Technical Report TI–04/02, Technische Universtät Darmstadt, 22.04.2002.
URL: http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR/Welcome.html

On the Security of a Modified Paillier Public-Key Primitive

Kouichi Sakurai* Tsuyoshi Takagi**

∗ Kyushu University
Department of Computer Science and Communication Engineering
Hakozaki, Fukuoka 812-81, Japan
sakurai@csce.kyushu-u.ac.jp

∗∗ Technische Universtät Darmstadt
Fachbereich Informatik
Alexanderstr. 10, D-64283 Darmstadt, Germany
ttakagi@cdc.informatik.tu-darmstadt.de

Abstract

Choi et al. proposed the modified Paillier cryptosystem (M-Paillier cryptosystem). They use a special public-key $g \in \mathbb{Z}/n\mathbb{Z}$ such that $g^{\varphi(n)} = 1 + n \bmod n^2$, where n is the RSA modulus. The distribution of the public key g is different from that of the original one. In this paper, we study the security of the usage of the public key. Firstly, we prove that the one-wayness of the M-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, we 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. Thirdly, we propose a chosen ciphertext attack against the M-Paillier cryptosystem. Our attack can factor the modulus n by only one query to the decryption oracle. This type of total breaking attack has not been reported for the original Paillier cryptosystem. Finally, we discuss the relationship between the M-Paillier cryptosystem and the Okamoto-Uchiyama scheme.

Keywords: One-wayness, Factoring, Chosen ciphertext attack, Key distribution, Composite residuosity problem, Paillier cryptosystem.

1 Introduction

Paillier proposed a probabilistic encryption scheme [Pai99]. The Paillier cryptosystem encrypts a message m by $E(m,r) = g^m h^n \bmod n^2$, where g, n is the public key and h is a random integer. The encryption function $E(m,r)$ has a homomorphic property: $E(m_1,r_1)E(m_2,r_2) = E(m_1+m_2, r_1r_2)$. Therefore, the Paillier cryptosystem has several attractive applications, for example, voting systems, threshold schemes, etc.

The security of the Paillier cryptosystem has been investigated [Pai99]. Its one-wayness is as intractable as breaking the computational composite residuosity problem (C-CRP). Its semantic security (IND-CPA) is as hard as breaking the decisional composite residuosity problem (D-CRP) in the standard model. Paillier and Pointcheval proposed a conversion technique to be semantically secure against the adaptive chosen ciphertext attack (IND-CCA2) in the random oracle model [PP99]. Catalano et al. proved that $n - b$ least significant bits of the message are simultaneously secure under the difficulty 2^b-hard C-CRP [CGH01].

The Paillier cryptosystem have been extended to various schemes. Damgård and Jurik proposed a scheme with moduli $n^i (i > 2)$ that is useful for voting systems [DJ01]. Galbraith extended the Paillier cryptosystem to a scheme over elliptic curves [Gal01]. Catalano et al. proposed an efficient variant scheme that encrypts a message by $r^e(1+mn) \bmod n^2$, where e, n is the RSA public key and r is random integer in $(\mathbb{Z}/n\mathbb{Z})^\times$ [CGHN01]. 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 [ST02]. Galindo et al. constructed their scheme over elliptic curves [GMMV02].

The decryption algorithm of the Paillier cryptosystem involves a modular inversion $L(g^\lambda)^{-1} \bmod n$, where $n = pq$ and $\lambda = \mathrm{lcm}(p-1, q-1)$. Choi et al. proposed how to eliminate the inverse by modifying the generation of the key g [CCW01]. They use a special public-key g that satisfies $g^\lambda = 1 + n \bmod n^2$. 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. We call their scheme as the modified Paillier cryptosystem (M-Paillier cryptosystem).

Contribution of this paper

In this paper, we investigate the security of the M-Paillier cryptosystem. Let $G_{\textit{M-Paillier}}$ be the set of all keys g for the M-Paillier cryptosystem. The density of the set $G_{\textit{M-Paillier}}$ is n, and the probability that a random $g \in (\mathbb{Z}/n^2\mathbb{Z})^\times$ is contained in the set $G_{\textit{M-Paillier}}$ is at most $1/\varphi(n)$, which is negligible in the bit-length of the public modulus n. Firstly, we prove that the one-wayness of the M-Paillier cryptosystem is as intractable as factoring the modulus n if the public key g can be generated only by the public modulus n, i.e., g is samplable from $\mathbb{Z}/n^2\mathbb{Z}$ in the polynomial time of $\log n$. The semantic security of the M-Paillier cryptosystem is as hard as breaking the decisional composite residuosity problem for the key distribution $G_{\textit{M-Paillier}}$. Secondly, we 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. Thirdly, we propose a chosen ciphertext attack against the M-Paillier cryptosystem. Our attack can factor the modulus n by only one query to the decryption oracle. This type of total breaking attack has not been reported for the original Paillier cryptosystem. Finally, we discuss the relationship between the M-Paillier cryptosystem and the Okamoto-Uchiyama scheme, regarding the distribution of the public key g.

The proposed chosen ciphertext attack is similar to that for the Rabin cryptosystem [Rab79]. The public key of the Rabin cryptosystem is only the modulus n, however for the M-Paillier cryptosystem not only the modulus n but also the key g compose the public key pair. If we can generate the public key g only by the public modulus n, the one-wayness of the M-Paillier cryptosystem can be proved as intractable as factoring n, like in the case of the Rabin cryptosystem. However, we prove that the public key g can not be generated without factoring n. There is a gap between the one-wayness of the M-Paillier and factoring. The Okamoto-Uchiyama scheme uses a similar public key, which is not only the modulus n but also a key $g \in \mathbb{Z}/n\mathbb{Z}$ such that the order of g in $\mathbb{Z}/p^2\mathbb{Z}$ is divisible by p [OU98]. The Okamoto-Uchiyama scheme can be proved as intractable as factoring n. Although the public key g is used, we can generate the public key g of the Okamoto-Uchiyama scheme from only the public modulus n in the polynomial time of $\log n$. It is an open problem to consider the security of the Okamoto-Uchiyama for the special public key g, e.g., $g^{p-1} = 1 + p \bmod p^2$ proposed by [CCW01].

Notation. In this paper we choose $\{0, 1, 2, .., m-1\}$ as the residue class of modulo m, namely the elements of $\mathbb{Z}/m\mathbb{Z}$ are $\{0, 1, 2, .., m-1\}$. We denote by $(\mathbb{Z}/m\mathbb{Z})^\times$ the reduced residue class of modulo m such that $\{a \in \mathbb{Z}/m\mathbb{Z} | \gcd(a, m) = 1\}$. The notation $ord_m(r)$ means the order of element r in $(\mathbb{Z}/m\mathbb{Z})^\times$, in the other words, the smallest positive integer x such that $r^x = 1 \bmod m$.

2 Paillier Cryptosystem

We review the Paillier cryptosystem [Pai99] in this section.

The public key of the Paillier cryptosystem is the RSA modulus n and an element $g \in (\mathbb{Z}/n^2\mathbb{Z})^\times$ whose order is divisible by n. The secret key is $\lambda = \text{lcm}\ (p-1, q-1)$, where p, q are the primes of $n = pq$. A message $m \in \{0, 1, ..., n-1\}$ is encrypted by $c = g^m h^n \bmod n^2$ for a random integer $h \in \mathbb{Z}/n\mathbb{Z}$. Therefore the

Key Generation
$n = pq$, the RSA modulus $\lambda = \text{lcm}\ (p-1, q-1)$ $g \in \mathbb{Z}/n^2\mathbb{Z}$ s.t. $n \mid ord_{n^2}(g)$ Public-key: (n, g), Secret key: λ
Encryption of m
$m \in \{0, 1, ..., n-1\}$, a message $h \in_R \mathbb{Z}/n\mathbb{Z}$ $c = g^m h^n \bmod n^2$, a ciphertext
Decryption of c
$m = L(c^\lambda \bmod n^2) L(g^\lambda \bmod n^2)^{-1} \bmod n$

Figure 1: Paillier Cryptosystem

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

The key g is the element of $(\mathbb{Z}/n^2\mathbb{Z})^\times$ s.t. $n \mid ord_{n^2}(g)$. In the group $(\mathbb{Z}/n^2\mathbb{Z})^\times$, there are $(n-1)\varphi(n)$ elements whose order is divisible by n. The order of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is $n\varphi(n)$. 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 we can use a random g of $\mathbb{Z}/n^2\mathbb{Z}$ as the public key.

2.1 Security of the Paillier Cryptosystem

In order to discuss the security of the Paillier cryptosystem, we define the following number theoretic problems. Denote by $RSA_{modulus}$ 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 $(\mathbb{Z}/n^2\mathbb{Z})^\times$. The n-th residuosity class of c with respect to $g \in G_{Paillier}$ is the unique integer x which satisfies $c = g^x h^n \bmod n^2$ for an integer $h \in \mathbb{Z}/n\mathbb{Z}$. 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 $c \in (\mathbb{Z}/n^2\mathbb{Z})^\times$, $g \in G_{Paillier}$, and $n \in RSA_{modulus}$. The decisional composite residuosity problem (D-CRP) is to decide whether $x = [[c]]_g$ holds for given $x \in \mathbb{Z}/n\mathbb{Z}$, $c \in (\mathbb{Z}/n^2\mathbb{Z})^\times$, $g \in G_{Paillier}$, and $n \in RSA_{modulus}$. 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 $n \in RSA_{modulus}$, $g \in G_{Paillier}$, $h \in \mathbb{Z}/n\mathbb{Z}$, 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

$$\begin{aligned} Pr_{m \in_R \mathbb{Z}/n\mathbb{Z}}[n \leftarrow RSA_{modulus}, h \leftarrow_R \mathbb{Z}/n\mathbb{Z},& \\ g \leftarrow G_{Paillier}, c = g^m h^n \bmod n^2 : A^{OW}_{Paillier}(c) = m]& \end{aligned}$$

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) [Pai99].

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 ciphertext of either m_0 or m_1. The $A^{SS1}_{Paillier}$ guesses whether the ciphertext c is the encryption of $m_b (b \in \{0,1\})$ 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

$$\begin{aligned} 2Pr\ \ [n \leftarrow RSA_{modulus}, (m_0, m_1, st) \leftarrow A^{SS1}_{Paillier}(e, n), b \leftarrow \{0,1\}, h \leftarrow_R \mathbb{Z}/n\mathbb{Z},& \\ g \leftarrow_R G_{Paillier}, c = g^m h^n \bmod n^2 : A^{SS2}_{Paillier}(c, m_0, m_1, st) = b] - 1& \end{aligned}$$

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) [Pai99]. 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 ciphertext attack. A public cryptosystem that is semantically secure against the chosen ciphertext attack is called an IND-CCA2 scheme [BDPR98]. The IND-CCA2 security has become one of the criteria for a general purpose public-key cryptosystem.

3 The Modified Paillier Cryptosystem

We review the modified Paillier cryptosystem [CCW01], which we call the M-Paillier cryptosystem in the following.

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

$$G_{M\text{-}Paillier} = \{g \in (\mathbb{Z}/n^2\mathbb{Z})^\times \ \ s.t.\ \ g^\lambda = 1 + n \bmod n^2\}. \tag{1}$$

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

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

Key Generation
$n = pq$, the RSA modulus
$\lambda = \mathrm{lcm}\ (p-1, q-1)$
$g \in \mathbb{Z}/n^2\mathbb{Z}$ s.t. $g^\lambda = 1 + n \bmod n^2$
Public-key: (n, g), Secret key: λ

Encryption of m
$m \in \{0, 1, ..., n-1\}$, a message
$h \in_R \mathbb{Z}/n\mathbb{Z}$
$c = g^m h^n \bmod n^2$, a ciphertext

Decryption of c
$m = L(c^\lambda \bmod n^2)$

Figure 2: The Modified Paillier Cryptosystem

process for any $g \in S_{M\text{-}Paillier}$. The encryption and the decryption of the M-Paillier cryptosystem is as follows:

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

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

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

The density of the $G_{M\text{-}Paillier}$ is at most n. The probability that a random element of $(\mathbb{Z}/n^2\mathbb{Z})^\times$ is contained in the $G_{M\text{-}Paillier}$ is at most $1/\varphi(n)$, which is negligible in the bit-length of the public key n. This is an important observation for the security of the M-Paillier cryptosystem and we state it in the following lemma.

1. Lemma *The probability that a random $g \in (\mathbb{Z}/n^2\mathbb{Z})^\times$ is contained in the set $G_{M\text{-}Paillier}$ is at most $1/\varphi(n)$.*

We have the other description of the $G_{M\text{-}Paillier}$. Because of $g^\lambda = 1 + n \bmod n^2$, we have the following relations $[[1+n]]_g = \lambda \bmod n$ and $[[g]]_{1+n} = \lambda^{-1} \bmod n$. Therefore, the element $g \in G_{M\text{-}Paillier}$ can be represented as

$$\{g \in (\mathbb{Z}/n^2\mathbb{Z})^\times | [[g]]_{1+n} = \lambda^{-1} \bmod n\}. \tag{3}$$

The n-th residuosity class of the key g with respect to $1+n$ is $\lambda^{-1} \bmod n$.

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

$$\begin{aligned} Pr_{m \in_R \mathbb{Z}/n\mathbb{Z}}[&n \leftarrow RSA_{modulus}, h \leftarrow_R \mathbb{Z}/n\mathbb{Z}, \\ &g \leftarrow G_{M\text{-}Paillier}, c = g^m h^n \bmod n^2 : A^{OW}_{M\text{-}Paillier}(c) = m] \end{aligned}$$

is negligible in $\log n$. The semantic security of the M-Paillier cryptosystem is that for any probabilistic polynomial time algorithm $A^{SS}_{M\text{-}Paillier}$ the probability

$$2Pr\ \ [n \leftarrow RSA_{modulus}, (m_0, m_1, st) \leftarrow A^{SS1}_{M\text{-}Paillier}(e, n), b \leftarrow \{0,1\}, h \leftarrow_R \mathbb{Z}/n\mathbb{Z}, \\ g \leftarrow_R G_{M\text{-}Paillier}, c = g^m h^n \bmod n^2 : A^{SS2}_{M\text{-}Paillier}(c, m_0, m_1, st) = b] - 1$$

is negligible in $\log n$. The distribution of the public key $g \in G_{M\text{-}Paillier}$ in the security assumption is different from that of the original one. The author asserted that the one-wayness or semantic security is as intractable as the C-CRP or D-CRP, respectively [CCW01]. However, there is no proof for their statements. We will investigate the security of the M-Paillier cryptosystem in the following.

4 Security of the M-Paillier Cryptosystem

We will redefine the number theoretic problems related to the M-Paillier cryptosystem. The only difference between the Paillier cryptosystem and the M-Paillier cryptosystem is the distribution of the public key g. We discuss the C-CRP and D-CRP for the public key g from the M-Paillier cryptosystem. We can prove that the one-wayness of the M-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 $\mathbb{Z}/n^2\mathbb{Z}$ in the polynomial time of $\log n$.

The computational composite residuosity problem for the $G_{M\text{-}Paillier}$ is to compute the $[[c]]_g$ for given $c \in (\mathbb{Z}/n^2\mathbb{Z})^\times$, $g \in G_{M\text{-}Paillier}$, and $n \in RSA_{modulus}$. Then we can prove the following theorem.

2. Theorem *Breaking the C-CRP for the $G_{M\text{-}Paillier}$ 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. We prove the different direction. Let A be the algorithm, which solves the C-CRP for the $G_{M\text{-}Paillier}$ in time t and with advantage ε. The algorithm A can compute the $[[c]]_g$ for given $c \in (\mathbb{Z}/n^2\mathbb{Z})^\times$, $g \in G_{M\text{-}Paillier}$, and $n \in RSA_{modulus}$. Note that if the key g is generated only by public key information, there is no information leakage about the secret keys from the $G_{M\text{-}Paillier}$. Here, let $c = (1 + rn)h^n \bmod n^2$ for random integers $r \in \mathbb{Z}/n\mathbb{Z}$ and $h \in (\mathbb{Z}/n\mathbb{Z})^\times$, then the integer c is uniformly distributed in the ring $(\mathbb{Z}/n^2\mathbb{Z})^\times$. The distribution of c is equivalent to that of instances to C-CRP. Note that $L(c^\lambda \bmod n^2) = r\lambda \bmod n$ holds for the decryption of the M-Paillier cryptosystem, where the λ is the secret key. Thus the algorithm A outputs $t = r\lambda \bmod n$ for inputs c and the secret key λ is recovered by $\lambda = tr^{-1} \bmod n$. 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 $t + \mathcal{O}((\log n)^2)$ and ε, respectively. ■

We can mount this result to the one-wayness of the M-Paillier cryptosystem.

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

Proof: We prove that breaking the one-wayness of the M-Paillier cryptosystem is as hard as breaking the D-CRP for the $G_{\textit{M-Paillier}}$. 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 [FO99a], [FO99b], [OP01b], [Poi00]. The conversion techniques [FO99b], [Poi00] can convert a one-way public-key scheme to be an IND-CCA2 scheme. Therefore the M-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 M-Paillier cryptosystem is also different from the original D-CRP. We have to redefine the D-CRP. The decisional composite residuosity problem (D-CRP) for the $G_{\textit{M-Paillier}}$ is to decide whether $x = [[c]]_g$ holds for given $x \in \mathbb{Z}/n\mathbb{Z}$, $c \in (\mathbb{Z}/n^2\mathbb{Z})^\times$, $g \in G_{\textit{-Paillier}}$, and $n \in RSA_{modulus}$. Then we can prove that the semantic security of the M-Paillier cryptosystem is as hard as breaking the D-CRP for the $G_{\textit{M-Paillier}}$. We state that as a theorem:

4. Theorem *The semantic security of the M-Paillier cryptosystem is as hard as breaking the decisional composite residuosity problem for the $G_{\textit{M-Paillier}}$.*

If an algorithm A breaks the original D-CRP, then the D-CRP for the $G_{\textit{M-Paillier}}$ 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 we 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 $g \in \mathbb{Z}/n^2\mathbb{Z}$ 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 M-Paillier cryptosystem can factor the RSA modulus. We cannot generate the key g for the M-Paillier without factoring n.

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

5. Theorem *The RSA modulus n can be factored using the oracle $\mathcal{O}_n$.*

Proof: We will construct an algorithm A, which computes λ using the oracle $\mathcal{O}_n$. 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 $\mathbb{Z}/n\mathbb{Z}$, runs $\mathcal{O}_n(a_1)$ and obtains b_1 such that $g_1 = a_1 + b_1 n \in G_{M\text{-}Paillier}$.
2. A generates a random a_2 in $\mathbb{Z}/n\mathbb{Z}$, runs $\mathcal{O}_n(a_2)$ and obtains b_2 such that $g_2 = a_2 + b_2 n \in G_{M\text{-}Paillier}$.
3. A computes $a_3 = a_1 a_2 \bmod n$, runs $\mathcal{O}_n(a_3)$ and obtains b_3 such that $g_3 = a_3 + b_3 n \in G_{M\text{-}Paillier}$.
4. Output $\lambda = (a_1^{-1}b_1 + a_2^{-1}b_2 - (a_1a_2)^{-1}b_3)^{-1} \bmod n$.

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 $L(a_1^\lambda) + L(a_2^\lambda) + \lambda(a_1a_2)^{-1}b_3 = 1 \bmod n$ in step 3. Thus we obtain the following equation:

$$\lambda a_1^{-1}b_1 + \lambda a_2^{-1}b_2 - \lambda(a_1a_2)^{-1}b_3 = 1 \bmod n. \tag{4}$$

If we 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 M-Paillier cryptosystem is essentially different from that for the original Paillier cryptosystem. The C-CRP/D-CRP for the $G_{M\text{-}Paillier}$ differs from the original C-CPR/D-CRP. Thus the one-wayness or semantic security for the M-Paillier cryptosystem are generally not same as those for the original Paillier cryptosystem.

We 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 [BFL91], the product of quasi-safe primes [GMR98], or the product of safe primes [CM99], etc. In this case, the public key of the Paillier/M-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 $\mathbb{Z}/n^2\mathbb{Z}$, or g is in the set $G_{M\text{-}Paillier}$. It is an open problem to investigate the relationship between the proof system and theorem 5.

6 Chosen Ciphertext Attack

We describe the chosen ciphertext attack against the M-Paillier cryptosystem. An attacker is allowed to ask queries to the decryption oracle. The proposed chosen ciphertext attack against the M-Paillier cryptosystem factors the modulus n. If we use the technique used in section 4, the chosen ciphertext attack can be constructed. In the real attack we do not have to generate a ciphertext, which is randomly distributed in $(\mathbb{Z}/n^2\mathbb{Z})^\times$ and therefore the attack is easier.

Our chosen ciphertext attack works as follows: At first we change the public key g to $g+n$, and we encrypt a message m and the public key $g+n$ using a random $h \in \mathbb{Z}/n\mathbb{Z}$. The decryption oracle decrypts the ciphertext based on the secret key λ, which computes $L((g+n)^\lambda \bmod n^2)$. Then the attacker can recover the secret key λ based on the answer $L((g+n)^\lambda \bmod n^2)$ from the decryption oracle. Thus the modulus n is factored. We summarize the chosen ciphertext attack as follows:

- Generation of a ciphertext:
  1. Choose a random integer $h \in \mathbb{Z}/n\mathbb{Z}$.
  2. Change the public key g to $g+n$.
  3. Compute $c = (g+n)^m h^n \bmod n^2$.
  4. Return the ciphertext c of the message m.
- Decryption oracle:
  1. Return $m' = L(c^\lambda)$.
- Factorization of n:
  1. Compute $\lambda = g(m'm^{-1} - 1) \bmod n$.
  2. Factor n using the λ.

We can prove the correctness of the chosen ciphertext. We have the following theorem.

6. Theorem *The above chosen ciphertext attack factors the modulus n.*

Proof: Let $g = a + bn \in G_{M\text{-}Paillier}$, then we have the following relationships:

$$\begin{aligned}(g+n)^\lambda &= g^\lambda + \lambda g^{\lambda-1} n \bmod n^2\\ &= (a+bn)^\lambda + \lambda g^{\lambda-1} n \bmod n^2\\ &= 1 + (L(a^\lambda) + \lambda a^{-1} b + \lambda a^{-1}) n \bmod n^2\\ &= 1 + (1 + \lambda a^{-1}) n \bmod n^2.\end{aligned}$$

Here the decryption oracle decrypts the ciphertext c as follows: $c^\lambda = ((g+n)^\lambda)^m h^{\lambda n} \bmod n^2 = 1 + (1+\lambda a^{-1})mn$, and $L(c^\lambda) = (1+\lambda a^{-1})m$. We thus obtain the message $m' = (1+\lambda a^{-1})m$ from the decryption oracle. The λ can be recovered by $\lambda = a(m'm^{-1} - 1) \bmod n = g(m'm^{-1} - 1) \bmod n$. ■

The chosen ciphertext attack against the M-Paillier cryptosystem is effective because the public key is chosen from a special distribution $G_{M\text{-}Paillier}$. The attacker knows that the key g satisfies the condition $g^\lambda = 1+n \bmod n^2$. On the contrary, the public key g from the original Paillier cryptosystem does not satisfy such a condition, but it satisfies $g^\lambda = 1 + rn \bmod n^2$ for an unknown random integer $r \in \mathbb{Z}/n\mathbb{Z}$. Attackers have to guess the random integer r in addition with the secret key λ. The chosen ciphertext attack does not work for the original Paillier cryptosystem. There is a security gap in the M-Paillier scheme and the original Paillier scheme.

The above chosen ciphertext attack aims at the cryptographic primitive of the M-Paillier cryptosystem. As we discussed in section 5, we can enhance a cryptographic primitive of a public-key cryptosystem to be semantically secure against the chosen ciphertext attack [FO99a], [FO99b], [OP01b], [Poi00]. Especially, Paillier and Pointcheval proposed a conversion technique, which makes the Paillier public-key primitive to be an IND-CCA2 scheme [PP99]. If we use these techniques, we can make the M-Paillier cryptosystem secure against the chosen ciphertext. However, the M-Paillier cryptosystem is used as a cryptographic primitive without the conversions for security protocols, and we should take care of its security.

7 Okamoto-Uchiyama Scheme

In this section we discuss the relationship between the Okamoto-Uchiyama scheme [OU98] and the M-Paillier cryptosystem. We call the Okamoto-Uchiyama scheme as the OU scheme in the following. The OU scheme is constructed over the ring $\mathbb{Z}/n\mathbb{Z}$, where $n = p^2 q$ 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 [OU98].

The public key of the OU scheme is the modulus n and an element $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ whose order in the subgroup $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is divisible by p. If we choose a random g from $(\mathbb{Z}/n\mathbb{Z})^\times$, the probability that the order of g in $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is divisible by p is $1 - 1/p$. The secret key is the primes p and $g_p = g^{p-1} \bmod p^2$. A message $m \in \{0, 1, ..., 2^{k-2}\}$ is encrypted by $c = g^{m+rn} \bmod n$ for a random integer $r \in \mathbb{Z}/n\mathbb{Z}$, where k is the bit-length of p. The ciphertext c is decrypted by $m = L(c^{p-1} \bmod p^2)L(g^{p-1} \bmod p^2)^{-1} \bmod n$ using the secret key p, where $L(a \bmod n^2) = (a-1)/n$ for an integer a such that $a = 1 \bmod n$.

Key Generation
k, the bit length of prime p
$n = p^2q$, the modulus
$g \in \mathbb{Z}/n\mathbb{Z}$ s.t. $p \| ord_{p^2}(g)$
$g_p = g \bmod p^2$
Public-key: (n, g, k), Secret key: p, g_p

Encryption of m
$m \in \{0, 1, ..., 2^{k-2}\}$, a message
$r \in \mathbb{Z}/n\mathbb{Z}$, a random integer
$c = g^{m+rn} \bmod n$, a ciphertext

Decryption of c
$m = L(c^{p-1} \bmod p^2)L(g_p^{p-1} \bmod p^2)^{-1} \bmod p$

Figure 3: Okamoto-Uchiyama Cryptosystem

Fujisaki and Okamoto enhanced the security of the OU scheme using the random oracle model [FO99a]. We 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 $(\mathbb{Z}/n\mathbb{Z})^\times$ whose order in the group $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is $p(p-1)$. The probability that the order of g in $(\mathbb{Z}/p^2\mathbb{Z})^\times$ 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 a modified version of the Okamoto-Uchiyama scheme [CCW01]. We call it the modified OU (M-OU) scheme in the following. The M-OU scheme uses a key contained in the following the set

$$G_{M\text{-}OU} = \{g \in (\mathbb{Z}/n^2\mathbb{Z})^\times \ \ s.t.\ \ g^{p-1} = 1 + p \bmod p^2\}. \tag{5}$$

There are at most p elements which satisfy $a^{p-1} = 1 + p \bmod p^2$ for $a \in (\mathbb{Z}/p^2\mathbb{Z})^\times$. Then the probability that a random g from $(\mathbb{Z}/n\mathbb{Z})^\times$ is contained in the set of keys is at most $1/\varphi(p)$, 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 $g \in G_{M\text{-}OU}$.

In table 1, we summarize the probability on the distribution for the public key g for different schemes described in this paper. The probabilities for the M-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

Paillier[Pai99]	M-Paillier[CCW01]		OU[OU98]	FO[FO99a]	M-OU[CCW01]
$1 - 1/n$ overwhelming	$\boldsymbol{1/\varphi(n)}$ **negligible**		$1 - 1/p$ overwhelming	$> 2^{-1}(1 - 2^{-k+1})$ $\approx 1/2$	$\boldsymbol{1/\varphi(p)}$ **negligible**

8 Conclusion

We analyzed the modified Paillier (M-Paillier) cryptosystem proposed by Choi et al [CCW01]. Firstly, we proved the one-wayness of the M-Paillier cryptosystem is as intractable as factoring the modulus n, if the public key g can be generated only by the public information n. Secondly, we proved that 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. Thirdly, we proposed a chosen ciphertext attack against the M-Paillier cryptosystem. Our attack can factor the modulus n by only one query to the decryption oracle. This type of total breaking attack has not been reported for the original Paillier cryptosystem. Finally, we discussed the relationship between the M-Paillier cryptosystem and the Okamoto-Uchiyama scheme.

The Paillier cryptosystem has been extended to the schemes over elliptic curves [Gal01] or other types of modulus [DJ01]. It is an interesting open problem to enhance the results in this paper to these schemes. Coi et al. also proposed a modification of the Okamoto-Uchiyama scheme, which uses the key $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $g^{p-1} = p + 1 \bmod p^2$ [CCW01]. It is also an open problem to investigate the security of the modified Okamoto-Uchiyama scheme.

References

[BDPR98] 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.

[BFL91] 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.

[CM99] J. Camenish and M. Michels, "Proving that a number is the product of two safe primes," Eurocrypt '99, LNCS 1592, pp.107-122, 1999.

[CGH01] D. Catalano, R. Gennaro, and N. Howgraw-Graham, “The bit security of Paillier’s encryption scheme and its applications,” Eurocrypt 2001, LNCS 2045, pp.229-243, 2001.

[CGHN01] 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/`)

[CCW01] 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.

[DJ01] I. Damgård 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.

[FO99a] 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.

[FO99b] E. Fujisaki and T. Okamoto, “Secure integration of asymmetric and symmetric encryption schemes,” Advances in Cryptology – CRYPTO’99, LNCS 1666, pp.537-554, 1999.

[Gal01] S. Galbraith, “Elliptic curve Paillier schemes,” to appear in Journal of Cryptology, 2001. (available from `http://www.isg.rhul.ac.uk/~sdg/`)

[GMMV02] D. Galindo, S. Martín, 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/`)

[GMR98] 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.

[OP01a] T. Okamoto and D. Pointcheval, “The Gap-Problems: a new class of problems fro the security of cryptographic schemes,” 2001 International Workshop on Practice and Theory in Public Key Cryptography, LNCS 1992, pp.104-118, 2001.

[OP01b] 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.

[OU98] T. Okamoto and S. Uchiyama, “A new public-key cryptosystem as secure as factoring,” Eurocrypt’98, LNCS 1403, pp.308-318, 1998.

[Pai99] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” Eurocrypt’99, LNCS 1592, pp.223-238, 1999.

[PP99] P. Paillier and D. Pointcheval, “Efficient public key cryptosystems provably secure against active adversaries,” Asiacrypt’99, LNCS 1716, pp.165-179, 1999.

[Poi00] 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.

[Rab79] M. Rabin, “Digitalized signatures and public-key functions as intractable as factorization”, Technical Report No.212, MIT, Laboratory of Computer Science, Cambridge, pp.1-16, 1979.

[ST02] K. Sakurai and T. Takagi, “New semantically secure public-key cryptosystems from the RSA-primitive,” PKC 2002, LNCS 2274, pp.1-16, 2002.