Some RSA-based Encryption Schemes with Tight Security Reduction

Kaoru Kurosawa[1] and Tsuyoshi Takagi[2]

[1] Ibaraki University,
4-12-1 Nakanarusawa, Hitachi, Ibaraki, 316-8511, Japan
kurosawa@cis.ibaraki.ac.jp
[2] Technische Universität Darmstadt, Fachbereich Informatik,
Alexanderstr.10, D-64283 Darmstadt, Germany
ttakagi@cdc.informatik.tu-darmstadt.de

Abstract. In this paper, we study some RSA-based semantically secure encryption schemes (IND-CPA) in the standard model. We first derive the exactly tight one-wayness of Rabin-Paillier encryption scheme which assumes that factoring Blum integers is hard. We next propose the first IND-CPA scheme whose one-wayness is equivalent to factoring *general* $n = pq$ (not factoring Blum integers). Our reductions of one-wayness are very tight because they require only one decryption-oracle query.

Keywords: Factoring, semantic security, tight reduction, RSA-Paillier, Rabin-Paillier.

1 Introduction

1.1 Background

An encryption scheme should have strong one-wayness as well as high semantic security. Therefore, it is desirable to construct a semantically secure encryption scheme whose one-wayness is equivalent to factoring $n = pq$ in the *standard* model. (There are several provably secure constructions in the *random oracle* model. For example, see [Sho01,FOPS01,Bon01].)

RSA-Paillier encryption scheme is semantically secure against chosen plaintext attacks (IND-CPA) in the standard model under the RSA-Paillier assumption [CGHN01]. The assumption claims that

$$SMALL_{RSAP} = \{r^e \bmod n^2 | r \in Z_n\} \text{ and } LARGE_{RSAP} = \{r^e \bmod n^2 | r \in Z_{n^2}\}$$

are indistinguishable, where (n, e) is the public-key of RSA. Further, it is one-way if breaking RSA is hard. The latter problem was first raised by [ST02] and finally proved by [CNS02] using LLL algorithm of lattice theory.

On the other hand, $n(= pq)$ is called a Blum integer if $p = q = 3 \bmod 4$. Galindo et al. recently considered Rabin-Paillier encryption scheme and showed that it is one-way if factoring Blum integers is hard [GMMV03].

However, there is a large gap between the one-wayness which they proved and the difficulty of factoring. That is, suppose that the one-wayness is broken with probability ε. Then what Galindo et al. proved is that Blum integers can be factored with probability ε^2. Further the factoring problem is restricted to *Blum* integers, but not *general* p, q.

(The one-wayness of Okamoto-Uchiyama scheme [OU98] is equivalent to factoring $n = p^2q$, but not $n = pq$.)

1.2 Our Contribution

In this paper, we study the tight one-wayness of some RSA-based semantically secure encryption schemes (IND-CPA) in the standard model, where the one-wayness must be equivalent to factoring $n = pq$.

We first show that Rabin-Paillier encryption scheme has no gap between the *real* one-wayness and the difficulty of factoring Blum integers. (In other words, we give a factoring algorithm with success probability ε.) Our proof technique is quite different from previous proofs. In particular:

- Our proof technique requires only *one* decryption-oracle query while the previous proofs for RSA/Rabin-Paillier encryption schemes require *two* oracle queries [CNS02,GMMV03].
- No LLL algorithm is required, which was essentially used in the previous proofs for RSA/Rabin-Paillier schemes [CNS02,GMMV03].

We next propose the first IND-CPA scheme such that the one-wayness is equivalent to factoring *general* $n = pq$ (not factoring *Blum* integers). The one-wayness is proved by applying our proof technique as mentioned above. Therefore, our security reduction of one-wayness is very tight. That is, there is almost no gap between the one-wayness and the hardness of the general factoring problem.

The proposed scheme is obtained from an encryption scheme presented by Kurosawa et al. [KIT88,KOMM01]. The semantic security holds under a natural extension of RSA-Paillier assumption. That is, it is semantically secure (IND-CPA) if two distributions $SMALL_{RSAK}$ and $LARGE_{RSAK}$ are indistinguishable, where we define $SMALL_{RSAK}$ and $LARGE_{RSAK}$ as appropriate subsets of $SMALL_{RSAP}$ and $LARGE_{RSAP}$, respectively. We also show a close relationship between our assumption and RSA-Paillier assumption.

This paper is organized as follows: In Section 2, we describe notions required for the security description in this paper. In Section 3, the exact security reduction algorithm for Rabin-Paillier encryption scheme is presented. In Section 4, the proposed scheme is presented. In Section 5, we prove that the one-wayness of the proposed scheme is as hard as general factoring problem. In Section 6, we discuss the semantic security of the proposed scheme. Sec.7 includes some final comments.

Related works: Cramer and Shoup showed an semantically secure encryption scheme against chosen ciphertext attacks (IND-CCA) under the decision Diffie-Hellamn assumption [CS98]. They recently showed a general framework to construct IND-CCA schemes [CS02].

It will be a further work to develop an IND-CCA scheme whose one-wayness is equivalent to the factoring problem in the standard model. We hope that our results provide us a good starting point to this challenging problem.

2 Security of Encryption Schemes

PPT will denote a "probabilistic polynomial time".

2.1 Encryption Scheme

A public-key encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of three algorithms. The key generation algorithm $\mathcal{K}$ outputs (pk, sk) on input 1^l, where pk is a public key, sk is the secret key and l is a security parameter. We write $(pk, sk) \stackrel{R}{\leftarrow} \mathcal{K}$. The encryption algorithm $\mathcal{E}$ outputs a ciphertext c on input the public key pk and a plaintext (message) m; we write $c \stackrel{R}{\leftarrow} \mathcal{E}_{pk}(m)$. The decryption algorithm $\mathcal{D}$ outputs m or *reject* on input the secret key sk and a ciphertext c; we write $x \leftarrow \mathcal{D}_{sk}(c)$, where $x = m$ or *reject*. We require that $\mathcal{D}_{sk}(\mathcal{E}_{pk}(m)) = m$ for each plaintext m. $\mathcal{K}$ and $\mathcal{E}$ are PPT algorithms, and $\mathcal{D}$ is a polynomial time algorithm.

2.2 One-Wayness

The one-wayness problem is as follows: given a public key pk and a ciphertext c, find the plaintext m such that $c \stackrel{R}{\leftarrow} \mathcal{E}_{pk}(m)$. Formally, for an adversary A, consider an experiment as follows.

$$(pk, sk) \stackrel{R}{\leftarrow} \mathcal{K},\ c \stackrel{R}{\leftarrow} \mathcal{E}_{pk}(m), \tilde{m} \stackrel{R}{\leftarrow} A(pk, c).$$

where m is randomly chosen from the domain of pk. Let

$$Adv^{ow}_{\mathcal{PE}}(A) = \Pr(\tilde{m} = m).$$

For any $t > 0$, define

$$Adv^{ow}_{\mathcal{PE}}(t) = \max_{A} Adv^{ow}_{\mathcal{PE}}(A),$$

where the maximum is over all A who run in time t.

Definition 1. *We say that $\mathcal{PE}$ is (t, ε)-one-way if $Adv^{ow}_{\mathcal{PE}}(t) < \varepsilon$. We also say that $\mathcal{PE}$ is one-way if $Adv^{ow}_{\mathcal{PE}}(A)$ is negligible for any PPT adversary A.*

2.3 Semantic Security

We say that a public-key encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is semantically secure against chosen plaintext attacks (SS-CPA) if it is hard to find any (partial) information on m from c. This notion is equivalent to indistinguishability (IND-CPA), which is described as follows [BDPR98,Gol01].

We consider an adversary $B = (B_1, B_2)$ as follows. In the "find" stage, B_1 takes a public key pk and outputs $(m_0, m_1, state)$, where m_0 and m_1 are two equal length plaintexts and $state$ is some state information. In the "guess" stage, B_2 gets a challenge ciphertext $c \stackrel{R}{\leftarrow} \mathcal{E}_{pk}(m_b)$ from an oracle, where b is a randomly chosen bit. B_2 finally outputs a bit $\tilde{b}$. We say that an encryption scheme $\mathcal{PE}$ is secure in the sense of IND-CPA if $|\Pr(\tilde{b} = b) - 1/2|$ is negligible.

Formally, for each security parameter l, let

$$(pk, sk) \stackrel{R}{\leftarrow} \mathcal{K},\ (m_0, m_1, state) \stackrel{R}{\leftarrow} B_1(pk), c \stackrel{R}{\leftarrow} \mathcal{E}_{pk}(m_b),\ \tilde{b} \stackrel{R}{\leftarrow} B_2(c, state).$$

Definition 2. *We say that $\mathcal{PE}$ is secure in the sense of indistinguishability against chosen-plaintext attack (IND-CPA) if*

$$\mathtt{Adv}^{ind}_{\mathcal{PE}}(B) \stackrel{\triangle}{=} |\Pr(\tilde{b} = b) - 1/2|$$

is negligible for any PPT adversary B.

If an adversary $B = (B_1, B_2)$ is allowed to access the decryption oracle $\mathcal{D}_{sk}(\cdot)$, we denote it by $B^{\mathcal{D}} = (B_1^{\mathcal{D}}, B_2^{\mathcal{D}})$. If $\mathtt{Adv}^{ind}_{\mathcal{PE}}(B^{\mathcal{D}})$ is negligible for any PPT adversary $B^{\mathcal{D}}$, we say that $\mathcal{PE}$ is secure in the sense of indistinguishability against adaptive chosen-ciphertext attack (IND-CCA).

2.4 Factoring Assumptions

The *general* factoring problem is to factor $n = pq$, where p and q are two primes such that $|p| = |q|$. Formally, for an factoring algorithm B, consider the following experiment. Generate two primes p and q such that $|p| = |q|$ randomly. Give $n = pq$ to B. We say that B succeeds if B can output p or q.

Definition 3. *We say that the general factoring problem is (t, ε)-hard if* $\Pr(B$ *succeeds*$) < \varepsilon$ *for any B who runs in time t. We also say that it is hard if* $\Pr(B$ *succeeds*$)$ *is negligible for any PPT algorithm B.*

The general factoring assumption claims that the general factoring problem is hard.

We say that $n(= pq)$ is a *Blum* integer if p and q are prime numbers such that $p = q = 3 \bmod 4$ and $|p| = |q|$. The *Blum*-factoring problem is defined similarly. *Blum*-factoring assumption claims that the *Blum*-factoring problem is hard.

3 Exact One-Wayness of Rabin-Paillier Scheme

Galindo et al. recently constructed Rabin-Paillier encryption scheme [GMMV03] and showed that its one-wayness is as hard as factoring Blum integers, where $n = pq$ is called a Blum integer if $p = q = 3 \bmod 4$. However, there is a polynomially bounded gap between the difficulty of factoring and the *claimed* one-wayness. This is because they used the same proof technique as that of [CNS02].

In this section, we show that there exists no gap between the difficulty of factoring Blum integers and the *real* one-wayness of Rabin-Paillier encryption scheme. In other words, we present the exactly tight one-wayness of Rabin-Paillier encryption scheme.

Our proof is very simple and totally elemental. In particular, no LLL algorithm is required which was essentially used in the previous proofs for RSA/Rabin-Paillier [CNS02,GMMV03].

3.1 Rabin-Paillier Encryption Scheme

Rabin-Paillier encryption scheme is described as follows. Let

$$Q_n \stackrel{\triangle}{=} \{r^2 \bmod n^2 \mid r \in Z_n^*\}.$$

We say that $\bar{r} \in Z_n^*$ is *conjugate* if $(\bar{r}/n) = -1$, where (m/n) denotes Jacobi's symbol.

(Secret key) Two prime numbers p and q such that $|p| = |q|$ and $p = q = 3 \bmod 4$.

(Public key) $n(= pq), e$, where e is a prime such that $|n|/2 < e < |n|$.

(Plaintext) $m \in Z_n$.

(Ciphertext)

$$c = r^{2e} + mn \bmod n^2, \tag{1}$$

where $r \in Q_n$ is randomly chosen.

(Decryption) Since e is a prime such that $|n|/2 < e < |n|$, it satisfies that

$$\gcd(e, p-1) = \gcd(e, q-1) = 1. \tag{2}$$

Therefore, there exists d such that $ed = 1 \bmod lcm(p-1, q-1)$.
Now let $E = c^d \bmod n$. Then it is easy to see that

$$E = r^2 \bmod n.$$

We can find r such that $r \in Q_n$ uniquely because $p = q = 3 \bmod 4$. Finally, by substituting r into eq.(1), we can obtain m.

In [GMMV03], the authors showed that Rabin-Paillier encryption scheme is secure in the sense of IND-CPA if $(n, e, \mathcal{E}(n, e; 0))$ and (n, e, Q_{n^2}) are indistinguishable, where

$$\mathcal{E}(n, e; 0) \stackrel{\triangle}{=} \{r^{2e} \bmod n^2 \mid r \in Q_n\}.$$

Remarks:

1. In [GMMV03], the condition on e is restricted to $\gcd(e, \lambda(n)) = 1$, where λ is Carmichael's function. However, for this parameter choice, we cannot prove that the one-wayness is as hard as the factoring problem, because we cannot generally choose such e for a given n. In Appendix B, we also point out a flaw on their claim for the semantic security of Rabin-Paillier cryptosystem.

2. RSA-Paillier encryption scheme is obtained by letting

$$c = r^e(1 + mn) \bmod n^2$$

for $m \in Z_n$ and $r \in Z_n$ [CGHN01].

3.2 Exactly Tight One-Wayness

Suppose that there exists a PPT algorithm that breaks the one-wayness with probability ε. Then Galindo et al. proved that there exists a PPT algorithm that can factor Blum integers n with probability ε^2 (see the proof of [GMMV03, Proposition 6]).

In this subsection, we show that there exists a PPT algorithm that can factor Blum integers n with probability ε. Since the converse is clear, our reduction is exactly tight.

Scheme	Factoring Probability
Galindo et al. [GMMV03]	ε^2
Our Proposed Proof	ε

Table 1. Factoring probability using OW-oracle with probability ε

Lemma 1. *Let n be a Blum integer. For any conjugate $\bar{r}$, there exists a unique $r \in Q_n$ such that*

$$r^2 = \bar{r}^2 \bmod n. \tag{3}$$

Further, $\gcd(r - \bar{r}, n) = p$ *or* q.

Proof. Note that $(-1/p) = -1$ and $(-1/q) = -1$ for a Blum integer $n = pq$. A conjugate $\bar{r} \in Z_n^*$ satisfies $(\bar{r}/n) = -1$, namely $(I) : (\bar{r}/p) = 1 \wedge (\bar{r}/q) = -1$ or $(II) : (\bar{r}/p) = -1 \wedge (\bar{r}/q) = 1$. In the case of (I), define $r = \bar{r} \bmod p$ and $r = -\bar{r} \bmod q$, then the statement of the lemma is obtained. Similarly in the case of (II) we assign $r = -\bar{r} \bmod p$ and $r = \bar{r} \bmod q$.

Theorem 1. Rabin-Paillier encryption scheme is (t, ε)-one-way if Blum factoring problem is (t', ε)-hard, where $t' = t + \mathcal{O}((\log n)^3)$.

Proof. Suppose that there exists an oracle $\mathcal{O}$ which breaks the one-wayness of Rabin-Paillier encryption scheme with probability ε in time t. We will show a factoring algorithm A.

We show how to find r and $\bar{r}$ satisfying eq.(3). On input n, A first chooses a prime e such that $|n|/2 < e < |n|$ randomly. A next chooses a conjugate $\bar{r} \in Z_n^*$ and a (fake) plaintext $\bar{m} \in Z_n$ randomly, and computes a (fake) ciphertext

$$c = \bar{r}^{2e} + \bar{m}n \bmod n^2.$$

It is clear that c is uniquely written as $c = B_0 + B_1 n \bmod n^2$ for some $B_0 \in Q_n, B_1 \in Z_n$. Note that

1. B_1 is uniformly distributed over Z_n because $\bar{m}$ is randomly chosen from Z_n, and
2. B_0 is uniformly distributed over $\{r^{2e} \bmod n \mid r \in Q_n\}$ from Lemma 1.

Therefore, c is distributed in the same way as valid ciphertexts.

Now A queries c to the oracle $\mathcal{O}$. $\mathcal{O}$ then answers a (valid) plaintext m such that

$$c = r^{2e} + mn \bmod n^2$$

with probability ε in time t, where $r \in Q_n$. Then we have

$$c = r^{2e} = \bar{r}^{2e} \bmod n.$$

Hence we see that $r^2 = \bar{r}^2 \bmod n$. Therefore, r^2 is written as

$$r^2 = \bar{r}^2 + yn \tag{4}$$

for some $y \in Z_n$ (with no modulus). By letting $x = \bar{r}^2 \bmod n^2$, we obtain that

$$w \stackrel{\triangle}{=} c - mn = r^{2e} = (x + yn)^e = x^e + eynx^{e-1} \bmod n^2. \tag{5}$$

It is easy to see that

$$eyx^{e-1} = \frac{w - x^e}{n} \bmod n.$$

Therefore y is obtained as

$$y = (ex^{e-1})^{-1} \frac{w - x^e}{n} \bmod n.$$

Substitute y into eq.(4). Then we can compute a square root $r > 0$ because eq.(4) has no modulus. Finally we can factor n by using $(r, \bar{r})$ from Lemma 1. $\square$

Our algorithm A for Rabin-Paillier scheme is summarized as follows.

Exact_OW_Rabin_Paillier

Input: (n, e), public key of Rabin-Paillier scheme
Output: p, q, factoring of n

1. choose a random $\bar{r} \in Z_n^*$ such that $(\bar{r}/n) = -1$.
2. compute $x = \bar{r}^2 \bmod n^2$.
3. choose a random (fake) plaintext $\bar{m} \in Z_n$.
4. compute a ciphertext $c = x^e + \bar{m}n \bmod n^2$.
5. obtain a valid plaintext $m = \mathcal{O}(c)$
6. compute $w = c - mn = r^{2e} \bmod n^2$.
7. compute $u = (w - x^e \bmod n^2)/n$.
8. compute $y = u(ex^{(e-1)})^{-1} \bmod n$.
9. compute $v = \bar{r}^2 + ny$.
10. find $r > 0$ such that $r^2 = v$ in Z.
11. return $gcd(\bar{r} - r, n)$.

4 New Encryption Scheme

In this section, we propose an encryption scheme such that its one-wayness is as hard as the *general* factoring problem of $n = pq$ (not factoring Blum integers). The proposed scheme is obtained from an encryption scheme proposed by Kurosawa et al. [KIT88,KOMM01].

4.1 Kurosawa et al.'s Encryption Scheme

Kurosawa et al.'s showed an encryption scheme as follows [KIT88].

(Secret key) Two prime numbers p and q such that $|p| = |q|$.
(Public key) $n(= pq)$ and α such that

$$(\alpha/p) = (\alpha/q) = -1, \tag{6}$$

where (α/p) denotes Legendre's symbol.
(Plaintext) $m \in Z_n^*$.
(Ciphertext) $c = (E, s, t)$ such that

$$E = m + \frac{\alpha}{m} \bmod n \tag{7}$$

$$s = \begin{cases} 0 & \text{if } (m/n) = 1; \\ 1 & \text{if } (m/n) = -1, \end{cases} \qquad t = \begin{cases} 0 & \text{if } (\alpha/m \bmod n) > m; \\ 1 & \text{if } (\alpha/m \bmod n) < m. \end{cases}$$

(Decryption) From eq.(7), it holds that

$$m^2 - Em + \alpha = 0 \bmod n. \tag{8}$$

The above equation has four roots. However, we can decrypt m uniquely from (s, t) due to eq.(6) [KIT88,KOMM01]. Also see [KT03, Appendix E].

In [KIT88,KOMM01], it is proved that this encryption scheme is one-way under the general factoring assumption.

4.2 Proposed Encryption Scheme

(Secret key) Two prime numbers p and q such that $|p| = |q|$.
(Public key) $n(= pq), e, \alpha$, where e is a prime such that $|n|/2 < e < |n|$ and $\alpha \in Z_n^*$ satisfies

$$(\alpha/p) = (\alpha/q) = -1. \tag{9}$$

(Plaintext) $m \in Z_n$.
(Ciphertext)

$$c = \left(r + \frac{\alpha}{r}\right)^e + mn \bmod n^2, \tag{10}$$

where $r \in Z_n^*$ is a random element such that $(r/n) = 1$ and $(\alpha/r \bmod n) > r$. (We can compute $1/r \bmod N^2$ faster than the direct method [KT03, Sec.4.3].)

(Decryption) Let $E = c^d \bmod n$, where $ed = 1 \bmod lcm(p-1, q-1)$. Then it is easy to see that

$$E = r + \frac{\alpha}{r} \bmod n.$$

Note that $(E, 0, 0)$ is the ciphertext of r by Kurosawa et al.'s encryption scheme. Therefore we can find r by decrypting $(E, 0, 0)$ with the decryption algorithm. Finally, by substituting r into eq.(10), we can obtain m.

5 One-Wayness of the Proposed Scheme

In this section, we show the one-wayness of the proposed scheme by applying our proof technique developed in Sec.3. Our security reduction is very tight. That is, there is almost no gap between the one-wayness and the hardness of the general factoring problem. Indeed, our proof requires only one decryption-oracle query while the previous proof for RSA/Rabin-Paillier encryption scheme requires two oracle queries [CNS02,GMMV03].

5.1 Proof of One-Wayness

We say that

1. $r \in Z_n^*$ is *principal* if $(r/n) = 1$ and $(\alpha/r \bmod n) > r$.
2. $\bar{r} \in Z_n^*$ is *conjugate* if $(\bar{r}/n) = -1$.

Note that in terms of the parameters of Kurosawa et al's encryption scheme, $r \in Z_n^*$ is *principal* if $(s, t) = (0, 0)$ and $\bar{r} \in Z_n^*$ is *conjugate* if $s = 1$.

Lemma 2. *For any conjugate $\bar{r}$, there exists a unique principal r such that*

$$E \stackrel{\triangle}{=} \bar{r} + \frac{\alpha}{\bar{r}} = r + \frac{\alpha}{r} \bmod n. \tag{11}$$

Further, $\gcd(r - \bar{r}, n) = p$ *or* q.

Proof. There are four different solutions of Kurosawa et al's encryption E corresponding to $(s, t) = (0, 0), (0, 1), (1, 0), (1, 1)$ as shown in [KIT88,KOMM01]. (Also see [KT03, Appendix E].) A conjugate $\bar{r}$ satisfies $(\bar{r}/p) = 1 \wedge (\bar{r}/q) = -1$ or $(\bar{r}/p) = -1 \wedge (\bar{r}/q) = 1$ for $s = 1$. Define $r_1 = \bar{r} \bmod p \wedge r_1 = \alpha/\bar{r} \bmod q$ and $r_2 = \alpha/\bar{r} \bmod p \wedge r_2 = \bar{r} \bmod q$. Then either r_1 or r_2 is the required principle r. Hence, the former part of this Lemma holds. Further, $r \neq \bar{r} \bmod p \wedge r = \bar{r} \bmod q$ or $r = \bar{r} \bmod p \wedge r \neq \bar{r} \bmod q$ holds due to $(\alpha/p) = (\alpha/q) = -1$. Therefore, we can see that $\gcd(r - \bar{r}, n) = p$ or q. □

From eq.(11), it holds that

$$r + \alpha/r = (\bar{r} + \alpha/\bar{r}) + yn \bmod n^2 \tag{12}$$

for some unique $y \in Z_n^*$.

Lemma 3. *Suppose that we have $(\bar{r}, y)$ satisfying eq.(12) for some principal r, where $\bar{r}$ is conjugate. Then we can factor n.*

Proof. We show that r can be computed from $(y, \bar{r})$. Let

$$v = (\bar{r} + \alpha/\bar{r}) + yn \bmod n^2.$$

Then we have

$$r^2 - vr + \alpha = 0 \bmod n^2$$

from eq.(12). We can solve this quadratic equation by using the Coppersmith's algorithm [Cop96] because of $0 < r < n$. Then we can factor n from Lemma 2. □

Lemma 4. Suppose that there exists an oracle $\mathcal{O}$ that breaks the one-wayness of the proposed scheme with probability ε and in time t. Then there exists an algorithm A which factors n from (n, e, α) with probability ε in time $t + poly(\log n)$, where $\mathcal{O}$ is invoked once.

Proof. We show how to find $\bar{r}$ and y satisfying eq.(12). On input (n, e, α), A first chooses a conjugate $\bar{r} \in Z_n^*$ randomly and computes

$$x = \bar{r} + \frac{\alpha}{\bar{r}} \bmod n^2. \tag{13}$$

It next chooses a (fake) plaintext $\bar{m} \in Z_n$ randomly and computes

$$c = x^e + \bar{m}n \bmod n^2.$$

It is clear that c is uniquely written as $c = B_0 + B_1 n \bmod n^2$ for some $B_0, B_1 \in Z_n$. Note that (1) B_1 is uniformly distributed over Z_n because $\bar{m}$ is randomly chosen from Z_n. (2) B_0 is uniformly distributed over $\{(r + \alpha/r)^e \bmod n \mid r \in Z_n^* \text{ is principal}\}$ from Lemma 2. Therefore, c is distributed in the same way as valid ciphertexts.

Now A queries c to the oracle $\mathcal{O}$. $\mathcal{O}$ then answers a (valid) plaintext m such that

$$c = \left(r + \frac{\alpha}{r}\right)^e + mn \bmod n^2$$

with probability ε and in time t, where $r \in Z_n^*$ is principal. Then we have

$$c = \left(r + \frac{\alpha}{r}\right)^e = x^e \bmod n.$$

Hence we see that $r + \frac{\alpha}{r} = x \bmod n$. Therefore, there exists $y \in Z_n$ such that

$$r + \frac{\alpha}{r} = x + yn \bmod n^2.$$

We then obtain that

$$w \overset{\triangle}{=} c - mn = (r + \alpha/r)^e = (x + yn)^e = x^e + eynx^{e-1} \bmod n^2.$$

It is easy to see that

$$eyx^{e-1} = \frac{w - x^e}{n} \bmod n.$$

Therefore y is obtained as

$$y = \frac{w - x^e}{n}(ex^{e-1})^{-1} \bmod n.$$

Finally we can factor n by using $(\bar{r}, y)$ from Lemma 3. □

Our algorithm A for the proposed scheme is summarized as follows:

OW_Reciprocal_Paillier

Input: (n, e, α), public-key of the proposed scheme
Output: p, q, factoring of n

1. choose a random $\bar{r} \in Z_n^*$ such that $(\bar{r}/n) = -1$.
2. compute $x = \bar{r} + \alpha/\bar{r} \bmod n^2$.
3. choose a random (fake) plaintext $\bar{m} \in Z_n^*$.
4. compute a ciphertext $c = x^e + \bar{m}n \bmod n^2$.
5. obtain a valid plaintext $m = \mathcal{O}(c)$
6. compute $w = c - mn = (r + \alpha/r)^e \bmod n^2$.
7. compute $u = (w - x^e)/n$.
8. compute $y = u(ex^{(e-1)})^{-1} \bmod n$.
9. compute $v = (\bar{r} + \alpha/\bar{r}) + ny \bmod n$.
10. solve $r^2 - vr + \alpha = 0 \bmod n^2$ using Coppersmith's algorithm [Cop96].
11. return $gcd(\bar{r} - r, n)$.

Theorem 2. *The proposed encryption scheme is (t, ε) one-way if the general factoring problem is $(t', \varepsilon/2)$-hard, where $t' = t + poly(\log n)$.*

Proof. Suppose that there exists a PPT algorithm that breaks the one-wayness of the proposed scheme with probability ε in time t. Then we show a PPT algorithm which can factor n.

For a given n, we choose a prime e such that $|n|/2 < e < |n|$ randomly. We also choose $\alpha \in Z_n^*$ such that $(\alpha/n) = 1$ randomly. It is easy to see that α satisfies eq.(9) with probability 1/2. Next apply Lemma 4 to (n, e, α). Then we can factor n with probability $\varepsilon/2$ in time $t' = t + poly(\log n)$. □

The proposed scheme is a combination of the scheme of Kurosawa et al. and the RSA-Paillier scheme. Another construction is to encrypt a message $m \in Z/nZ$ as follows:

$$c = \left(r^e + \frac{\alpha}{r^e}\right) + mn \bmod n^2, \tag{14}$$

where $r \in Z_n^*$ is a random element such that $(r^e \bmod n/n) = 1$ and $(\alpha/r^e \bmod n) > r$. After computing $r^e \bmod n^2$ the reciprocal encryption is applied. However, the security analysis of this construction is more difficult — we cannot apply the above proof technique to this scheme, because $r^e \bmod n^2$ is larger than n.

5.2 Hensel Lifting and Large Message Space

Catalano et al. proved that Hensel-RSA problem is as hard as breaking RSA for any lifting index l [CNS02].

In this section, we define Hensel-Reciprocal problem and show that it is as hard as general factorization for any lifting index l. This result implies that we can enlarge the message space of the proposed encryption scheme for $m \in Z_{n^2}$ in such a way that

$$c = r^e + mn \bmod n^l.$$

Suppose that we are given a public key (n, e, α) of the proposed encryption scheme and

$$y = \left(r + \frac{\alpha}{r}\right)^e \bmod n,$$

where $r \in Z_n^*$ is principal. The Hensel-Reciprocal problem is to compute

$$Y = \left(r + \frac{\alpha}{r}\right)^e \bmod n^l$$

from (n, e, α, y) and l, where $r \in Z_n^*$ is principal and l is a positive integer. Then we can prove the following theorem (See [KT03]).

Theorem 3. *The Hensel-Reciprocal problem is as hard as general factorization for any lifting index $l \geq 2$.*

Proof. It is easy to see that we can solve the Hensel-Reciprocal problem if we can factor n. We will prove the converse.

Suppose that there exists a PPT algorithm which can solve the Hensel-Reciprocal problem with probability ε for some $l \geq 2$. That is, the PPT algorithm can compute $Y = \left(r + \frac{\alpha}{r}\right)^e \bmod n^l$ from (n, e, α, y) and $l \geq 2$, where $r \in Z_n^*$ is principal. Then we can compute $Y' = \left(r + \frac{\alpha}{r}\right)^e \bmod n^2$. Now similarly to the proof of Lemma 4 and Theorem 2, we can factor n with probability $\varepsilon/2$ in polynomial time. □

6 Semantic Security of the Proposed Scheme

In this section, we discuss the semantic security of the proposed scheme. Let (n, e, α) be a public key of the proposed encryption scheme.

6.1 Semantic security

Let

$$SMALL_{RSAP}(n, e) \stackrel{\triangle}{=} \{(n, e, x) \mid x = r^e \bmod n^2, r \in Z_n\}$$
$$LARGE_{RSAP}(n, e) \stackrel{\triangle}{=} \{(n, e, x) \mid x = r^e \bmod n^2, r \in Z_{n^2}\}$$

Note that

$$|SMALL_{RSAP}(n, e)| = n, \quad \text{and} \quad |LARGE_{RSAP}(n, e)| = n^2.$$

It is known that RSA-Paillier encryption scheme is IND-CPA if $SMALL_{RSAP}(n, e)$ and $LARGE_{RSAP}(n, e)$ are indistinguishable [CGHN01]. We call it RSA-Paillier assumption.

We now define $SMALL_{RSAK}(n, e, \alpha)$ and $LARGE_{RSAK}(n, e, \alpha)$ as follows.

$$SMALL_{RSAK}(n, e, \alpha) \stackrel{\triangle}{=} \{(n, e, \alpha, x) \mid x = \left(r + \frac{\alpha}{r}\right)^e \bmod n^2, r \in Z_n^* \text{ is principal}\}$$
$$LARGE_{RSAK}(n, e, \alpha) \stackrel{\triangle}{=} \{(n, e, \alpha, x) \mid x = \left(r + \frac{\alpha}{r}\right)^e \bmod n^2, r \in Z_{n^2}^*\}.$$

Note that

$$|SMALL_{RSAK}(n, e, \alpha)| = \phi(n)/4, \quad \text{and} \quad |LARGE_{RSAK}(n, e, \alpha)| = \phi(n)n/4,$$

because $r + \frac{\alpha}{r} \bmod n^2$ is a $4:1$ mapping.

Theorem 4. *The proposed encryption scheme is secure in the sense of IND-CPA if two distributions $SMALL_{RSAK}(n, e, \alpha)$ and $LARGE_{RSAK}(n, e, \alpha)$ are indistinguishable.*

We call the above indistinguishability Reciprocal-Paillier assumption. A proof will be given in Appendix A.

6.2 Relationship with RSA-Paillier Assumption

We investigate the relationship between RSA-Paillier assumption and Reciprocal-Paillier assumption. We first generalize $SMALL_{RSAP}$ and $LARGE_{RSAP}$ so that they include α. That is, let

$$SMALL'_{RSAP}(n, e, \alpha) \stackrel{\triangle}{=} \{(n, e, \alpha, x) \mid x = r^e \bmod n^2, r \in Z_n^*\}$$
$$LARGE'_{RSAP}(n, e, \alpha) \stackrel{\triangle}{=} \{(n, e, \alpha, x) \mid x = r^e \bmod n^2, r \in Z_{n^2}^*\}$$

We then define *modified RSA-Paillier assumption* as follows: $SMALL'_{RSAP}(n, e, \alpha)$ and $LARGE'_{RSAP}(n, e, \alpha)$ are indistinguishable. We next define *reciprocal assumption* as follows: $SMALL_{RSAK}(n, e, \alpha)$ and $SMALL'_{RSAP}(n, e, \alpha)$ are indistinguishable.

Then we have the following corollary of Theorem 4.

Corollary 1. *The proposed encryption scheme is secure in the sense of IND-CPA if both modified RSA-Paillier assumption and the reciprocal assumption hold.*

Proof. We prove that $LARGE_{RSAK}(n, e, \alpha)$ and $LARGE'_{RSAP}(n, e, \alpha)$ are indistinguishable under the reciprocal assumption. Let $\mathcal{O}$ be an oracle that distinguishes two distributions $LARGE_{RSAK}(n, e, \alpha)$ and $LARGE_{RSAP}(n, e, \alpha)$. We construct a distinguisher D which can distinguish between $SMALL_{RSAK}(n, e, \alpha)$ and $SMALL'_{RSAP}(n, e, \alpha)$. For (n, e, α, c), D chooses a random $s \in Z_n$, and computes $c' = c + ns \bmod n^2$. Then it asks (n, e, α, c') to the oracle $\mathcal{O}$. Because s

is randomly chosen in Z_n, we can show that (n, e, α, c') is uniformly distributed in either $LARGE_{RSAK}(n, e, \alpha)$ or $LARGE'_{RSAP}(n, e, \alpha)$. Thus the oracle $\mathcal{O}$ can correctly distinguish between $SMALL_{RSAK}(n, e, \alpha)$ and $SMALL'_{RSAP}(n, e, \alpha)$.

Therefore

$$SMALL_{RSAK} \approx SMALL'_{RSAP} \approx LARGE'_{RSAP} \approx LARGE_{RSAK},$$

where $\approx$ means indistinguishable. This implies that Reciprocal-Paillier assumption holds. $\square$

7 On Chosen Ciphertext Security

For chosen ciphertext security, we can obtain a variant of our encryption scheme as follows by applying the technique of [Poi99].

$$c = (\left(r + \frac{\alpha}{r}\right)^e + mn \bmod n^2)||H(r, m)$$

where H is a random hash function and $||$ denotes concatenation. In the random oracle model, (1) this scheme is one-way against chosen ciphertext attacks under the general factoring assumption. (2) It is also IND-CCA under the assumption given in Sec.6.

In the standard model, it still remains one-way and IND-CPA against chosen plaintext attacks. In general, we can prove the following theorem.

Theorem 5. *Let $\mathcal{PE}$ be an encryption scheme with ciphertexts $c = E_{pk}(m, r)$. Suppose that (1) the set of r belongs to BPP and (2) there exists a decryption algorithm which outputs not only m but also r. For $\mathcal{PE}$, consider an encryption scheme $\widetilde{\mathcal{PE}}$ such that*

$$\tilde{c} = E_{pk}(m, r)||H(m, r).$$

If PE is one-way against chosen plaintext attacks (IND-CPA, resp.), then $\widetilde{\mathcal{PE}}$ is one-way against chosen ciphertext attacks (IND-CCA, resp.) in the random oracle model. $\widetilde{\mathcal{PE}}$ still remains one-way against chosen plaintext attacks (IND-CPA, resp.) in the standard model.

The details will be given in the final paper.

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.

[Bon01] D. Boneh, "Simplified OAEP for RSA and Rabin Functions," CRYPTO 2001, LNCS 2139, pp.275-291, 2001.

[CGHN01] D. Catalano, R. Gennaro, N. Howgrave-Graham, and P. Nguyen; "Paillier's cryptosystem revisited," The 8th ACM conference on Computer and Communication Security, pp.206-214, 2001.

[CNS02] D. Catalano, P. Nguyen, and J. Stern, "The Hardness of Hensel Lifting: The Case of RSA and Discrete Logarithm," ASIACRYPT 2002, LNCS 2501, pp.299-310, 2002.
[Cop96] D. Coppersmith, "Finding a Small Root of a Univariate Modular Equation," EUROCRYPT '96, LNCS 1070, pp.155-165, 1996.
[CS98] R. Cramer and V. Shoup, "A Practical Public-Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attacks," CRYPTO'98, LNCS 1462, pp.13-25, 1998.
[CS02] R. Cramer and V. Shoup, "Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption," EUROCRYPT 2002, LNCS 2332, pp.45-64, 2002.
[FOPS01] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern, "RSA-OAEP is Secure under the RSA Assumption," CRYPTO 2001, LNCS 2139, pp.260-274, 2001.
[GMMV03] D. Galindo, S. Molleví, P. Morillo, J. Villar, "A Practical Public Key Cryptosystem from Paillier and Rabin Schemes," PKC 2003, LNCS 2567, pp.279-291, 2003.
[Gol01] O. Goldreich, *Foundations of Cryptography: Basic Tools*, Cambridge University Press, 2001.
[KIT88] K. Kurosawa, T. Itoh, M. Takeuchi, "Public Key Cryptosystem using a Reciprocal Number with the Same Intractability as Factoring a Large Number," CRYPTOLOGIA, XII, pp.225-233, 1988.
[KT03] K. Kurosawa and T. Takagi, "Some RSA-based Encryption Schemes with Tight Security Reduction," A long version of this paper, IACR ePrint archive, 2003/157, 2003. (available from http://eprint.iacr.org/)
[KOMM01] K. Kurosawa, W. Ogata, T. Matsuo, S. Makishima, "IND-CCA Public Key Schemes Equivalent to Factoring n=pq, PKC 2001, LNCS 1992, pp36-47, 2001.
[OU98] T.Okamoto and S.Uchiyama, "A New Public Key Cryptosystem as Secure as Factoring," Eurocrypt'98, LNCS 1403, pp.308–318, 1998/
[Poi99] D.Pointcheval, "New Public Key Cryptosystems based on the Dependent-RSA Problems," Eurocrypt'99, LNCS 1592, pp.239-254, 1999.
[ST02] K. Sakurai, T. Takagi, "New Semantically Secure Public-Key Cryptosystems from the RSA-Primitive," PKC 2002, LNCS 2274, pp.1-16, 2002.
[Sho01] V. Shoup, "OAEP Reconsidered," CRYPTO 2001, LNCS 2139, pp.239–259, 2001.
[Tak97] T. Takagi, "Fast RSA-Type Cryptosystems using N-adic Expansion," CRYPTO '97, LNCS 1294, pp.372-384, 1997.

A Semantic Security of the Proposed Scheme

A.1 Basic Result

Let $ZERO(n,e,\alpha)$ be the set of ciphertexts for $m=0$ and $ALL(n,e,\alpha)$ be the set of ciphertexts for all $m \in Z_n$. That is,

$$\begin{aligned} ZERO(n,e,\alpha) &\triangleq \{\left(r+\frac{\alpha}{r}\right)^e \bmod n^2 \mid r \in Z_n^* \text{ is principal}\} \\ ALL(n,e,\alpha) &\triangleq \{\left(r+\frac{\alpha}{r}\right)^e + mn \bmod n^2 \mid m \in Z_n \text{ and } r \in Z_n^* \text{ is principal}\}. \end{aligned}$$

Define

$$Reciprocal_0(n,e,\alpha) \stackrel{\triangle}{=} \{(n,e,\alpha,x) \mid x \in ZERO(n,e,\alpha)\}$$
$$Reciprocal_{ALL}(n,e,\alpha) \stackrel{\triangle}{=} \{(n,e,\alpha,x) \mid x \in ALL(n,e,\alpha)\}$$

Note that we have $Reciprocal_0(n,e,\alpha) = SMALL_{RSAK}(n,e,\alpha)$ from their definition.

Theorem 6. *The proposed encryption scheme is secure in the sense of IND-CPA if and only if $Reciprocal_0(n,e,\alpha)$ and $Reciprocal_{ALL}(n,e,\alpha)$ are indistinguishable.*

Proof. Suppose that there exists an adversary $B = (B_1, B_2)$ which breaks our encryption scheme in the sense of IND-CPA, where B_1 works in the find stage and B_2 works in the guess stage.

We will show a distinguisher D which can distinguish between two distributions $Reciprocal_0(n,e,\alpha)$ and $Reciprocal_{ALL}(n,e,\alpha)$. Let (n,e,α,x) be the input to D, where $x \in ZERO(n,e,\alpha)$ or $x \in ALL(n,e,\alpha)$.

1. D gives $pk = (n,e,\alpha)$ to B_1.
2. Then B_1 outputs $(m_0, m_1, state)$.
3. D chooses a bit b randomly and computes

$$c_b = x + m_b n \bmod n^2.$$

   D gives $(c_b, state)$ to B_2.
4. B_2 outputs a bit $\tilde{b}$.
5. D outputs "0" if $\tilde{b} = b$. Otherwise, D outputs "1".

Let P_0 denote the probability that $D = 0$ for $x \in ZERO(n,e,\alpha)$ and P_{ALL} denote the probability that $D = 0$ for $x \in ALL(n,e,\alpha)$.

Now if $x \in ALL(n,e,\alpha)$, then c_b is uniformly distributed over $ALL(n,e,\alpha)$ for both $b = 0$ and 1. Therefore, it is clear that

$$P_{ALL} = 1/2.$$

On the other hand, if $x \in ZERO(n,e,\alpha)$, then c_b is a valid ciphertext of m_b. Therefore, from our assumption and from Def.2, we obtain that

$$|P_0 - 1/2| = |\Pr(\tilde{b} = b) - 1/2|$$

is non-negligible. Hence

$$|P_0 - P_{ALL}|$$

is non-negligible because $P_{ALL} = 1/2$. This means that D can distinguish between $Reciprocal_0(n,e,\alpha)$ and $Reciprocal_{ALL}(n,e,\alpha)$.

Next suppose that there exists a distinguisher D which is able to distinguish between $Reciprocal_0(n,e,\alpha)$ and $Reciprocal_{ALL}(n,e,\alpha)$. We will show an adversary $B = (B_1, B_2)$ which breaks our encryption scheme in the sense of

IND-CPA, where B_1 works in the find stage and B_2 works in the guess stage. On input $pk = (n, e, \alpha)$, B_1 outputs $m_0 = 0$ and $m_1 \in Z_n$, where m_1 is randomly chosen from Z_n. For a given ciphertext c_b, B_2 gives (n, e, α, c_b) to D, where c_b is a ciphertext of m_b.

Note that c_0 is randomly chosen from $ZERO(n, e, \alpha)$ and c_1 is randomly chosen from $ALL(n, e, \alpha)$. Therefore, D can distinguish them from our assumption. Hence B_2 can distinguish them. □

A.2 Extended Result

Lemma 5. *$Reciprocal_{ALL}(n, e, \alpha) = LARGE_{RSAK}(n, e, \alpha)$.*

Proof. First suppose that $(n, e, \alpha, c) \in LARGE_{RSAK}(n, e, \alpha)$. Then

$$c = \left(r + \frac{\alpha}{r}\right)^e \bmod n^2$$

for some $r \in Z_{n^2}^*$. Decrypt c by our decryption algorithm. Then we can find $m \in Z_n$ and a principal $r' \in Z_n^*$ such that

$$c = \left(r' + \frac{\alpha}{r'}\right)^e + mn \bmod n^2.$$

Therefore $(n, e, \alpha, c) \in Reciprocal_{ALL}(n, e, \alpha)$. This means that

$$LARGE_{RSAK}(n, e, \alpha) \subseteq Reciprocal_{ALL}(n, e, \alpha).$$

Next suppose that $(n, e, \alpha, c) \in Reciprocal_{ALL}(n, e, \alpha)$. Then

$$c = \left(r + \frac{\alpha}{r}\right)^e + mn \bmod n^2$$

for some $m \in Z_n$ and a principal $r \in Z_n^*$. We will show that there exists $u \in Z_{n^2}^*$ such that

$$c = \left(u + \frac{\alpha}{u}\right)^e \bmod n^2 \tag{15}$$

and $u \bmod n$ is principal. The above equation holds if and only if

$$u^2 - c^d u + \alpha = 0 \bmod n^2, \tag{16}$$

where $ed = 1 \bmod \phi(n)n$. For y_p such that

$$(r^2 - c^d r + \alpha) + p y_p (2r - c^d) = 0 \bmod p^2,$$

let $u_p = r + p y_p \bmod p^2$. Then it is easy to see that

$$u_p^2 - c^d u_p + \alpha = 0 \bmod p^2.$$

Similarly for y_q such that

$$(r^2 - c^d r + \alpha) + q y_q (2r - c^d) = 0 \bmod q^2,$$

let $u_q = r + qy_q \bmod q^2$. Then

$$u_q^2 - c^d u_q + \alpha = 0 \bmod p^2.$$

Now consider u such that

$$u = u_p \bmod p^2, \ u = u_q \bmod q^2.$$

Then u satisfies eq.(16). Therefore u satisfies eq.(15). This means that $c \in LARGE_{RSAK}(n, e, \alpha)$. Hence

$$Reciprocal_{ALL}(n, e, \alpha) \subseteq LARGE_{RSAK}(n, e, \alpha).$$

Consequaently

$$LARGE_{RSAK}(n, e, \alpha) = Reciprocal_{ALL}(n, e, \alpha).$$

$\square$

A.3 Proof of Theorem 4

From Theorem 6 and Lemma 5, the proposed encryption scheme is IND-CPA if if $Reciprocal_0(n, e, \alpha)$ and $LARGE_{RSAK}(n, e, \alpha)$ are indistinguishable. From the definition we have $Reciprocal_0(n, e, \alpha) = SMALL_{RSAK}(n, e, \alpha)$.

B Flaw on the Semantic Security of Rabin-Paillier

Let

$$SMALL_{QR}(n, e) \triangleq \{(n, e, x) \mid x = r^{2e} \bmod n^2, r \in Q_n\}$$
$$LARGE_{QR}(n, e) \triangleq \{(n, e, x) \mid x = r^{2e} \bmod n^2, r \in Q_{n^2}\}$$

Rabin-Paillier encryption scheme is IND-CPA if and only if $SMALL_{QR}(n, e)$ and $LARGE_{QR}(n, e)$ are indistinguishable [GMMV03, Proposition 9].

Galindo et al. further claimed that $SMALL_{QR}(n, e)$ and $LARGE_{QR}(n, e)$ are indistinguishable if

- $SMALL_{RSAP}(n, e)$ and $LARGE_{RSAP}(n, e)$ are indistinguishable (RSA-Paillier is IND-CPA under this condition) and
- $QR(n)$ and $QNR(n, +)$ are indistinguishable, where

$$QR(n) \triangleq \{(n, x) \mid x \in Q_n\}$$
$$QNR(n, +) \triangleq \left\{(n, x) \mid x \in Z_n^*, \left(\frac{x}{n}\right) = 1\right\}$$

in [GMMV03, Proposition 11].

However, this claim is wrong. In the proof, they say that D_1 and D_2 are indistinguishable, where

$$D_1 \triangleq \{x \mid x = r^e \bmod n^2, r \in Q_n\}$$
$$D_2 \triangleq \{x \mid x = r^e \bmod n^2, r \in Z_n^*\}.$$

However, we can distinguish them easily by computing $\left(\frac{x}{n}\right)$.