)^{\lambda} = 1 + \left(L\left(a^{\lambda}\right) + \lambda a^{-1}b\right)n \bmod n^2$, the public key g = a+bn has relationship:

$$L\left(a^{\lambda}\right) + \lambda a^{-1}b = 1 \bmod n, \qquad (2)$$

Where L(r) = (r − 1)/n. Thus, b is computed by b = $(1 - L\left(a^{\lambda}\right)a\lambda^{-1}b$ mod n for a given random a ϵ ZZ/n ZZ, and the secret keyλ. The density of the $G_{modified-Paillier}$ is at most n. The probability that a random element of $(ZZ/n^2ZZ)^x$ is contained in the $G_{modified-Paillier}$ is at most 1/φ (n), which is negligible in the bit-length of the public key n.

2-3 Okamoto-Uchiyama Schemes

In this section discuss the relationship between the Okamoto-Uchiyama scheme [16] and the E-Paillier cryptosystem. We call the Okamoto-Uchiyama scheme as the OU scheme in the following. The OU scheme is constructed over the ring ZZ/nZZ, where $n = p^2q$ and p, q are primes. The one-wayness and the semantic security of the OU scheme are as intractable as factoring the modulus n and solving the p subgroup problem, respectively [16].

The public key of the OU scheme is the modulus n and an element g ϵ $(ZZ/nZZ)^x$ whose order in the subgroup $(ZZ/p^2ZZ)^x$ is divisible by p. If we choose a random g from $(ZZ/nZZ)^x$, the probability that the order of g in $(ZZ/p^2ZZ)^x$ is divisible by pis 1 − 1/p. The secret key is the primes p and $g_p = g^{p-1} mod\ p^2$. A message m ϵ {0, 1, ..., 2^{K-2}} is encrypted by $c = g^{m+rn} mod\ n$ for a random integer r ϵ ZZ/nZZ, where k is the bit-length of p. The ciphertext c is decrypted by m = L (c^{p-1} mod p^2)L(g^{p-1} modp^2)$^{-1}$ mod n using the secret key p, where L(a mod n^2) = (a − 1)/n for an integer a such that a = 1 mod n. Figure (3) illustrates Okamoto-Uchiyama cryptosystem.

Key Generation
k =the bit length of prime p n = p^2q, the modulus g ϵ ZZ/nZZ s.t. p\ord_{p^2}(g) $g_p = g\ mod\ p^2$ Public-key: (n, g, k), Secret key: p, g_p
Encryption of m
m ϵ {0, 1, ..., 2^{k-1}}, a message r ϵ R ZZ/n ZZ, a random integer c = g^{m+rn} mod n, a ciphertext
Decryption of c
m = L(c^{p-1} mod p^2)L(g_p^{p-1}mod p^2)$^{-1}$ mod p

Figure 3: Okamoto-Uchiyama Cryptosystem

Fujisaki and Okamoto enhanced the security of the OU scheme using the random oracle model [9]. call it as the FO scheme in the following. The IND-CCA2 security of the FO scheme can be proved as hard as factoring the modulus n with a tight security reduction. They modified the generation of the keys n, g in order to match their security proof. The primes p, q of the key n = p^2q are safe primes, i.e., (p − 1)/2,(q − 1)/2 are also primes. The key g is the integer g of $(ZZ/nZZ)^x$ whose order in the group $(ZZ/p^2ZZ)^x$ is p(p − 1). The probability that the order of g in $(ZZ/p^2ZZ)^x$ is p(p − 1), which is at least $2^{-1}(1 - 2^{-k+1})$, where k is the bit-length of prime p. Coi et al. proposed enhanced version of the Okamoto-Uchiyama scheme [7].

call it the enhanced OU (M-OU) scheme in the following. The E-OU scheme uses a key contained in the following the set

$$G_{M-OU} = \{g \in (\mathrm{ZZ}/p^2\mathrm{ZZ})^x \text{ s.t. } g^{p-1} = 1 + p \bmod p^2\}. \quad (5)$$

There are at most p elements which satisfy $a^{p-1} = 1 + p \bmod p^2$ for aϵ $(\mathrm{ZZ}/p^2\mathrm{ZZ})^x$.Then the probability that a random g from $(\mathrm{ZZ}/n\mathrm{ZZ})^x$is contained in the set of keys is at most 1/φ(p), which is negligible in the bit length of p. It is an open problem to prove the one-wayness of the Okamoto-Uchiyama scheme for g ϵ G_{M-OU} .

3- The Proposed Enhanced Paillier Cryptosystem

3-1 First Proposed Enhanced Paillier Cryptosystem

The main differences of the First E-Paillier cryptosystem from the original one are the choice of the public keys g and the decryption algorithm. The public keys g is chosen from the set

$G_{First\ E-Pailler}$ = {g ϵ ZZ/nZZ s.t. $g^{\lambda} = 1 + n$ mod n}. (1)

The set $G_{First\ E-Pailler}$ is a subset of all public keys g of the original Paillier cryptosystem, i.e., $G_{efirst\ EPailler}$ _$G_{Pailler}$.

Then the computation L(c^{λ} mod n) $L'(g^{\lambda} \bmod n)^{-1}$ in the Paillier decryption is equal to 1, due to g_ mod n = 1 + n. We do not have to compute the inversion in the decryption process for any g ϵ $S_{First\ E-Paillier}$. The encryption and the decryption of the First E-Paillier cryptosystem are as follows in Figure (4).

Key Generation
n = pq, the RSA modulus λ = lcm (p − 1, q − 1) g ϵ ZZ/nZZ s.t. $g^{\lambda} = 1 + n$ mod n Public-key: (n, g), Secret key: λ
Encryption of m
m ϵ {0, 1, ..., n − 1}, a message h ϵ R ZZ/n ZZ $C' = (g^m h^n \bmod n)^s$, a ciphertext
Decryption of c
C=$(C')^{s^{-1}}$mod n M = L(c^{λ} mod n) $L'(g^{\lambda} \bmod n)^{-1}$ mod n

Figure 4: The First Enhanced Paillier Cryptosystem

Generate the public key g as follows: Write the public-key g as the n-adic representation such that g = a + bn, where 0 ≤ a, b < n are unique. Because of$(a + bn)^{\lambda} = 1 + (L(a^{\lambda}) + \lambda a^{-1} b)n \bmod n$, the public key g = a+bn has relationship:

$$L(a^{\lambda}) + \lambda a^{-1} b = 1 \bmod n, \quad (2)$$

Where L(r) = (r − 1)/n. Thus, b is computed by b = $(1 - L(a^{\lambda}) a\lambda^{-1} b \bmod n$ for a given random a ϵ ZZ/n ZZ, and the secret key λ.

3-2 Second Proposed Enhanced Paillier Cryptosystem

The main differences of the Second E-Paillier cryptosystem from the original one are the choice of the public keys g and the decryption algorithm. The public keys g is chosen from the set

$G_{second\ E-Pailler}$ = {g ϵ ZZ/nZZ s.t. $g^{\lambda} = 1 + n$ mod n}. (1)

The set $G_{second\ E-Paillier}$ is a subset of all public keys g of the original Paillier cryptosystem, i.e., $G_{second\ E-Paillier} \_ G_{Paillier}$.

Then the computation L (c^{λ}) $L(g^{\lambda})^{-1}$ in the Paillier decryption is equal to 1, due to g_ mod n = 1 + n. We do not have to compute the inversion in the decryption process for any g ϵ $S_{second\ E-Paillier}$. The encryption and the decryption of the second E-Paillier cryptosystem are as follows in Figure (5).

Key Generation
n = p-q, the RSA modulus λ = lcm (p − 1, q − 1) g ϵ ZZ/nZZ s.t. $g^{\lambda} = 1 + n$ mod n Public-key: (n, g), Secret key: λ
Encryption of m
m ϵ {0, 1, ..., n − 1}, a message \\VVY7888S ϵ R ZZ/n ZZ $C = g^{m}h^{n}$ mod n , a ciphertext
Decryption of c
M = L(c^{λ}) $L(g^{\lambda})^{-1}$ mod n

Figure 5: The Second Enhanced Paillier Cryptosystem

Generate the public key g as follows: write the public-key g as the n-adic representation such that g = a + bn, where 0 ≤ a, b < n are unique. Because of $(a + bn)^{\lambda} = 1 + \left(L\left(a^{\lambda}\right) + \lambda a^{-1} b\right) n \bmod n$, the public key g = a+bn has relationship:

$$L\left(a^{\lambda}\right) + \lambda a^{-1} b = 1 \bmod n, \qquad (2)$$

Where L(r) = (r − 1)/n. Thus, b is computed by b = (1 − $L\left(a^{\lambda}\right) a \lambda^{-1} b$ mod n for a given random a ϵ ZZ/n ZZ, and the secret key λ.

4- Security of the Proposed Enhanced-Paillier Cryptosystem

Redefine the number theoretic problems related to the Enhanced-Paillier cryptosystem. The only difference between the Paillier cryptosystem and the Enhanced-Paillier cryptosystem is the distribution of the public key g. discusses the C-CRP and D-CRP for the public key g from the E-Paillier cryptosystem. can prove that the one-wayness of the E-Paillier cryptosystem is as intractable as factoring the modulus n, if the public key g can be generated only by the public information n, i.e., g is samplable from ZZ/n^2ZZ in the polynomial time of log n.

The computational composite residuosity problem for the $G_{enhanced-Paillier}$ is to compute the [[c]] g for given c ϵ (ZZ/n^2ZZ)^x, g ϵ $G_{enhanced-Paillier}$, and n ϵ $RSA_{modulus}$. Then can prove the following theorem.

2. Theorem Breaking the C-CRP for the $G_{enhanced-Paillier}$ is as intractable as factoring n, if the public key g can be generated only by the public modulus n.

Proof: If the modulus n is factored, the C-CRP can be easily solved. Prove the different direction. Let A be the algorithm, which solves the C-CRP for the $G_{enhanced-Paillier}$ in time t and with advantage ε. The algorithm A can compute the $[[c]]_g$ for given c ϵ (ZZ/n^2ZZ)^x, g ϵ $G_{enhanced-Paillier}$, and n ϵ $RSA_{modulus}$. Note that if the key g is generated only by public key information, there is no information leakage about the secret keys from the $G_{enhanced-Paillier}$. Here, let c = (1 + rn)h^n mod n^2 for random integers r ϵ (ZZ/n ZZ)^{x}and h ϵ (ZZ/nZZ)^x, then the integer c is uniformly distributed in the ring (ZZ/n^2ZZ)^x. The distribution of c is equivalent to that of instances to C-CRP. Note that L (c^{λ} mod n^2) = r λ mod n holds for the decryption of the enhanced- Paillier cryptosystem, where the λ is the secret key.

Thus the algorithm A outputs t = r λ mod n for inputs c and the secret key λ is recovered by λ = $tr^{-1} mod\ n$. The probability that gcd (r, n) > 1 holds is negligible. The modulus n can be factored using λ. The time and advantage of the algorithm A is $t + \partial((\log n)^2)$ and ε, respectively. Can mount this result to the one-wayness of the enhanced-Paillier cryptosystem.

3. Corollary The one-wayness of the enhanced-Paillier cryptosystem is as intractable as factoring n, if the public key g can be generated by only the public modulus n.

Proof: To prove that breaking the one-wayness of the enhanced-Paillier cryptosystem is as hard as breaking the D-CRP for the $G_{enhanced-Paillier}$. However, this is trivial from the definitions. There are several general conversion techniques, which enhance the security of a public-key cryptosystem to make it an IND-CCA2 scheme [9], [10], [11], [12]. The conversion techniques [10], [12] can convert a one-way public-key scheme to be an IND-CCA2 scheme. Therefore the enhanced-Paillier cryptosystem converted using these techniques can be proved as intractable as factoring the modulus n if the public key g can be generated by only the public modulus n.
The semantic security of the enhanced -Paillier cryptosystem is also different from the original D-CRP. to redefine the D-CRP. The decisional composite residuosity problem (D-CRP) for the $G_{enhanced-Paillier}$ is to decide whether $x = [[c]]_g$ holds for given x ϵ (ZZ/n ZZ)^x , c ϵ (ZZ/n^2 ZZ)^x, $g \in G_{Paillier}$, and $n \in \mathrm{RSA}_{modulus}$. Then can prove that the semantic security of the enhanced-Paillier cryptosystem is as hard as breaking the D-CRP for the $G_{enhanced-Paillier}$. State that as a theorem:

4. Theorem The semantic security of the enhanced-Paillier cryptosystem is as hard as breaking the decisional composite residuosity problem for the $G_{enhanced-Paillier}$. If an algorithm A breaks the original D-CRP, then the D-CRP for the $G_{enhanced-Paillier}$ can be solved using this algorithm A. It is an open problem to investigate the opposite direction.

5- Power of Generating the Key g

In this section investigate the computational ability of generating the public key g. The public key g for the original Paillier cryptosystem can be chosen as random from g ϵ (ZZ/n^2 ZZ)^x or as g = 1 + n using only the public information n.

Therefore anyone can generate the key g for the original Paillier cryptosystem. On the contrary, we prove that the power to generate the public key g for the enhanced-Paillier cryptosystem can factor the $\mathrm{RSA}_{modulus}$. cannot generate the key g for the enahanced-Paillier without factoring n.

Let ∂_n be the oracle, which answers b such that g = a + bn ϵ $G_{enhanced-Paillier}$ for given $\mathrm{RSA}_{modulus}$ n and a random integer a ϵ ZZ/n ZZ. In the real world, the oracle is an algorithm, which computes the public key g for a given public key n. As reviewed in section 3, the key g is represented as two integers g = a + bn, where 0≤_ a, b < n. The integer b can be computed by $b = (1 - L(a^{\lambda}))a\lambda^{-1} mod\ n$ for a given integer a if the secret key λ is known. Then we have the following theorem.

5. Theorem The $\mathrm{RSA}_{modulus}$ n can be factored using the oracle ∂_n.
Proof: construct an algorithm A, which computes λ using the oracle ∂_n. It is known that, once the secret key λ is obtained, the modulus can be easily factored.
The algorithm A works as follows:
1. A generates a random a_1 in ZZ/nZZ, runs ∂_n (a_1) and obtains b_1 such that
$g_1 = a_1 + b_1 n \in G_{enhanced-Paillier}$.
2. A generates a random a_2 in ZZ/nZZ, runs ∂_n (a_2) and obtains b_2 such that
$g_2 = a_2 + b_2 n \in G_{enhanced-Paillier}$.

3. A computes $a_3 = a_1 a_2 \bmod n$, runs $\mathcal{O}_n(a_3)$ and obtains b_3 such that
$g_3 = a_3 + b_3 n \in G_{enhanced-Paillier}$.
4. Output $\lambda = (a_1^{-1}b_1 + a_2^{-1}b_2 - (a_1 a_2)^{-1}b_3)^{-1} \bmod n$.
In step 1 and step 2 we know the relationships: $L(a_1^{\lambda} + \lambda a_1^{-1}b_1 = 1 \bmod n$ and $L(a_2^{\lambda} + \lambda a_2^{-1}b_2 = 1 \bmod n$. From $L(a_1^{\lambda}a_2^{\lambda}) = L(a_1^{\lambda}) + L(a_2^{\lambda}) \bmod n$, we have $L(a_1^{\lambda}) + L(a_2^{\lambda}) + \lambda(a_1 a_2)^{-1}b_3 = 1 \bmod n$ in step 3. Thus we obtain the following equation:

$$\lambda a_1^{-1}b_1 + \lambda a_2^{-1}b_2 - \lambda(a_1 a_2)^{-1}b_3 = 1 \bmod n. \quad (4)$$

If know λ, the modulus n can be factored with at least probability 1/2. Let t, ϵ be the time and the advantage of the oracle $\mathcal{O}_n$. The time and the advantage of the algorithm A is $t + \mathcal{O}((\log n)^2)$ and ϵ^3, respectively.

From this theorem, it is as intractable as factoring n to generate the public key g for a given public key n. The information obtained from the public key g for the E-Paillier cryptosystem is essentially different from that for the original Paillier cryptosystem. The C-CRP/D-CRP for the $G_{M-Paillier}$ differs from the original C-CPR/D-CRP. Thus the one-wayness or semantic security for the E-Paillier cryptosystem are generally not same as those for the original Paillier cryptosystem. Often proof the correctness of key generation during the key generation in order to convince of it to other parties. There are several researches for the modulus n, namely proving that the modulus is a square free Blum integer [13], the product of quasi-safe primes [14], or the product of safe primes [15], etc. In this case, the public key of the Paillier/E-Paillier cryptosystem is not only the modulus n but also the key g. We have to develop a proof system that the public key g is correctly generated, e.g., g is random in ZZ/N^2ZZ, or g is in the set $G_{E-Paillier}$. It is an open problem to investigate the relationship between the proof system and theorem 5.

In table 1, summarize the probability on the distribution for the public key g for different schemes described in this paper. The probabilities for the E-Paillier cryptosystem and the M-OU cryptosystem are negligible in the bit length of the public key.

Table 1: Comparison of the probability on the distribution for public key g

Method	***Probability On The Distribution For Public Key G***
Paillier	1 − 1/n overwhelming
M-Paillier	1/φ(n) Negligible
OU	1 − 1/p overwhelming
Enhanced 1 Paillier	1/φ(n) Negligible
Enhanced 2 Paillier	1/φ(n) Negligible
FO	$> 2^{-1}(1 - 2^{-k+1})$ ≈1/2
M-OU	1/φ(p) Negligible

6- The Running Time Comparision of the Proposed Methods

We programmed these algorithms by programming language Visual Basic 6 on P4 PC computer with CPU of 1.7 G.B and RAM of 256 M.B. Then we applied it on messages that has different size, where we takes plaintext of 1MB then encrypts it and computes the running time of its operation, then decrypts its and computes the running time of its operation. Then we take 2MB, 3MB, 4MB, and 5MB and computes the running time of the encryption and decryption of each messages. Figure (6) represents

the encryption times for our proposed methods compare with Pailler, Modified Pailler and Okamoto-Uchiyama. Figure (7) represents the decryption times for our proposed methods compare with Pailler, Modified Pailler and Okamoto-Uchiyama.

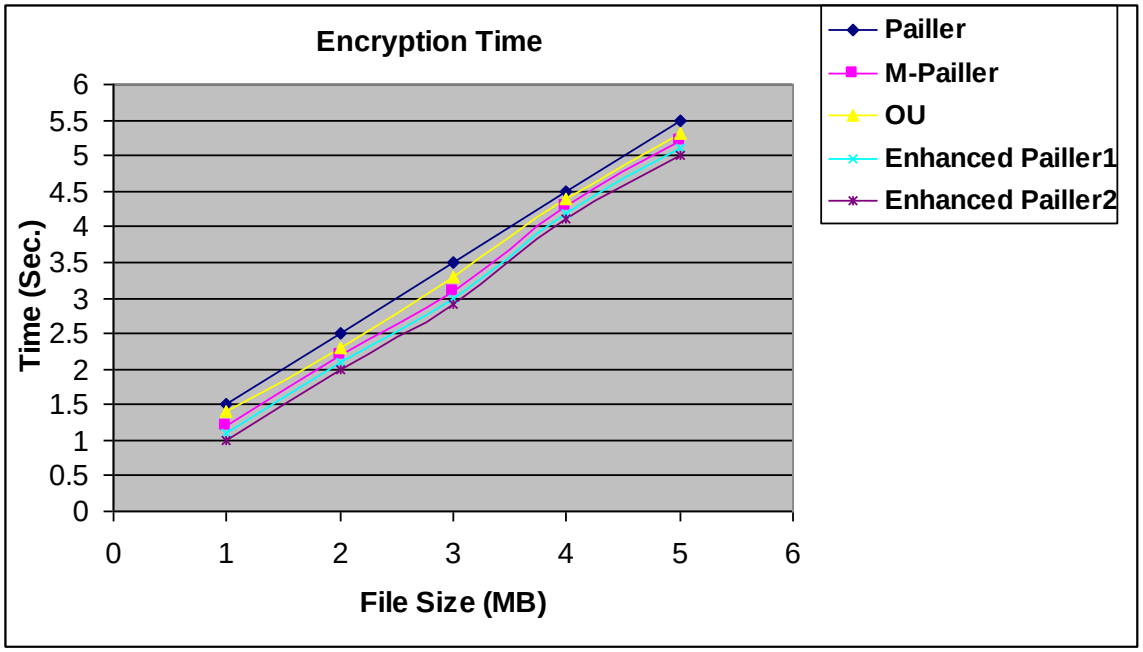

Figure 6: Encryption Time Curve for 2 Proposed Methods Compare with Pailler, Modified Pailler and Okamoto-Uchiyama

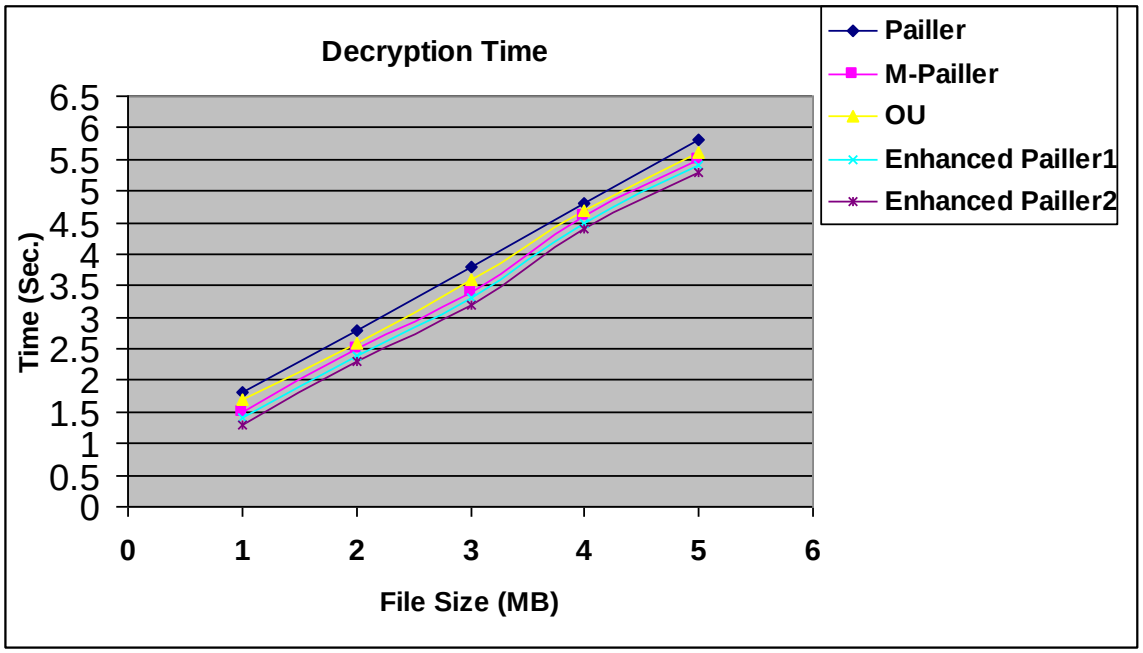

Figure 7: Decryption Time Curve for 2 Proposed Methods Compare with Pailler, Modified Pailler and Okamoto-Uchiyama

7- Conclusions

This paper presented two enhanced Paillier (E1 and E2 -Paillier) cryptosystem. The one-wayness of the E-Paillier cryptosystem is as intractable as factoring the modulus n, if the public key g can be generated only by the public information n. The oracle that can generate the public-key can factor the modulus n. Thus the public keys cannot be generated without knowing the factoring n, although the public key of the original Paillier cryptosystem can be generated from only the public modulus information. The proposed Enhanced Pailler (E1 and E2 – Paillier) has complexity time equal to the Modified Pailler algorithm and less than original Pailler. Also the running time of Enhanced Pailler (E1 and E2 – Paillier) are less than the original and Modified Pailler by less than 1 second. The M-Paillier uses the key g ϵ ZZ/n^2ZZ while the Okamoto-Uchiyama scheme, which uses the key g ϵ (ZZ/nZZ)^x such that $g^{p-1} = p + 1 \; mod \; p^2$. The two proposed enhanced Paillier use the key g ϵ ZZ/nZZ s.t. $g^{\lambda} = 1 + n \bmod n$.

References

[1] P. Paillier, "***Public-Key Cryptosystems Based On Composite Degree Residuosity Classes,***" Eurocrypt'99, LNCS 1592, pp.223-238, 1999.

[2] I. Damg°ard and M. Jurik, "***A Generalization, A Simplification And Some Applications Of Paillier's Probabilistic Public-Key System,*** " PKC 2001, LNCS 1992, pp.119-136, 2001.

[3] S. Galbraith, "***Elliptic Curve Paillier Schemes,***" to appear in Journal of Cryptology, 2001. (available from http://www.isg.rhul.ac.uk/~sdg/)

[4] D. Catalano, R. Gennaro, N. Howgrave-Graham, and P. Nguyen, "***Paillier's Cryptosystem Revisited,***" to appear in the ACM conference on Computer and Communication Security, 2001. (available from http://www.di.ens.fr/~pnguyen/)

[5] K. Sakurai and T. Takagi, "***New Semantically Secure Public-Key Cryptosystems From The RSA-Primitive,***" PKC 2002, LNCS 2274, pp.1-16, 2002.

[6] D. Galindo, S. Mart´ın, P. Morillo, and J. Villar, "***An Efficient Semantically Secure Elliptic Curve Cryptosystem Based On KMOV Scheme,***" Cryptology ePrint Archive, Report 2002/037, 2002. (available from http://eprint.iacr.org/)

[7] D. -H. Choi, S. Choi, and D. Won, "***Improvement Of Probabilistic Public Key Cryptosystem Using Discrete Logarithm,***" The 4th International Conference on Information Security and Cryptology, ICISC 2001, LNCS 2288, pp.72-80, 2002.

[8] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "***Relations Among Notions Of Security For Public-Key Encryption Schemes,***" CRYPTO'98, LNCS 1462, pp.26-45, 1998.

[9] E. Fujisaki and T. Okamoto, "***How To Enhance The Security Of Public-Key Encryption At Minimum Cost,***" 1999 International Workshop on Practice and Theory in Public Key Cryptography, LNCS 1560, pp.53-68, 1999.

[10] E. Fujisaki and T. Okamoto, "***Secure Integration Of Asymmetric And Symmetric Encryption Schemes,***" Advances in Cryptology – CRYPTO'99, LNCS 1666, pp.537-554, 1999.

[11] T. Okamoto and D. Pointcheval, "***REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform,***" In Proceedings of the Cryptographers' Track at RSA Conference '2001, LNCS 2020, pp.159-175, 2001.

[12] D. Pointcheval, "***Chosen-Ciphertext Security For Any One-Way Cryptosystem,***" 2000 International Workshop on Practice and Theory in Public Key Cryptography, LNCS 1751, pp.129-146, 2000.

[13] J. Boyar, K. Friedl, and C. Lund, "***Practical Zero-Knowledge Proofs: Giving Hits And Using Deficiencies,***" Journal of Cryptology, 4(3), pp.185-206, 1991.

[14] R. Gennaro, D. Micciancio, and T. Rabin, "***An Efficient Non-Interactive Statistical Zero-Knowledge Proof System For Quasi-Safe Prime Products***," ACM Conference on Computer and Communications Security, pp.67-72, 1998.

[15] J. Camenish and M. Michels, "***Proving That A Number Is The Product Of Two Safe Primes,***" Eurocrypt '99, LNCS 1592, pp.107-122, 1999.

[16] T. Okamoto and S. Uchiyama, "***A New Public-Key Cryptosystem As Secure As Factoring,***" Eurocrypt'98, LNCS 1403, pp.308-318, 1998.

[17] Kouichi Sakurai*and Tsuyoshi Takagi**, "***On The Security Of A Modified Paillier Public-Key Primitive***", Technical Report,Technische Universtat Darmstadt, Germany, 2002.