コンピュータセキュリティ　14－5
（2001．7．25）

# 単一仮定の下で IND-CCA2 である効率的な公開鍵暗号方式

西岡　玄次

（株）日立製作所システム開発研究所
〒244-0817　横浜市戸塚区吉田町292番地

nishioka@sdl.hitachi.co.jp

**あらまし.** 本論文では，Cramer-Shoup スキーム [5] をベースとした新しい公開鍵暗号方式について述べる．提案方式は，Cramer-Shoup スキームよりも弱い仮定の下で，適応的選択暗号文攻撃に対して強秘匿（IND-CCA2）であることが証明できる．具体的には，関数的仮定を必要とせず，また Diffie-Hellman 決定問題（DDH）の困難性の仮定よりも弱い仮定のもとで IND-CCA2 であることを証明できる特徴を持つ．

また，提案方式は，単一仮定の下で安全性が証明できる従来の公開鍵暗号方式に比べて実用的である．

**キーワード.** 公開鍵暗号，安全性証明，適応的選択暗号文攻撃，強秘匿，標準的モデル

# A Practical Public-Key Cryptosystem that is IND-CCA2 under a Single Assumption

Mototsugu Nishioka

Systems Development Laboratory, Hitachi, Ltd.
292 Yoshida-cho, Totsuka-ku, Yokohama 244, Japan

nishioka@sdl.hitachi.co.jp

**Abstract.** The new public-key encryption scheme described in this paper is based on the Cramer-Shoup scheme [5] but can be proven to be semantically secure against an adaptive chosen ciphertext attack (IND-CCA2) under a weaker assumption than that of the Cramer-Shoup scheme. It requires no functional assumptions and requires only one number theoretic assumption to assure the ideal security. This number theoretic assumption is weaker than the Decisional Diffie-Hellman (DDH) assumption underlying the Carmer-Shoup scheme. The new scheme is also more practical than the previous public-key cryptosystems that are IND-CCA2 under a single assumption.

**Keywords.** Public-key cryptosystem, Provably secure, Adaptive chosen-ciphertext attack, Semantic security, Standard model

# 1 Introduction

It is widely agreed that the desirable security level of public-key cryptosystems is to be semantically secure against an adaptive chosen ciphertext attack (IND-CCA2) or non-malleable against that attack (NM-CCA2) [6, 13] (It is proven that these two security levels, respectively, IND-CCA2 and NM-CCA2, are equivalent [1]).

Provably secure public-key encryption schemes can be classified into two categories: those like the RSA-OAEP scheme, for which the security proof is based on the *random oracle model*, and those like the Cramer-Shoup scheme, for which the security proof is based on the *standard model* of computation. Those in the first category are generally more practical, but those in the later category are based on assumptions that are more reasonable.

It is disirable that public-key encryption schemes should provide the ideal security, namely IND-CCA2, under weak assumptions and should not have excessive computation costs.

To the best of our knowledge, Cramer-Shoup scheme is the only practical public-key encryption scheme proven to be IND-CCA2 in the standard model. Its security is based on the intractability of the Decisional Diffie-Hellman (DDH) problem and the existence of a family of universal one-way hash functions. But because real security systems uses practical hash functions, such as the SHA and MD5 algorithms, in place of the universal one-way hash function to increase the efficiency[14], the real-world security of the Cramer-Shoup scheme cannot be proved unless the practical function is assumed to be a universal hash function. Note that although the SHA is designed to be *collision resistant* (stronger notion than a universal one-way hush function), the proof has not been given without making assumptions.

Cramer and Shoup also described a hash-free variant of their scheme, but as we will see in section 6, the encryption procedure that hash-free variant requires is computationally expensive.

This paper describes a new public-key encryption scheme that is based on the Cramer-Shoup scheme [5] but can be proven to be semantically secure against an adaptive chosen ciphertext attack (IND-CCA2) under a weaker assumption than that of the Cramer-Shoup scheme. It requires no functional assumptions and requires only one number theoretic assumption to assure the ideal security. This number theoretic assumption is weaker than the Decisional Diffie-Hellman (DDH) assumption underlying the Carmer-Shoup scheme. This scheme is more practical than the previous public-key cryptosystems that are IND-CCA2 under a single assumption.

# 2 Definitions

This section defines the Decisional Diffie-Hellman (DDH) problem. For definitions of *public-key encryption* or *semantic security*, see other literature, such as [1] and [8].

**Definition 2.1 (DDH).** Let $G$ be a multiplicative group with a prime order $q$, and let $g_1, g_2 \in G$. Let $\delta$ be a sequence that belongs in one of the following two sets:

$$\mathbf{D}_0 = \{(g_1, g_2, u_1, u_2) \mid u_1 = {g_1}^r, u_2 = {g_2}^r \text{ for } r \in \mathbb{Z}_q\},$$
$$\mathbf{D}_1 = \{(g_1, g_2, u_1, u_2) \mid u_1, u_2 \in G \text{ with } \log_{g_1} u_1 \neq \log_{g_2} u_2\}.$$

Then, the *Decisional Diffie-Hellman* (DDH) *problem in* $G$ is the problem of guessing $t$ such that $\delta \in \mathbf{D}_t$ for a given sequence $\delta$. And we say that the DDH *assumption in* $G$ *is true* if, for any probabilistic polynomial time algorithm $A$, any constant $c$, and sufficiently large $k$,

$$\Pr[\,(g_1, g_2) \leftarrow G\,;\; b \leftarrow \{0,1\}\,;\; \delta \leftarrow \mathbf{D}_b \;:\; A(g_1, g_2, \delta) = b\,] < \frac{1}{2} + \frac{1}{k^c}.$$

# 3 The Basic Scheme

Let $G$ be a multiplicative group with a prime order $q$, and let $G'$ be a multiplicative group that includes $G$ as a subgroup.

## 3.1 Key Generation

The key generation algorithm runs as follows: Random elements $g_1, g_2 \in G$ are chosen, and random elements

$$x_1, x_2, y_{i1}, y_{i2}, z \in \mathbb{Z}_q \qquad (i = 1, 2)$$

are also chosen. Next, the elements in $G$

$$c = {g_1}^{x_1} {g_2}^{x_2}, \quad d_i = {g_1}^{y_{i1}} {g_2}^{y_{i2}}, \quad h = {g_1}^{z} \qquad (i = 1, 2)$$

are computed. Next, an injective map

$$\pi : X_1 \times X_2 \times M \longrightarrow G'$$

is chosen, where $X_1$ and $X_2$ are finite sets consisting of positive integers such that $\alpha_1 || \alpha_2 < q$ for any $\alpha_1 \in X_1$ and $\alpha_2 \in X_2$, and $M$ is a message space consisting of positive integers such that $m < q$ for any $m \in M$. We assume here that the elements in $X_1$ and $X_2$ respectively have $k_1$ and $k_2$ digits. Then the secret and public keys are given as follows:

Secret Key: $(x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z)$

Public Key: $(g_1, g_2, c, d_1, d_2, h, \pi, \pi^{-1})$

We give an actual example of $(G, G', \pi)$ in section 5.

### 3.2 Encryption

For a given message $m$ ($m \in M$), the encryption algorithm runs as follows: It chooses $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, and $r \in \mathbb{Z}_q$ at random and then computes

$$u_1 = {g_1}^{r}, \quad u_2 = {g_2}^{r}, \quad e = \pi(\alpha_1, \alpha_2, m) h^r, \quad v = {g_1}^{\alpha_1} c^r {d_1}^{\alpha r} {d_2}^{mr},$$

where $\alpha = \alpha_1 || \alpha_2$.

Note that $e$ is defined as an element of $G'$ and $u_1, u_2, v$ are defined as elements of $G$.

Then the ciphertext of $m$ is given as follows:

Ciphertext: $(u_1, u_2, e, v)$

### 3.3 Decryption

For a given ciphertext $(u_1, u_2, e, v)$, the decryption algorithm runs as follows: It computes $\bar{\alpha}_1 \in X_1, \bar{\alpha}_2 \in X_2$ and $\bar{m} \in M$ such that

$$\pi(\bar{\alpha}_1, \bar{\alpha}_2, \bar{m}) = e / {u_1}^{z},$$

by using $z$ and $\pi^{-1}$. It then tests if

$$ {g_1}^{\bar{\alpha}_1} {u_1}^{x_1 + \bar{\alpha} y_{11} + \bar{m} y_{21}} {u_2}^{x_2 + \bar{\alpha} y_{12} + \bar{m} y_{22}} = v, \tag{1}$$

where $\bar{\alpha} = \bar{\alpha}_1 || \bar{\alpha}_2$, and outputs the plaintext

$$m = \begin{cases} \bar{m} & \text{if the condition (1) holds,} \\ \text{“reject”} & \text{otherwise.} \end{cases}$$

## 4 Proof of Security

In this section, we prove the following theorem.

**Theorem 4.1 (IND-CCA2).** The basic scheme is semantically secure against an adaptive chosen ciphertext attack if the DDH assumption in group $G$ is true.

Theorem 4.1 says that if the DDH assumption is true, the basic scheme is IND-CCA2. Since $\alpha_1$ and $\alpha_2$ are secret, however, the converse (namely, the basic scheme is not IND-CCA2 when the DDH problem is solved) cannot be proven by the conventional method used to prove the security of the El Gamal scheme (IND-CPA) and the Cramer-Shoup scheme (IND-CCA2).

Hence, we can say that breaking the basic scheme is at least as difficult as solving the DDH problem. We think the problem of breaking the basic scheme is harder than solving the DDH problem, although this paper does not specify the difference between the difficulties of these problems.

To prove the theorem, we will assume that there is an adversary *Adv* that can break the basic scheme, and show how to use this adversary to construct a probabilistic polynomial time algorithm $A$ that can solve the DDH problem.

The input to $A$ is $(g_1, g_2, u_1, u_2)$, which comes from either **D** or **R** (To avoid a confusion, $\mathbf{D}_0$ and $\mathbf{D}_1$ in the definition 2.1 are respectively denoted **D** and **R** here). $A$ runs the following key generation algorithm, using the given $g_1, g_2$. $A$ chooses

$$x_1, x_2, y_{i1}, y_{i2}, z_1, z_2 \in \mathbb{Z}_q \qquad (i = 1, 2)$$

at random and computes the elements of $G$

$$c = {g_1}^{x_1} {g_2}^{x_2}, \quad d_i = {g_1}^{y_{i1}} {g_2}^{y_{i2}}, \quad h = {g_1}^{z_1} {g_2}^{z_2} \qquad (i = 1, 2).$$

$A$ also chooses a proper injective map $\pi$ (cf. section 3.1). The public key that *Adv* can see is $(g_1, g_2, c, d_1, d_2, h, \pi, \pi^{-1})$. Only $A$ knows $(x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z_1, z_2)$.

Note that the key generation in $A$ is slightly different from that in the basic scheme described in section 3. But, it can be easily shown that if there is a probabilistic polynomial time algorithm $B$ that can break the $z$-version of the basic scheme, then one can construct a probabilistic polynomial time algorithm $B'$ that can break the $(z_1, z_2)$-version of the basic scheme, by using $B$. Thus, it is sufficient only to prove the $(z_1, z_2)$-version.

The encryption oracle by $A$ is given as follows. For given $m_0, m_1$ $(\in M)$, $A$ chooses $b \in \{0, 1\}$ at random. $A$ also chooses $\alpha_1 \in X_1$ and $\alpha_2 \in X_2$ at random and computes

$$\begin{aligned} e &= \pi(\alpha_1, \alpha_2, m_b) {u_1}^{z_1} {u_2}^{z_2}, \\ v &= {g_1}^{\alpha_1} {u_1}^{x_1 + \alpha y_{11} + m_b y_{21}} {u_2}^{x_2 + \alpha y_{12} + m_b y_{22}}, \end{aligned}$$

where $\alpha = \alpha_1 || \alpha_2$. Then, it outputs $(u_1, u_2, e, v)$.

As we will see, the output of the encryption oracle is a perfectly legitimate ciphertext when the input to $A$ comes from **D**, but will not be legitimate when the input to $A$ comes from **R**. This is crucial to the proof of security of the basic scheme, as it is to the proof of the security of the Cramer-Shoup scheme [5].

Theorem 4.1 follows immediately from the following two lemmas.

**Lemma 4.1.** When the sequence $(g_1, g_2, u_1, u_2)$ comes from **D**, then *Adv* can guess a correct hidden bit $b$ with a probability of more than $1/2$.

We have $u_1 = {g_1}^r$ and $u_2 = {g_2}^r$ for some $r \in \mathbb{Z}$, since the sequence $(g_1, g_2, u_1, u_2)$ comes from **D**. It is clear in this case that the output of the encryption oracle has the right distribution, since ${u_1}^{x_1} {u_2}^{x_2} = c^r$, ${u_1}^{y_{i1}} {u_2}^{y_{i2}} = {d_i}^r$ $(i = 1, 2)$ and ${u_1}^{z_1} {u_2}^{z_2} = h^r$. Indeed, these equations imply that $e = \pi(\alpha_1, \alpha_2, m_b) h^r$ and $v = {g_1}^{\alpha_1} c^r {d_1}^{\alpha r} {d_2}^{m_b r}$.

To complete the proof, we need to argue that the output of the decryption oracle also has the right distribution. Let us call $(u_1', u_2', e', v') \in G^4$ a *valid ciphertext* if $\log_{g_1} u_1' = \log_{g_2} u_2'$.

Note that if a ciphertext is valid with $u_1' = {g_1}^{r'}$ and $u_2' = {g_2}^{r'}$, then $h^{r'} = {u_1'}^{z_1} {u_2'}^{z_2}$. Therefore the decryption oracle outputs $m' \in M$ such that $\pi(\alpha_1', \alpha_2', m') = e'/h^{r'}$, if it passes the test in the equation (1).

Consequently, Lemma 4.1 follows immediately from the following claim:

*Claim 1. When the target ciphertext is valid, then the decryption oracle – in both an actual attack against the cryptosystem and in an attack against A – rejects all invalid ciphertext, except with negligible probability.*

We now prove Claim 1 by considering the distribution of the point $P = (x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}) \in {\mathbb{Z}_q}^6$, conditioned on the adversary's view. Let $\log(\cdot)$ denote $\log_{g_1}(\cdot)$, and let $w = \log g_2$.

From the adversary's view, $P$ is a random point on the affine algebraic set $\mathcal{V}$ $(\subset A^6(\mathbb{Z}_q))$ formed by the intersecting hyperplanes

$$\log c = x_1 + w x_2, \tag{2}$$

$$\log d_1 = y_{11} + w y_{12}, \tag{3}$$

$$\log d_2 = y_{21} + w y_{22}. \tag{4}$$

These three equations come from the public key. The output from the encryption oracle does not constrain $P$ any further, as the hyperplane defined by

$$\log v = \alpha_1 + r(x_1 + w x_2) + r\alpha(y_{11} + w y_{12}) + rm(y_{21} + w y_{22}) \tag{5}$$

constrains $P$.

Now suppose that the adversary submits to the decryption oracle an invalid ciphertext $(u_1', u_2', e', v')$, where $\log u_1' = r_1'$ and $\log u_2' = r_2'$ $(r_1' \neq r_2')$. The decryption oracle will reject the ciphertext unless $P$ happens to lie on the hyperplane $\mathcal{H}$ defined by

$$\log v' = \alpha_1' + r_1' x_1 + w r_2' x_2 + \alpha'(r_1' y_{11} + r_2' w y_{12}) + m'(r_1' y_{21} + r_2' w y_{22}), \tag{6}$$

where $\pi(\alpha_1', \alpha_2', m') = e'/{u_1'}^{z_1} {u_2'}^{z_2}$ and $\alpha' = \alpha_1' || \alpha_2'$. But it is clear that equations (2), (3), (4) and (6) are linearly independent, so $\mathcal{H}$ intersects the algebraic set $\mathcal{V}$ at a plane.

Therefore, for $i = 1, 2, \ldots$, the $i$-th invalid ciphertext submitted by the adversary will be rejected with a probability of at least $1 - 1/(q^2 - i + 1)$. From this it follows that the decryption oracle rejects all invalid ciphertext, except with negligible probability.

**Lemma 4.2.** *When the sequence $(g_1, g_2, u_1, u_2)$ comes from* **R**, *the Adv cannot guess a correct hidden bit $b$ with a probability of more than $1/2$.*

Let $u_1 = {g_1}^{r_1}$ and $u_2 = {g_2}^{r_2}$ $(r_1 \neq r_2)$. Lemma 4.2 follows immediately from the following two claims.

*Claim 2. If the decryption oracle rejects all invalid ciphertexts during the attack, then Adv cannot guess the hidden bit $b$ with a probability of more than $1/2$.*

To see this, consider the point $Q = (z_1, z_2) \in {\mathbb{Z}_q}^2$. At the beginning of the attack, this is a random point on the line

$$\log h = z_1 + w z_2, \tag{7}$$

determined by the public key. Moreover, if the decryption oracle decrypts valid ciphertexts $(u_1', u_2', e', v')$, then *Adv* obtains only linearly dependent relations

$$r' \log h = r' z_1 + r' w z_2$$

since ${u_1'}^{z_1} {u_2'}^{z_1} = {g_1}^{r' z_1} {g_2}^{r' z_2} = h^{r'}$. Thus, no further information about $Q$ is leaked.

Consider now the output $(u_1, u_2, e, v)$ of the encryption oracle. Let $\epsilon = {u_1}^{z_1} {u_2}^{z_2}$. Consider the equation

$$\log \epsilon = r_1 z_1 + w r_2 z_2. \tag{8}$$

Equations (7) and (8) clearly are linearly independent, so the conditional distribution of $\epsilon$ – conditioning on $b$ and everything in the *Adv*'s view other than $e$ – is uniform. In other words, $\epsilon$ is a perfect one-time pad. It follows that $b$ is independent of the *Adv*'s view.

*Claim 3. When the target ciphertext is invalid, then the decryption oracle rejects all invalid ciphertexts, except with negligible probability.*

As in the proof of Lemma 4.1, we study the distribution of $P = (x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}) \in {\mathbb{Z}_q}^6$, conditioned on the adversary's view. From the adversary's view, this is a random point on the plane formed by the intersecting hyperplanes (2), (3), (4) and

$$\log v = \alpha_1 + r_1 x_1 + w r_2 x_2 + \alpha(r_1 y_{11} + r_2 w y_{12}) + m_b(r_1 y_{21} + r_2 w y_{22}). \tag{9}$$

Equation (9) comes from the output of the encryption oracle.

Now assume that the adversary submits an invalid ciphertext $(u_1', u_2', e', v') \neq (u_1, u_2, e, v)$, where $\log u_1' = r_1'$ and $\log u_2' = r_2'$ $(r_1' \neq r_2')$.

Let $\pi(\alpha_1', \alpha_2', m') = e'/{u_1'}^{z_1} {u_2'}^{z_2}$, where $\alpha_1' \in X_1$, $\alpha_2' \in X_2$ and $m' \in M$. Then, the decryption oracle rejects the ciphertext unless $P$ happens to lie on the hyperplane defined by

$$\log v' = \alpha_1' + r_1' x_1 + w r_2' x_2 + \alpha'(r_1' y_{11} + r_2' w y_{12}) + m'(r_1' y_{21} + r_2' w y_{22}), \tag{10}$$

where $\alpha' = \alpha_1' || \alpha_2'$.

From the equations (2), (3), (4), (9) and (10), we obtain the following relationship:

$$\begin{pmatrix} 1 & w & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & w & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & w \\ r_1 & r_2 w & \alpha r_1 & \alpha r_2 w & m_b r_1 & m_b r_2 w \\ r_1' & r_2' w & \alpha' r_1' & \alpha' r_2' w & m' r_1' & m' r_2' w \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ y_{11} \\ y_{12} \\ y_{21} \\ y_{22} \end{pmatrix} = \begin{pmatrix} \log c \\ \log d_1 \\ \log d_2 \\ \log v - \alpha_1 \\ \log v' - \alpha_1' \end{pmatrix} \tag{11}$$

For convenience, the $(5,6)$-matrix in the equation (11) is written in the following as $X$.

If rank $X = 5$, then the equations (2), (3), (4), (9) and (10) are linearly independent. Hence, in this case the decryption oracle reject the invalid ciphertext $(u_1', u_2', e', v')$ except with negligible probability.

We consider the case when rank $X < 5$. Since $r_1 \neq r_2$ and $r_1' \neq r_2'$, we have

$$\text{rank } X = 3 + \text{rank} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha - \alpha' & m_b - m' \end{pmatrix}.$$

It then follows that rank $X \geq 4$, and rank $X = 4$ if and only if $\alpha = \alpha'$ and $m_b = m'$.

Now suppose that $\alpha = \alpha'$ and $m_b = m'$. Then there exists $a_i \in \mathbb{Z}_q$ $(1 \leq i \leq 4)$ such that

$$\begin{aligned} r_1' &= a_1 + a_4 r_1, \\ r_2' w &= a_1 w + a_4 r_2 w, \\ r_1' \alpha' &= a_2 + a_4 r_1 \alpha, \\ r_2' \alpha' w &= a_2 w + a_4 r_2 \alpha w, \\ m' r_1' &= a_3 + a_4 m_b r_1, \\ m' r_2' w &= a_3 w + a_4 m_b r_2 w, \end{aligned}$$

since equations (2), (3), (4), (9) and (10) are linearly dependent.

Then $u_1'$ and $u_2'$ can be represented by

$$u_1' = {g_1}^{a_1} {u_1}^{a_3} \qquad \text{and} \qquad u_2' = {g_2}^{a_1} {u_2}^{a_3}.$$

And $v'$ can be represented by

$$\begin{aligned} v' &= {g_1}^{\alpha_1} {u_1'}^{x_1 + \alpha y_{11} + m_b y_{21}} {u_2'}^{x_2 + \alpha y_{12} + m_b y_{22}} \qquad (12) \\ &= {g_1}^{\alpha_1} (cd^{\alpha})^{a_1} \left( {u_1}^{x_1 + \alpha y_{11} + m_b y_{21}} {u_2}^{x_1 + \alpha y_{12} + m_b y_{22}} \right)^{a_3} \\ &= {g_1}^{\alpha_1} \left( cd^{10^{k_2}\alpha_1 + \alpha_2} \right)^{a_1} \left( {u_1}^{x_1 + (10^{k_2}\alpha_1 + \alpha_2) y_{11} + m_b y_{21}} {u_2}^{x_2 + (10^{k_2}\alpha_1 + \alpha_2) y_{12} + m_b y_{22}} \right)^{a_3}, \qquad (13) \end{aligned}$$

where it is assumed that all elements in $X_2$ have $k_2$-digits (cf. section 3).

We study the distribution of $R = (\alpha_1, \alpha_2) \in {\mathbb{Z}_q}^2$, condition on the adversary's view. From the adversary's view, this is a random point on the line

$$\begin{aligned} (1 + 10^{k_2} r_1 y_{11} + 10^{k_2} r_2 w y_{12}) \alpha_1 + (r_1 y_{11} + r_2 w y_{12}) \alpha_2 + r_1 x_1 + r_2 w x_2 \\ + m_b (r_1 y_{21} + r_2 w y_{22}) = \log v. \end{aligned} \qquad (14)$$

Equation (14) comes from equation (9).

The decryption oracle will reject the ciphertext, unless $R$ happens to lie on the line $\mathcal{L}$ defined by

$$\begin{aligned} \log v' &= \alpha_1 + a_1 (x_1 + w x_2 + (10^{k_2}\alpha_1 + \alpha_2)(y_{11} + w y_{12})) \\ &\quad + a_3 (r_1 x_1 + (10^{k_2}\alpha_1 + \alpha_2) r_1 y_{11} + r_1 m_b y_{21} + w r_2 x_2 + (10^{k_2}\alpha_1 + \alpha_2) w r_2 y_{12} + w r_2 m_b y_{22}) \\ &= a_1 x_1 + a_1 w x_2 + a_3 r_1 x_1 + a_3 r_1 m_b y_{21} + a_3 w r_2 x_2 + a_3 w r_2 m_b y_{22} \\ &\quad + (1 + 10^{k_2} a_1 y_{11} + 10^{k_2} a_1 w y_{12} + 10^{k_2} a_3 r_1 y_{11} + 10^{k_2} a_3 w r_2 y_{12}) \alpha_1 \\ &\quad + (a_1 y_{11} + a_1 w y_{12} + a_3 r_1 y_{11} + a_3 w r_2 y_{12}) \alpha_2. \end{aligned} \qquad (15)$$

This comes from equation (13).

When equations (14) and (15) are linearly independent, then the decryption oracle rejects the invalid ciphertext $(u_1', u_2', e', v')$ except with negligible probability (for the same reasons discussed in the proof of Lemma 4.1). To examine the conditions under which these equations are linearly dependent, we can computes the following determinant:

$$\begin{vmatrix} 1 + 10^{k_2}(r_1 y_{11} + r_2 w y_{12}) & r_1 y_{11} + r_2 w y_{12} \\ 1 + 10^{k_2}(a_1 y_{11} + a_1 w y_{12} + a_3 r_1 y_{11} + a_3 w r_2 y_{12}) & a_1 y_{11} + a_1 w y_{12} + a_3 r_1 y_{11} + a_3 w r_2 y_{12} \end{vmatrix}$$

$$= a_1 \log d_1 + (a_3 - 1) \log \delta_1, \qquad (16)$$

where $\delta_1 = {u_1}^{y_{11}} {u_2}^{y_{12}}$.

From equation (16) it follows that, unless $a_1 = 0$ and $a_3 = 1$, it is difficult for the $Adv$ to generate invalid ciphertext $(u_1', u_2', e', v')$ for which equations (14) and (15) are linearly dependent, because $\delta_1$ can take any value of $G$ and the $Adv$ cannot know the value of $\delta_1$. When $a_1 = 0$ and $a_3 = 1$, we have $u_1' = u_1$ and $u_2' = u_2$. On the other hand, $e = e'$ is induced from $\alpha = \alpha'$ and $m_b = m'$. So we have $v = v'$. Therefore, we finally have $(u_1, u_2, e, v) = (u_1', u_2', e', v')$. This is contrary to the assumption $(u_1, u_2, e, v) \neq (u_1', u_2', e', v')$.

## 5 Simple Implementation and Variations

This section gives an actual example how $G$, $G'$ and $\pi$ are chosen in the key generation of our basic scheme: Choose a large prime $p$ and a prime $q$ such that $q$ divides $p-1$. Then set $G' = \mathbb{Z}_p$ and let $G$ be the subgroup of order $q$ in $\mathbb{Z}_p$. And make $\pi$ an identity map from $X_1 \times X_2 \times M$ into $\mathbb{Z}_p$ in which $(x_1, x_2, m)$ corresponds to $x_1||x_2||m$. The message space $M$ is a finite set consisting of positive integers, and for any $x_1 \in X_1$, $x_2 \in X_2$ and $m \in M$ it must be $x_1||x_2||m < p$.

Using the idea of basic scheme described in this paper, we can make a converting method that can convert any encryption scheme (secret-key encryption scheme or public-key encryption scheme) that is IND-CPA or NM-CPA to one that is IND-CCA2. The details of the converting method are omitted here because of space limitations.

## 6 Performance

This section evaluates the efficiency of the encryption and the decryption in terms of the computational cost of the modular multiplications. The basic scheme is compared here with the hash-free variant of the Cramer-Shoup scheme because that is the most efficient of the previous public-key encryption schemes that are IND-CCA2 under a single assumption.

The modulus $p$ for both the new scheme and the hash-free variant of the Cramer-Shoup scheme is assumed to be 1024 bits, and $q$ is assumed to be 256 bits. In the standard binary method [10], a modular exponentiation with exponent $x$ ($k$ bits) requires an average of $3k/2$ modular multiplications. This is easily generalized to the extended binary method in which computing $\prod_{i=1}^{t} g_i^{x_i} \bmod n$ requires an average of $(2^{t+1}-1)k/2^t$ modular multiplications, provided that $2^t - t - 1$ elements of $\mathbb{Z}_p$ are pre-computed and recorded. Note that the standard binary method requires no pre-computation, but the extended binary method requires substantial pre-computation when $t$ is large.

Since public-key encryption schemes are normally used to distribute the secret keys of symmetric ciphers, assume that the size of a plaintext is at most 256 bits.

First, the efficiency of the encryption procedures in these schemes is evaluated. The encryption procedure of the new scheme requires about 2500 ($= 128 \times 3/2 + 256 \times 3/2 \times 6 + 4$) modular multiplications when the standard binary method is used. And when the extended binary method is used (and the size of both parameters $\alpha_1$ and $\alpha_2$ is 128 bits), the encryption requires about 1649 ($= 256 \times 3/2 \times 3 + 256 \times 31/16 + 1$) modular multiplications, provided that 11 elements of $\mathbb{Z}_p$ (= 11264 bits) are pre-computed and recorded. The encryption procedure of the hash-free variant of the Cramer-Shoup scheme requires about 6157 ($= 256 \times 3/2 \times 16 + 13$) modular multiplications when the standard binary method is used and requires about 1664 ($= 256 \times 3/2 \times 3 + 256 \times 16383/8192 + 1$) modular multiplications when the extended binary method is used, provided that 8178 elements of $\mathbb{Z}_p$ (= 8374272 bits) are pre-computed and recorded.

Thus when the binary extended method is used, one can not see a substantial difference between the numbers of the modular multiplications required in the two schemes, but there is a substantial difference in the number of the pre-computed elements.

Next, the efficiency of the decryption procedures of these schemes is evaluated. The extended binary method is used here, since the number of the pre-computation is very small in both schemes (5 elements in $\mathbb{Z}_p$ are pre-computed in the new scheme, and 1 element is pre-computed in the hash-free variant of the Cramer-Shoup scheme). The decryption procedure of the new scheme requires about 865 ($= 256 \times 3/2 + 256 \times 15/8 + 1$) modular multiplications and the decryption procedure of the hash-free variant of the Cramer-Shoup scheme requires about 833 ($= 256 \times 3/2 + 256 \times 7/4 + 1$) modular multiplications.

We can see from the above that the decryption speeds of the new scheme and the hash-free variant of the Cramer-Shoup scheme take almost same amount of time but the encryption procedure of the new scheme is more efficient than that of the hash-free variant of the Cramer-Shoup scheme.

## 7 Acknowledgement

We would like to thank Hisayoshi Satoh for his very useful comments on the extended binary method.

## References

[1] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology – Crypto'98*, LNCS 1462, pages 26–45. Springer-Verlag, 1998.

[2] M. Bellare and P. Rogaway. Random oracles are practical – a paradigm for designing efficient protocols. In *First ACM Conference on Computer and Communications Security*, pages 62–73, 1993.

[3] D. Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS#1. In *Advances in Cryptology – Crypto'98*, LNCS 1462, pages 1–12. Springer-Verlag, 1998.

[4] M. Blum and S. Goldwasser. An efficient probabilistic public-key encryption scheme which hides all partial information. In *Advances in Cryptology – Crypto'84*, LNCS 196, pages 289–302. Springer-Verlag, 1985.

[5] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Advances in Cryptology – Crypto'98*, LNCS 1462, pages 13–25. Springer-Verlag, 1998.

[6] D. Dolve, C. Dwork, and M. Naor. Non-malleable cryptography. In *Proceedings of the 23rd Annual Symposium on Theory of Computing*, pages 542–552. ACM, 1991.

[7] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *IEEE Trans. Information Theory*, number 4 in IT-31, pages 469–472, 1985.

[8] S. Goldwasser and M. Bellare. Lecture notes on cryptography. http:/www-cse.ucsd.edu/users/ mihir/, 1997.

[9] S. Goldwasser and S. Micali. Probabilistic encryption. In *Journal of Computer and System Sciences*, volume 28(2), pages 270–299, 1984.

[10] D. E. Knuth. *The Art of Computer Programming.* Addison-Wesley, 1981.

[11] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the 22nd Annual Symposium on Theory of Computing*, pages 427–437. ACM, 1990.

[12] T. Okamoto and S. Uchiyama. A new public-key cryptosystem as secure as factoring. In *Advances in Cryptology – Eurocrypt'98*, LNCS 1403, pages 308–318. Springer-Verlag, 1998.

[13] C. Rackoff and D. Simon. Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Advances in Cryptology – Crypto'91*, LNCS 576, pages 433–444. Springer-Verlag, 1991.

[14] T. Schweinberger and V. Shoup. *ACE Encrypt: The Advanced Cryptographic Engine's Public Key Encryption Scheme.* IBM, 2000. http:/www.zurich.ibm.com/Technology/Security/ extern/ace.

[15] V. Shoup. Lower bounds for discrete logarithms and related problems. In *Advances in Cryptology – Eurocrypt'97*, LNCS 1233, pages 256–266. Springer-Verlag, 1997.

[16] Y. Zheng and J. Seberry. Practical approaches to attaining security against adaptive chosen ciphertext attacks. In *Advances in Cryptology – Crypto'92*, LNCS 740, pages 292–304. Springer-Verlag, 1992.