ISSN 1342-2812

Research Reports on Mathematical and Computing Sciences

ElGamal and Cramer-Shoup Variants with Anonymity Using Different Groups
(Extended Abstract)

Ryotaro Hayashi and Keisuke Tanaka

November 2004, C–200

Department of
Mathematical and
Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

ElGamal and Cramer-Shoup Variants with Anonymity Using Different Groups
(Extended Abstract)

Ryotaro Hayashi and Keisuke Tanaka[*]

Dept. of Mathematical and Computing Sciences
Tokyo Institute of Technology
W8-55, 2-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan
{hayashi9, keisuke}@is.titech.ac.jp

November 17, 2004

Abstract

In this paper, we have proposed new variants of the El-Gamal and the Cramer-Shoup encryption schemes. In our schemes, the anonymity property holds even if each user chooses an arbitrary prime q where $|q| = k$ and $p = 2q + 1$ is also prime. More precisely, our El-Gamal variants provide anonymity against the chosen-plaintext attack, and our Cramer-Shoup variants provide anonymity against the adaptive chosen-ciphertext attack. These anonymity properties are proved under a slightly weaker assumption than the DDH assumption. Furthermore, our El-Gamal variants are secure in the sense of IND-CPA, and our Cramer-Shoup variants are secure in the sense of IND-CCA2.

Keywords: encryption, key-privacy, anonymity, ElGamal, Cramer-Shoup

1 Introduction

Bellare, Boldyreva, Desai, and Pointcheval [1] proposed a new security requirement of the encryption schemes called "key-privacy" or "anonymity." It asks that the encryption provide (in addition to privacy of the data being encrypted) privacy of the key under which the encryption was performed.

The anonymous encryption scheme has various applications. For example, anonymous authenticated key exchange protocol such as SKEME (Krawczyk [8]), anonymous credential system (Camenisch and Lysyanskaya [3]), and auction protocols (Sako [10]).

A simple observation that seems to be folklore is that standard RSA encryption, namely, a ciphertext is $x^e \bmod N$ where x is a plaintext and (N, e) is a public key, does not provide anonymity, even when all moduli in the system have the same length. Suppose an adversary knows that the ciphertext y is created under one of two keys (N_0, e_0) or (N_1, e_1), and suppose $N_0 \leq N_1$. If $y \geq N_0$ then the adversary bets it was created under (N_1, e_1), else the adversary bets it was created under (N_0, e_0). It is not hard to see that this attack has non-negligible advantage. To construct the schemes with anonymity, it is necessary that the space of ciphertexts is common to each user.

Recently, three techniques, expanding, repeating, and RSACD, were proposed for RSA-based cryptosystems for obtaining anonymity. With the expanding technique, computing the ciphertext

[*] Supported in part by NTT Information Sharing Platform Laboratories and Grant-in-Aid for Scientific Research, Ministry of Education, Culture, Sports, Science, and Technology, 14780190, 16092206.

and expanding it to the common domain. This technique was proposed by Desmedt [5]. In [6], Galbraith and Mao used this technique for the undeniable signature scheme. In [9], Rivest, Shamir, and Tauman also used this technique for the ring signature scheme. With the repeating technique, repeating the evaluation of the encryption function each time using different randomness until the ciphertext is into the common domain. In [1], Bellare, Boldyreva, Desai, and Pointcheval used this technique for the encryption scheme. The RSACD function was constructed by Hayashi, Okamoto, and Tanaka [7], which has a common domain whose structure is specialized to the RSA function.

In [1], they also proved that the El-Gamal and the Cramer-Shoup encryption schemes provide anonymity when all of the users use a common group. This setting can be considered to be reasonable because the space of the private keys is large when a common group is fixed.

However, it is more flexible that we do not fix a common group but a security parameter for groups. In this paper, we propose new variants of the El-Gamal and the Cramer-Shoup encryption schemes, using the techniques of expanding and repeating used in RSA-based cryptosystems.

In our schemes, the anonymity property holds even if each user chooses an arbitrary prime q where $|q| = k$ and $p = 2q+1$ is also prime. More precisely, our El-Gamal variants provide anonymity against the chosen-plaintext attack, and our Cramer-Shoup variants provide anonymity against the adaptive chosen-ciphertext attack. These anonymity properties are proved under a slightly weaker assumption than the DDH assumption. Furthermore, our El-Gamal variants are secure in the sense of IND-CPA, and our Cramer-Shoup variants are secure in the sense of IND-CCA2.

We show the anonymity property of our schemes by a similar argument as in [1]. The argument in [1] depends heavily on the situation where all of the users employ a common group. Therefore, we cannot straightforwardly apply their argument to our schemes. To prove the anonymity of our schemes, we employ the idea described in [4] by Cramer and Shoup, where we encode the element of QR_p where $p = 2q + 1$ and p, q are prime to that of $\mathbb{Z}_q$. This encoding is applied between the primitive encryption scheme and the expanding / repeating technique, and plays an important role in our schemes.

We also introduce a slightly weaker assumption than the DDH assumption which we call "the paired DDH assumption." It says that it is hard to decide whether $(g_1, g_1^{x_1}, g_1^{y_1}, g_1^{z_1})$ and $(g_2, g_2^{x_1}, g_2^{y_2}, g_2^{z_2})$ are both valid DDH-tuples (i.e. $z_1 = x_1y_1$ and $z_2 = x_2y_2$) or not.

The organization of this paper is as follows. In Section 2, we describe the definitions of the DDH problem and the paired DDH problem. We also review the definitions concerning families of hash functions. In Section 3, we describe the definitions of anonymity for public-key encryption schemes. In Section 4, we show the techniques for obtaining encryption schemes with the anonymity property. We propose the variants of the ElGamal encryption scheme with anonymity in Section 5, and those of the Cramer-Shoup encryption scheme with anonymity in Section 6. We conclude in Section 7.

2 Preliminaries

In this paper, we use the following notations. If A is a probabilistic algorithm, then $A(x_1, x_2, \cdots ; r)$ is the result of running A on inputs $x_1, x_2, \cdots$ and coins r. We let $y \leftarrow A(x_1, x_2, \cdots)$ denote the experiment of picking r at random and letting y be $A(x_1, x_2, \cdots ; r)$. If S is a finite set then $x \overset{R}{\leftarrow} S$ is the operation of picking an element uniformly from S. If α is not an algorithm then $x \leftarrow \alpha$ is a simple assignment statement.

We say the function $\epsilon : \mathbb{N} \to \mathbb{R}^+$ is negligible (in k) if for every constant $c > 0$ there exists an integer k' such that $\epsilon(k) < 1/k^c$ for all $k \geq k'$.

2.1 The Decisional Diffie-Hellman Problem

In this section, we describe the definitions of the DDH problem and the paired DDH problem.

Definition 1 (DDH)**.** *Let $\bar{\mathcal{G}}$ be a prime-order-group generator which takes as input a security parameter k and returns (q, g) where q is a k-bit prime and g is a generator of a cyclic group G_q of order q. Let D be an adversary. We consider the following experiments:*

```
Experiment $\mathbf{Exp}^{\text{ddh-real}}_{\bar{\mathcal{G}},D}(k)$
    $(q, g) \leftarrow \bar{\mathcal{G}}(k)$
    $x, y \xleftarrow{R} \mathbb{Z}_q$
    $X \leftarrow g^x;\ Y \leftarrow g^y;\ T \leftarrow g^{xy}$
    $d \leftarrow D(q, g, X, Y, T)$
    return $d$
```

```
Experiment $\mathbf{Exp}^{\text{ddh-rand}}_{\bar{\mathcal{G}},D}(k)$
    $(q, g) \leftarrow \bar{\mathcal{G}}(k)$
    $x, y, \xleftarrow{R} \mathbb{Z}_q$
    $X \leftarrow g^x;\ Y \leftarrow g^y;\ T \xleftarrow{R} G_q$
    $d \leftarrow D(q, g, X, Y, T)$
    return $d$
```

The advantage of D in solving the Decisional Diffie-Hellman (DDH) problem for $\bar{\mathcal{G}}$ is defined by

$$\mathbf{Adv}^{\text{ddh}}_{\bar{\mathcal{G}},D}(k) = |\Pr[\mathbf{Exp}^{\text{ddh-real}}_{\bar{\mathcal{G}},D}(k) = 1] - \Pr[\mathbf{Exp}^{\text{ddh-rand}}_{\bar{\mathcal{G}},D}(k) = 1]|.$$

We say that the DDH problem for $\bar{\mathcal{G}}$ is hard if the function $\mathbf{Adv}^{\text{ddh}}_{\bar{\mathcal{G}},D}(k)$ is negligible for every algorithm D whose time-complexity is polynomial in k.

The "time-complexity" is the worst case execution time of the experiment plus the size of the code of the adversary, in some fixed RAM model of computation.

We now define the paired DDH problem.

Definition 2 (paired DDH)**.** *Let $\bar{\mathcal{G}}$ be a prime-order-group generator. Let D be an adversary. We consider the following experiments:*

```
Experiment $\mathbf{Exp}^{\text{pddh-real}}_{\bar{\mathcal{G}},D}(k)$
    $(q_0, g_0) \leftarrow \bar{\mathcal{G}}(k);\ x_0, y_0 \xleftarrow{R} \mathbb{Z}_{q_0}$
    $X_0 \leftarrow g_0^{x_0};\ Y_0 \leftarrow g_0^{y_0};\ T_0 \leftarrow g_0^{x_0 y_0}$
    $(q_1, g_1) \leftarrow \bar{\mathcal{G}}(k);\ x_1, y_1 \xleftarrow{R} \mathbb{Z}_{q_1}$
    $X_1 \leftarrow g_1^{x_1};\ Y_1 \leftarrow g_1^{y_1};\ T_1 \leftarrow g_1^{x_1 y_1}$
    $d \leftarrow D((q_0, g_0, X_0, Y_0, T_0),$
            $(q_1, g_1, X_1, Y_1, T_1))$
    return $d$
```

```
Experiment $\mathbf{Exp}^{\text{pddh-rand}}_{\bar{\mathcal{G}},D}(k)$
    $(q_0, g_0) \leftarrow \bar{\mathcal{G}}(k);\ x_0, y_0 \xleftarrow{R} \mathbb{Z}_{q_0}$
    $X_0 \leftarrow g_0^{x_0};\ Y_0 \leftarrow g_0^{y_0};\ T_0 \xleftarrow{R} G_{q_0}$
    $(q_1, g_1) \leftarrow \bar{\mathcal{G}}(k);\ x_1, y_1 \xleftarrow{R} \mathbb{Z}_{q_1}$
    $X_1 \leftarrow g_1^{x_1};\ Y_1 \leftarrow g_1^{y_1};\ T_1 \xleftarrow{R} G_{q_1}$
    $d \leftarrow D((q_0, g_0, X_0, Y_0, T_0),$
            $(q_1, g_1, X_1, Y_1, T_1))$
    return $d$
```

The advantage of D in solving the paired Decisional Diffie-Hellman problem for $\bar{\mathcal{G}}$ is defined by

$$\mathbf{Adv}^{\text{pddh}}_{\bar{\mathcal{G}},D}(k) = |\Pr[\mathbf{Exp}^{\text{pddh-real}}_{\bar{\mathcal{G}},D}(k) = 1] - \Pr[\mathbf{Exp}^{\text{pddh-rand}}_{\bar{\mathcal{G}},D}(k) = 1]|.$$

We say that the paired DDH problem for $\bar{\mathcal{G}}$ is hard if the function $\mathbf{Adv}^{\text{pddh}}_{\bar{\mathcal{G}},D}(k)$ is negligible for every algorithm D whose time-complexity is polynomial in k.

2.2 Families of Hash Functions

In this section, we describe the definitions of families of hash functions, universal one-way, and collision resistant.

Definition 3. *A family of hash functions $\mathcal{H} = (\mathcal{GH}, \mathcal{EH})$ is defined by two algorithms. A probabilistic generator algorithm $\mathcal{GH}$ takes the security parameter k as input and returns a key K. A deterministic evaluation algorithm $\mathcal{EH}$ takes the key K and a string $M \in \{0,1\}^*$ and returns a string $\mathcal{EH}_K(M) \in \{0,1\}^{k-1}$.*

Definition 4. *Let $\mathcal{H} = (\mathcal{GH}, \mathcal{EH})$ be a family of hash functions and let $C = (C_1, C_2)$ be an adversary. We consider the following experiment:*

```
Experiment $\mathbf{Exp}^{\mathrm{uow}}_{\mathcal{H},C}(k)$
    $(x_0, \mathsf{si}) \leftarrow C_1(k);\ K \leftarrow \mathcal{GH}(k);\ x_1 \leftarrow C_2(K, x_0, \mathsf{si})$
    if $((x_0 \neq x_1) \wedge (\mathcal{EH}_K(x_0) = \mathcal{EH}_K(x_1)))$ then return 1 else return 0
```

Note that si *is the state information. We define the advantage of C via*

$$\mathbf{Adv}^{\mathrm{uow}}_{\mathcal{H},C}(k) = \Pr[\mathbf{Exp}^{\mathrm{uow}}_{\mathcal{H},C}(k) = 1].$$

We say that the family of hash functions $\mathcal{H}$ is universal one-way if $\mathbf{Adv}^{\mathrm{uow}}_{\mathcal{H},C}(k)$ is negligible for every algorithm C whose time-complexity is polynomial in k.

Definition 5. *Let $\mathcal{H} = (\mathcal{GH}, \mathcal{EH})$ be a family of hash functions and let C be an adversary. We consider the following experiment:*

```
Experiment $\mathbf{Exp}^{\mathrm{cr}}_{\mathcal{H},C}(k)$
    $K \leftarrow \mathcal{GH}(k);\ (x_0, x_1) \leftarrow C(K)$
    if $((x_0 \neq x_1) \wedge (\mathcal{EH}_K(x_0) = \mathcal{EH}_K(x_1)))$ then return 1 else return 0
```

We define the advantage of C via

$$\mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},C}(k) = \Pr[\mathbf{Exp}^{\mathrm{cr}}_{\mathcal{H},C}(k) = 1].$$

We say that the family of hash functions $\mathcal{H}$ is collision-resistant if $\mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},C}(k)$ is negligible for every algorithm C whose time-complexity is polynomial in k.

Note that if $\mathcal{H}$ is collision resistant then $\mathcal{H}$ is universal one-way.

3 Anonymity for Encryption Schemes

3.1 Definitions

The classical security requirements of public-key encryption schemes, for example indistinguishability or non-malleability under the chosen-ciphertext attack, provide privacy of the encryption data. In [1], Bellare, Boldyreva, Desai, and Pointcheval proposed a new security requirement of encryption schemes called "key-privacy" or "anonymity." It asks that the encryption provide (in addition to privacy of the data being encrypted) privacy of the key under which the encryption was performed. In a heterogeneous public-key environment, encryption will probably fail to be anonymous for trivial reasons. For example, different users might be using different cryptosystems, or, if the same cryptosystem, have keys of different lengths. In [1], a public-key encryption scheme with common-key generation is described as follows.

Definition 6. *A public-key encryption scheme with common-key generation $\mathcal{PE} = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of four algorithms. The common-key generation algorithm $\mathcal{G}$ takes as input some security parameter k and returns some common key I. The key generation algorithm $\mathcal{K}$ is a randomized algorithm that takes as input the common key I and returns a pair (pk, sk) of keys, the public key and a matching secret key. The encryption algorithm $\mathcal{E}$ is a randomized algorithm that takes the public key pk and a plaintext x to return a ciphertext y. The decryption algorithm $\mathcal{D}$ is a deterministic algorithm that takes the secret key sk and a ciphertext y to return the corresponding plaintext x or a special symbol $\perp$ to indicate that the ciphertext was invalid.*

In [1], they formalized the property of "key-privacy." This can be considered under either the chosen-plaintext attack or the chosen-ciphertext attack, yielding two notions of security, IK-CPA and IK-CCA. (IK means "indistinguishability of keys.")

Definition 7 (IK-CPA, IK-CCA [1])**.** *Let $\mathcal{PE} = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. Let $b \in \{0,1\}$ and $k \in \mathbb{N}$. Let $A_{\text{cpa}} = (A^1_{\text{cpa}}, A^2_{\text{cpa}})$, $A_{\text{cca}} = (A^1_{\text{cca}}, A^2_{\text{cca}})$ be adversaries that run in two stages and where A_{cca} has access to the oracles $\mathcal{D}_{sk_0}(\cdot)$ and $\mathcal{D}_{sk_1}(\cdot)$. Note that* si *is the state information. It contains pk_0, pk_1, and so on. For* atk $\in$ {cpa, cca}*, we consider the following experiment:*

```
Experiment $\mathbf{Exp}^{\text{ik-atk-}b}_{\mathcal{PE},A_{\text{atk}}}(k)$
  $I \xleftarrow{R} \mathcal{G}(k)$; $(pk_0, sk_0) \xleftarrow{R} \mathcal{K}(I)$; $(pk_1, sk_1) \xleftarrow{R} \mathcal{K}(I)$
  $(x, \mathsf{si}) \leftarrow A^1_{\text{atk}}(pk_0, pk_1)$; $y \leftarrow \mathcal{E}_{pk_b}(x)$; $d \leftarrow A^2_{\text{atk}}(y, \mathsf{si})$
  return $d$
```

Above it is mandated that A^2_{cca} never queries the challenge ciphertext y to either $\mathcal{D}_{sk_0}(\cdot)$ or $\mathcal{D}_{sk_1}(\cdot)$. For atk $\in$ {cpa, cca}*, we define the advantage via*

$$\mathbf{Adv}^{\text{ik-atk}}_{\mathcal{PE},A_{\text{atk}}}(k) = \left|\Pr[\mathbf{Exp}^{\text{ik-atk-1}}_{\mathcal{PE},A_{\text{atk}}}(k) = 1] - \Pr[\mathbf{Exp}^{\text{ik-atk-0}}_{\mathcal{PE},A_{\text{atk}}}(k) = 1]\right|.$$

The scheme $\mathcal{PE}$ is said to be IK-CPA secure (respectively IK-CCA secure) if the function $\mathbf{Adv}^{\text{ik-cpa}}_{\mathcal{PE},A_{\text{cpa}}}(\cdot)$ (resp. $\mathbf{Adv}^{\text{ik-cca}}_{\mathcal{PE},A_{\text{cca}}}(\cdot)$) is negligible for any adversary A whose time complexity is polynomial in k.

The encryption schemes which provide key-privacy are useful for anonymous authenticated key exchange protocol such as SKEME (Krawczyk [8]), anonymous credential system (Camenisch and Lysyanskaya [3]), auction protocols (Sako [10]), and so on.

4 Techniques for Anonymity

In this section, we describe the techniques for obtaining encryption schemes with the anonymity property.

Consider the encryption function $f : G \to G$. If each user U_i uses a different groups G_i for her encryption scheme and publishes the ciphertext directly, then the scheme does not provide anonymity. The adversary simply checks whether the ciphertext y is in the group G_i, and if $y \notin G_i$ then y was not encrypted by U_i. Hence, to construct the schemes with anonymity, it is necessary that the space of ciphertexts is common to each user.

In this paper, we mainly construct the variants of the Cramer-Shoup schemes which provides anonymity with prime-order groups. In the following, we will concentrate on the case that uses use prime-order groups. In order to construct our scheme, it is necessary that the space of ciphertexts is common to each user who can use a different prime-order group. To archive this, we consider the following two strategies. We assume that each user chooses a prime-order group of order q where $|q| = k$, which is a security parameter.

Strategy 1.

1. Compute a ciphertext c over each user's prime-order group.
2. Encode c to an element $\bar{c} \in \mathbb{Z}_q$ (encoding function).
3. Expand $\bar{c}$ to the common domain (expanding technique).

Strategy 2.

1. Compute a ciphertext c over each user's prime-order group.
2. Encode c to an element $\bar{c} \in \mathbb{Z}_q$ (encoding function).
3. If it is not in the common domain, go back to step 1 (repeating technique).

In the following, we describe the encoding function, and the expanding and repeating techniques.

4.1 The Encoding Function

Generally speaking, it is not easy to encode the elements of a prime-order group of order q to that of $\mathbb{Z}_q$. We employ the idea described in [4] by Cramer and Shoup. We can encode the element of QR_p where $p = 2q + 1$ and p, q are prime to that of $\mathbb{Z}_q$.

Let p be safe prime (i.e. $q = (p - 1)/2$ is also prime) and $QR_p \subset \mathbb{Z}_p^*$ be a group of quadratic residues modulo p. Then we have $|QR_p| = q$ and

$$QR_p = \{1^2 \bmod p,\ 2^2 \bmod p, \cdots,\ q^2 \bmod p\}.$$

It is easy to see that QR_p is a cyclic group of order q, and each $g \in QR_p \backslash \{1\}$ is a generator of QR_p.

We now define a function $F_q : QR_p \to \mathbb{Z}_q$ as

$$F_q(x) = \min \left\{ \pm x^{\frac{p-1}{4}} \bmod p \right\}.$$

Noticing that $\pm\, x^{\frac{p-1}{4}} \bmod p$ are the square roots of x modulo p, the function F_q is bijective and we have

$$F_q^{-1}(y) = y^2 \bmod p.$$

We call the function F_q an *encoding function.* We also define a t*-encoding function* $\bar{F}_{q,t} : (QR_p)^t \to (\mathbb{Z}_q)^t$. $\bar{F}_{q,t}$ takes as input $(x_1, \cdots, x_t) \in (QR_p)^t$ and returns $(y_1, \cdots, y_t) \in (\mathbb{Z}_q)^t$ where $y_i = F_q(x_i)$ for each $i \in \{1, \cdots, t\}$. It is easy to see that $\bar{F}_{q,t}$ is bijective and we can define $\bar{F}_{q,t}^{-1}$.

In the following, we define $\mathcal{Q}$ as a QR-group generator with safe prime which takes as input a security parameter k and returns (q, g) where q is k-bit prime, $p = 2q + 1$ is prime, and g is a generator of a cyclic group QR_p of order q.

4.2 Expanding Technique

In the expanding technique, we expand $\bar{c} \in \mathbb{Z}_q$ to the common domain $\{0, 1\}^{k+k_b}$. In particular, we choose $t \xleftarrow{R} \{0, 1, 2, \cdots, \lfloor (2^{k+k_b} - \bar{c})/q \rfloor\}$ and set $c' \leftarrow \bar{c} + tq$.

We assume that $\bar{c}$ is uniformly chosen from $\mathbb{Z}_q$ where $|q| = k$. Then, for any $c' \in \{0, 1\}^{k+k_b}$, the probability of observing c' (which we denote as $\Pr_{\text{exp}}[c']$) is

$$\frac{1}{2^{k+k_b}} \le \Pr_{\text{exp}}[c'] \le \frac{1}{2^{k+k_b} - 2q}.$$

Therefore

$$\sum_{c' \in \{0,1\}^{k+k_b}} \left| \Pr_{\text{exp}}[c'] - \frac{1}{2^{k+k_b}} \right| \le \frac{1}{2^{k_b - 1}}.$$

Hence, for any q where where $|q| = k$, if c is uniformly chosen from $\mathbb{Z}_q$, then the distribution of the outputs by the expanding technique is statistically indistinguishable from the uniform distribution over $\{0, 1\}^{k+k_b}$. In the following, we set $k_b = 160$.

4.3 Repeating Technique

In the repeating technique, we repeat the evaluation of the encryption until the value is smaller than the smallest prime q of users. If we assume $|q| = k$, the common domain is $\{0, 1\}^{k-1}$.

It is easy to see that for any q where $|q| = k$, if $\bar{c}$ is uniformly chosen from $\mathbb{Z}_q$, then the distribution of the outputs by the repeating technique is statistically indistinguishable from the uniform distribution over $\{0, 1\}^{k-1}$.

5 Variants of the El-Gamal Encryption Scheme

5.1 The El-Gamal Encryption Scheme

Definition 8. *The El-Gamal encryption scheme $\mathcal{PE}^{\mathsf{EG}} = (\mathcal{G}^{\mathsf{EG}}, \mathcal{K}^{\mathsf{EG}}, \mathcal{E}^{\mathsf{EG}}, \mathcal{D}^{\mathsf{EG}})$ is as follows.*

The common-key generation algorithm $\mathcal{G}^{\mathsf{EG}}$ is a prime-order-group generator which takes as input a security parameter k and returns (q, g) where q is a k-bit prime and g is a generator of a cyclic group G_q of order q. The rest of algorithms are described as follows:

```
Algorithm $\mathcal{K}^{\mathsf{EG}}(q, g)$
  $x \overset{R}{\leftarrow} \mathbb{Z}_q$
  $y \leftarrow g^x$
  return $pk = (q, g, y)$ and
         $sk = (q, g, x)$
```

```
Algorithm $\mathcal{E}^{\mathsf{EG}}_{pk}(m)$
  $r \overset{R}{\leftarrow} \mathbb{Z}_q$
  $c_1 \leftarrow g^r$
  $c_2 \leftarrow m \cdot y^r$
  return $(c_1, c_2)$
```

```
Algorithm $\mathcal{D}^{\mathsf{EG}}_{sk}(c_1, c_2)$
  $m \leftarrow c_2 \cdot c_1^{-x}$
  return $m$
```

The El-Gamal encryption scheme is secure in the sense of IND-CPA if the DDH problem is hard for $\mathcal{G}^{\mathsf{EG}}$. Bellare, Boldyreva, Desai, and Pointcheval [1] proved that the El-Gamal encryption scheme is secure in the sense of IK-CPA if the DDH problem is hard.

We note that in this scheme, each user uses a *common* k-bit prime q and a corresponding group G_q for obtaining the anonymity property.

In the following, we propose two variants of El-Gamal encryption schemes. In our schemes, the anonymity property holds even if each user chooses an arbitrary prime q where $|q| = k$ and $p = 2q + 1$ is also prime, and uses a group of quadratic residues modulo p.

Note that in the our schemes we employ the techniques for anonymity in Section 4.

5.2 Our ElGamal Variant with Expanding

Definition 9. *Our ElGamal variant with expanding $\mathcal{PE}^{\mathsf{MEG}} = (\mathcal{G}^{\mathsf{EGE}}, \mathcal{K}^{\mathsf{EGE}}, \mathcal{E}^{\mathsf{EGE}}, \mathcal{D}^{\mathsf{EGE}})$ is as follows. The common-key generation algorithm $\mathcal{G}^{\mathsf{EGE}}$ takes a security parameter k and returns k. The rest of the algorithms are described as follows:*

```
Algorithm $\mathcal{K}^{\mathsf{EGE}}(k)$
  $(q, g) \leftarrow \mathcal{Q}(k)$;  $((q, g, y), (q, g, x)) \leftarrow \mathcal{K}^{\mathsf{EG}}(q, g)$
  return $pk = (q, g, y)$ and $sk = (q, g, x)$
```

```
Algorithm $\mathcal{E}^{\mathsf{EGE}}_{pk}(m)$
  $(c_1, c_2) \leftarrow \mathcal{E}^{\mathsf{EG}}_{pk}(m)$
  $(\bar{c}_1, \bar{c}_2) \leftarrow \bar{F}_{q,2}(c_1, c_2)$
  $t_1 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor (2^{k+160} - \bar{c}_1)/q \rfloor\}$
  $t_2 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor (2^{k+160} - \bar{c}_2)/q \rfloor\}$
  $c'_1 \leftarrow \bar{c}_1 + t_1 q$;  $c'_2 \leftarrow \bar{c}_2 + t_2 q$
  return $(c'_1, c'_2)$
```

```
Algorithm $\mathcal{D}^{\mathsf{EGE}}_{sk}(c'_1, c'_2)$
  $\bar{c}_1 \leftarrow c'_1 \bmod p$;  $\bar{c}_2 \leftarrow c'_2 \bmod p$
  $(c_1, c_2) \leftarrow \bar{F}^{-1}_{q,2}(\bar{c}_1, \bar{c}_2)$
  $m \leftarrow \mathcal{D}^{\mathsf{EG}}_{sk}(c_1, c_2)$
  return $m$
```

In order to prove that our ElGamal variant with expanding is secure in the sense of IK-CPA and IND-CPA, we need the restriction as follows.

We define the set of ciphertexts $EC((c'_1, c'_2), pk)$ called "equivalence class" as

$$EC((c'_1, c'_2), pk) = \{(\check{c}_1, \check{c}_2) \in (\{0,1\}^{k+160})^2 | \check{c}_1 \bmod q = c'_1 \wedge \check{c}_2 \bmod q = c'_2\}.$$

If (c'_1, c'_2) is a ciphertext of m under $pk = (q, g, y)$, then any element $(c''_1, c''_2) \in EC((c'_1, c'_2), pk)$ is also a ciphertext of m under pk. Therefore, if (c'_1, c'_2) is a challenge ciphertext and the adversary makes a query $(c''_1, c''_2) \in EC((c'_1, c'_2), pk)$ to the decryption oracle $\mathcal{D}_{sk}$, the adversary can get the plaintext of the challenge.

To prevent this attack, we add some natural restriction to the adversaries in the definitions of IK-CCA. That is, it is mandated that the adversary never queries either $(c''_1, c''_2) \in EC((c'_1, c'_2), pk_0)$ to D_{sk_0} or $(c''_1, c''_2) \in EC((c'_1, c'_2), pk_1)$ to D_{sk_1}.

Similarly, in order to prove that our ElGamal variant with expanding is secure in the sense of IND-CPA, we need the same restriction. That is, in the definition of IND-CPA, it is mandated that the adversary never queries $(c''_1, c''_2) \in EC((c'_1, c'_2), pk)$ to D_{sk}.

We think these restrictions are natural and reasonable. Actually, in the case of undeniable and confirmer signature schemes, Galbraith and Mao [6] defined the anonymity on undeniable signature schemes with the equivalence class.

Noticing the equivalence class, we can prove that our ElGamal variant with expanding is secure in the sense of IND-CPA if the DDH problem for $\mathcal{Q}$ is hard. More precisely, we can prove that if there exists a CPA-adversary $A = (A_1, A_2)$ attacking the indistinguishability of our ElGamal variant with expanding with advantage ϵ, then there exists a CPA-adversary $B = (B_1, B_2)$ attacking indistinguishability of the original ElGamal encryption scheme with the same advantage ϵ.

The proof of the following theorem is in Appendix A.

Theorem 1. *Our ElGamal variant with expanding is secure in the sense of IK-CPA if the paired DDH problem for $\mathcal{Q}$ is hard.*

5.3 Our ElGamal Variant with Repeating

Definition 10. *Our ElGamal variant with repeating $\mathcal{PE}^{\mathsf{EGR}} = (\mathcal{G}^{\mathsf{EGR}}, \mathcal{K}^{\mathsf{EGR}}, \mathcal{E}^{\mathsf{EGR}}, \mathcal{D}^{\mathsf{EGR}})$ is as follows. The common-key generation algorithm $\mathcal{G}^{\mathsf{EGR}}$, and the key generation algorithm $\mathcal{K}^{\mathsf{EGR}}$ are the same as those for our ElGamal variant with expanding. The rest of the algorithms are described as follows:*

```
Algorithm $\mathcal{E}_{pk}^{\mathsf{EGR}}(m)$
  $ctr = -1$
  repeat
    $ctr \leftarrow ctr + 1$
    $(c_1, c_2) \leftarrow \mathcal{E}_{pk}^{\mathsf{EG}}(m)$
    $(\bar{c}_1, \bar{c}_2) \leftarrow F_{q,2}(c_1, c_2)$
  until $((\bar{c}_1, \bar{c}_2 < 2^{k-1}) \vee (ctr = k))$
  return $(\bar{c}_1, \bar{c}_2)$
```

```
Algorithm $\mathcal{D}_{sk}^{\mathsf{EGR}}(\bar{c}_1, \bar{c}_2)$
  $(c_1, c_2) \leftarrow \bar{F}_{q,2}^{-1}(\bar{c}_1, \bar{c}_2)$
  $m \leftarrow \mathcal{D}_{sk}^{\mathsf{EG}}(c_1, c_2)$
  return $m$
```

We can easily prove that our ElGamal variant with repeating is secure in the sense of IND-CPA if the DDH problem for $\mathcal{Q}$ is hard. More precisely, we can prove that if there exists a CPA-adversary $A = (A_1, A_2)$ attacking the indistinguishability of our ElGamal variant with repeating with advantage ϵ, then there exists a CPA-adversary $B = (B_1, B_2)$ attacking the indistinguishability of the original ElGamal encryption scheme with advantage greater than $\epsilon/4$.

Noticing that the space of valid ciphertext changes, the proof of the following theorem is similar to that for our ElGamal variant with expanding.

Theorem 2. *Our ElGamal variant with repeating is secure in the sense of IK-CPA if the paired DDH problem for $\mathcal{Q}$ is hard.*

5.4 The Comparison

We show the number of modular exponentiations to encrypt and decrypt, the size of ciphertexts, and the number of random bits to encrypt in Figure 1. For fairness, we assume that the orig-

	Expanding	Repeating	Original
# of mod. exp. to encrypt (average / worst)	2 / 2	3 / $2k$	2 / 2
# of mod. exp. to decrypt	1	1	1
size of ciphertexts	$2(k+160)$	$2(k-1)$	$2(k+1)$
# of random bits to encrypt (average / worst)	$k+320$ / $k+320$	$1.5k$ / k^2	k / k

Figure 1: The comparison of the ElGamal encryption scheme and its variants

inal ElGamal scheme employs $\mathcal{Q}$ as the prime-order-group generator. We also assume that q is uniformly distributed over $(2^{k-1}, 2^k)$.

6 Variants of the Cramer-Shoup Encryption Scheme

6.1 The Cramer-Shoup Encryption Scheme

Definition 11. *The Cramer-Shoup Encryption Scheme* $\mathcal{CS} = (\mathcal{G}^{\mathsf{CS}}, \mathcal{K}^{\mathsf{CS}}, \mathcal{E}^{\mathsf{CS}}, \mathcal{D}^{\mathsf{CS}})$ *is defined as follows. Note that* $\bar{\mathcal{G}}$ *is a prime-order-group generator and* $\mathcal{H} = (\mathcal{GH}, \mathcal{EH})$ *is a family of hash functions.*

```
Algorithm $\mathcal{G}^{\mathsf{CS}}(k)$
  $(q,g) \leftarrow \bar{\mathcal{G}}(k)$; $g_1 \leftarrow g$; $g_2 \overset{R}{\leftarrow} G_q$; $K \leftarrow \mathcal{GH}(k)$; return $(q, g_1, g_2, K)$
```

```
Algorithm $\mathcal{K}^{\mathsf{CS}}(q, g_1, g_2, K)$
  $x_1, x_2, y_1, y_2, z \overset{R}{\leftarrow} \mathbb{Z}_q$
  $c \leftarrow g_1^{x_1} g_2^{x_2}$; $d \leftarrow g_1^{y_1} g_2^{y_2}$
  $h \leftarrow g_1^{z}$
  $pk \leftarrow (g_1, g_2, c, d, h, K)$
  $sk \leftarrow (x_1, x_2, y_1, y_2, z)$
  return $(pk, sk)$
```

```
Algorithm $\mathcal{E}^{\mathsf{CS}}_{pk}(M)$
  $r \overset{R}{\leftarrow} \mathbb{Z}_q$
  $u_1 \leftarrow g_1^r$; $u_2 \leftarrow g_2^r$
  $e \leftarrow h^r M$
  $\alpha \leftarrow \mathcal{EH}_K(u_1, u_2, e)$
  $v \leftarrow c^r d^{r\alpha}$
  return $(u_1, u_2, e, v)$
```

```
Algorithm $\mathcal{D}^{\mathsf{CS}}_{sk}(u_1, u_2, e, v)$
  $\alpha \leftarrow \mathcal{EH}_K(u_1, u_2, e)$
  if $(u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = v)$
    then $M \leftarrow e/u_1^z$
  else $M \leftarrow \perp$
  return $M$
```

Cramer and Shoup [4] proved that the Cramer-Shoup encryption scheme is secure in the sense of IND-CCA2 assuming that $\mathcal{H}$ is universal one-way and the DDH problem for $\bar{\mathcal{G}}$ is hard. Bellare, Boldyreva, Desai, and Pointcheval [1] proved that the Cramer-Shoup encryption scheme is secure in the sense of IK-CCA assuming that $\mathcal{H}$ is collision resistant and the DDH problem is hard for $\bar{\mathcal{G}}$.

We note that in this scheme, each user uses a *common* k-bit prime q and a corresponding group G_q for obtaining the anonymity property.

In the following, we propose two variants of the Cramer-Shoup encryption scheme. In our schemes, the anonymity property holds even if each user chooses an arbitrary prime q where $|q| = k$ and $p = 2q + 1$ is also prime, and uses a group of quadratic residues modulo p.

Note that in the our schemes we employ the techniques for anonymity in Section 4.

6.2 Our Cramer-Shoup Variant with Expanding

Definition 12. *Our Cramer-Shoup Variant* $\mathcal{PE}^{\mathsf{CSE}} = (\mathcal{G}^{\mathsf{CSE}}, \mathcal{K}^{\mathsf{CSE}}, \mathcal{E}^{\mathsf{CSE}}, \mathcal{D}^{\mathsf{CSE}})$ *is as follows. The common-key generation algorithm* $\mathcal{G}^{\mathsf{CSE}}$ *takes a security parameter* k *and returns* k*. The rest of* *the algorithms are described as follows. Note that $\mathcal{Q}$ is a QR-group generator with safe prime.*

```
Algorithm $\mathcal{K}^{\mathsf{CSE}}(k)$
  $(q, g) \leftarrow \mathcal{Q}(k);\ g_1 \leftarrow g;\ g_2 \overset{R}{\leftarrow} G_q;\ K \leftarrow \mathcal{GH}(k)$
  $((q, g_1, g_2, c, d, h, K), (x_1, x_2, y_1, y_2, z)) \leftarrow \mathcal{K}^{\mathsf{CS}}(q, g_1, g_2, K)$
  return $pk = (q, g_1, g_2, c, d, h, K)$ and $sk = (x_1, x_2, y_1, y_2, z)$
```

```
Algorithm $\mathcal{E}^{\mathsf{CSE}}_{pk}(m)$
  $(u_1, u_2, e, v) \leftarrow \mathcal{E}^{\mathsf{CS}}_{pk}(m)$
  $(\bar{u}_1, \bar{u}_2, \bar{e}, \bar{v}) \leftarrow F_{q,4}(u_1, u_2, e, v)$
  $t_1 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{u}_1)/q\rfloor\}$
  $t_2 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{u}_2)/q\rfloor\}$
  $t_3 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{e})/q\rfloor\}$
  $t_4 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{v})/q\rfloor\}$
  $c'_1 \leftarrow \bar{c}_1 + t_1 q;\ c'_2 \leftarrow \bar{c}_2 + t_2 q$
  $e' \leftarrow \bar{e} + t_3 q;\ v' \leftarrow \bar{v} + t_4 q$
  return $(u'_1, u'_2, e', v')$
```

```
Algorithm $\mathcal{D}^{\mathsf{CSE}}_{sk}(u'_1, u'_2, e', v')$
  $\bar{u}_1 \leftarrow u'_1 \bmod p;\ \bar{u}_2 \leftarrow u'_2 \bmod p$
  $\bar{e} \leftarrow e' \bmod p;\ \bar{v} \leftarrow v' \bmod p$
  $(u_1, u_2, e, v) \leftarrow \bar{F}^{-1}_{q,4}(\bar{u}_1, \bar{u}_2, \bar{e}, \bar{v})$
  $m \leftarrow \mathcal{D}^{\mathsf{CS}}_{sk}(u_1, u_2, e, v)$
  return $m$
```

In order to prove that our Cramer-Shoup variant with expanding is secure in the sense of IK-CCA and IND-CCA2, we need to add restrictions similar to those for our ElGamal variant with expanding. We define the equivalence class for our Cramer-Shoup variant with expanding as follows:

$$\begin{aligned} EC((u'_1, u'_2, e', v'), pk) = \{(\check{u}'_1, \check{u}'_2, \check{e}', \check{v}') \in (\{0,1\}^{k+160})^4 |\\ \check{u}'_1 \bmod q = u'_1 \wedge \check{u}'_2 \bmod q = u'_2 \wedge \check{e}' \bmod q = e' \wedge \check{v}'_1 \bmod q = v'\} \end{aligned}$$

Noticing the equivalence class, we can prove that our Cramer-Shoup variant with expanding is secure in the sense of IND-CCA2 if the DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is universal one-way. More precisely, we can prove that if there exists a CCA2-adversary $A = (A_1, A_2)$ attacking the indistinguishability of our Cramer-Shoup variant with expanding with advantage ϵ, then there exists a CCA2-adversary $B = (B_1, B_2)$ attacking the indistinguishability of the original Cramer-Shoup encryption scheme with the same advantage ϵ.

The proof of the following theorem is in Appendix B.

Theorem 3. *Our Cramer-Shoup variant with expanding is secure in the sense of IK-CCA if the paired DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is collision resistant.*

6.3 Our Cramer-Shoup Variant with Repeating

Definition 13. *Our Cramer-Shoup variant with repeating $\mathcal{PE}^{\mathsf{CSR}} = (\mathcal{G}^{\mathsf{CSR}}, \mathcal{K}^{\mathsf{CSR}}, \mathcal{E}^{\mathsf{CSR}}, \mathcal{D}^{\mathsf{CSR}})$ is as follows. The common-key generation algorithm $\mathcal{G}^{\mathsf{CSR}}$, and the key generation algorithm $\mathcal{K}^{\mathsf{CSR}}$ are the same as those for our Cramer-Shoup variant with expanding. The rest of the algorithms are described as follows:*

```
Algorithm $\mathcal{E}^{\mathsf{CSR}}_{pk}(m)$
  $ctr = -1$
  repeat
    $ctr \leftarrow ctr + 1$
    $(u_1, u_2, e, v) \leftarrow \mathcal{E}^{\mathsf{CS}}_{pk}(m)$
    $(\bar{u}_1, \bar{u}_2, \bar{e}, \bar{v}) \leftarrow F_{q,4}(u_1, u_2, e, v)$
  until $((\bar{u}_1, \bar{u}_2, \bar{e}, \bar{v} < 2^{k-1}) \vee (ctr = k))$
  return $(\bar{u}_1, \bar{u}_2, \bar{e}, \bar{v})$
```

```
Algorithm $\mathcal{D}^{\mathsf{CSR}}_{sk}(\bar{u}_1, \bar{u}_2, \bar{e}, \bar{v})$
  $(u_1, u_2, e, v) \leftarrow \bar{F}^{-1}_{q,4}(\bar{u}_1, \bar{u}_2, \bar{e}, \bar{v})$
  $m \leftarrow \mathcal{D}^{\mathsf{CS}}_{sk}(u_1, u_2, e, v)$
  return $m$
```

	Expanding	Repeating	Original [4]
# of mod. exp. to encrypt (average / worst)	5 / 5	7.5 / $5k$	5 / 5
# of mod. exp. to decrypt	3	3	3
size of ciphertexts	$4(k+160)$	$4(k-1)$	$4(k+1)$
# of random bits to encrypt (average / worst)	$k+640$ / $k+640$	$1.5k$ / k^2	k / k

Figure 2: The comparison of the Cramer-Shoup encryption scheme and its variants

We can prove that our Cramer-Shoup variant with repeating is secure in the sense of IND-CCA2 if the DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is universal one-way. More precisely, we can prove that if there exists a CCA2-adversary $A = (A_1, A_2)$ attacking the indistinguishability of our Cramer-Shoup variant with repeating with advantage ϵ, then there exists a CCA2-adversary $B = (B_1, B_2)$ attacking the indistinguishability of the original Cramer-Shoup encryption scheme with advantage greater than $\epsilon/16$.

Noticing that the space of valid ciphertexts changes, the proof of the following theorem is similar to that for our Cramer-Shoup variant with expanding.

Theorem 4. *Our Cramer-Shoup variant with repeating is secure in the sense of IK-CCA if the paired DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is collision resistant.*

6.4 The Comparison

We show the number of modular exponentiations to encrypt and decrypt, the size of ciphertexts, and the number of random bits to encrypt in Figure 2. For fairness, we assume that the original Cramer-Shoup scheme employs $\mathcal{Q}$ as the prime-order-group generator. We also assume that q is uniformly distributed over $(2^{k-1}, 2^k)$.

7 Concluding Remarks

In this paper, we have proposed new variants of the El-Gamal and the Cramer-Shoup encryption schemes. In our schemes, the anonymity property holds even if each user chooses an arbitrary prime q where $|q| = k$ and $p = 2q + 1$ is also prime. More precisely, our El-Gamal variants provide anonymity against the chosen-plaintext attack, and our Cramer-Shoup variants provide anonymity against the adaptive chosen-ciphertext attack. These anonymity properties are proved under a slightly weaker assumption than the DDH assumption. Furthermore, our El-Gamal variants are secure in the sense of IND-CPA, and our Cramer-Shoup variants are secure in the sense of IND-CCA2.

In the scheme with expanding, we can prove anonymity even if each user's q has the different size. In this situation, the security level of anonymity depends on the shortest size of q among the users, and the proof of anonymity is similar to that in the case of the size of q is fixed.

References

[1] Bellare, M., Boldyreva, A., Desai, A., and Pointcheval, D. Key-Privacy in Public-Key Encryption. In Boyd [2], pp. 566–582. Full version of this paper, available via http://www-cse.ucsd.edu/users/mihir/.

[2] Boyd, C., Ed. *Advances in Cryptology – ASIACRYPT 2001* (Gold Coast, Australia, December 2001), vol. 2248 of *Lecture Notes in Computer Science*, Springer-Verlag.

[3] Camenisch, J., and Lysyanskaya, A. Efficient Non-Transferable Anonymous Multi-Show Credential System with Optional Anonymity Revocation. In *Advances in Cryptology – EUROCRYPT 2001* (Innsbruck, Austria, May 2001), B. Pfitzmann, Ed., vol. 2045 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 93–118.

[4] Cramer, R., and Shoup, V. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack. In *Advances in Cryptology – CRYPTO '98* (Santa Barbara, California, USA, August 1998), H. Krawczyk, Ed., vol. 1462 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 13–25.

[5] Desmedt, Y. Securing traceability of ciphertexts: Towards a secure software escrow scheme. In *Advances in Cryptology – EUROCRYPT '95* (Saint-Malo, France, May 1995), L. C. Guillou and J.-J. Quisquater, Eds., vol. 921 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 147–157.

[6] Galbraith, S. D., and Mao, W. Invisibility and Anonymity of Undeniable and Confirmer Signatures. In *Topics in Cryptology – CT-RSA 2003* (San Francisco, CA, USA, April 2003), M. Joye, Ed., vol. 2612 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 80–97.

[7] Hayashi, R., Okamoto, T., and Tanaka, K. An RSA Family of Trap-door Permutations with a Common Domain and its Applications. In *Public Key Cryptography – PKC 2004* (Singapore, March 2004), F. Bao, R. H. Deng, and J. Zhou, Eds., vol. 2947 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 291–304.

[8] Krawczyk, H. SKEME: A Versatile Secure Key Exchange Mechanism for Internet. In *Proceedings of the 1996 Internet Society Symposium on Network and Distributed System Security* (San Diego, CA, USA, February 1996), pp. 114–127.

[9] Rivest, R. L., Shamir, A., and Tauman, Y. How to Leak a Secret. In Boyd [2], pp. 552–565.

[10] Sako, K. An Auction Protocol Which Hides Bids of Losers. In *Public Key Cryptography – PKC 2000* (Melbourne, Victoria, Australia, January 2000), H. Imai and Y. Zheng, Eds., vol. 1751 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 422–432.

A Proof of Theorem 1

We construct a distinguisher D for the paired DDH problem for $\mathcal{Q}$ in Figure 3. In this algorithm, we employ an adversary A attacking the anonymity of our El-Gamal variant with expanding.

Now we analyze D. First we consider $\mathbf{Exp}^{\text{pddh-real}}_{\mathcal{Q},D}(k)$. In this case, for $i \in \{0,1\}$, the inputs X_i, Y_i, T_i to D satisfy $T_i = g_i^{x_i y_i}$ where $X_i = g_i^{x_i}$ and $Y_i = g_i^{y_i}$ for some $x_i, y_i \in \mathbb{Z}_{q_i}$. Thus X_i has the proper distribution of public keys for our El-Gamal variant. Furthermore, the challenge ciphertext has the right form under the public key pk_b. Hence,

$$\Pr[\mathbf{Exp}^{\text{pddh-real}}_{\mathcal{Q},D}(k) = 1] = \frac{1}{2} + \frac{1}{2}\mathbf{Adv}^{\text{ik-cpa}}_{\mathcal{PE}^{\mathsf{EGE}},A}(k).$$

Now we consider $\mathbf{Exp}^{\text{pddh-rand}}_{\mathcal{Q},D}(k)$. In this case, for $i \in \{0,1\}$, the inputs X_i, Y_i, T_i to D are all independently and uniformly distributed over QR_{p_i}. We have proper distribution public keys for our El-Gamal variant with expanding. However, Y_b, T_b are random elements in QR_{p_b}, and the distribution of (c'_1, c'_2) is statistically indistinguishable from the uniform distribution over

```
Algorithm $D((q_0, g_0, X_0, Y_0, T_0), (q_1, g_1, X_1, Y_1, T_1))$
  $pk_0 \leftarrow (q_0, g_0, X_0)$; $pk_1 \leftarrow (q_1, g_1, X_1)$
  $(m, \mathsf{si}) \leftarrow A^1_{\rm cpa}(pk_0, pk_1)$
  $b \overset{R}{\leftarrow} \{0, 1\}$
  $(\bar{c}_1, \bar{c}_2) \leftarrow \bar{F}_{q_b,2}(Y_b, T_b \cdot m)$
  $t_1 \leftarrow \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{c}_1)/q_b\rfloor\}$;   $t_2 \leftarrow \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{c}_2)/q_b\rfloor\}$
  $c'_1 \leftarrow \bar{c}_1 + t_1 q_b$; $c'_2 \leftarrow \bar{c}_2 + t_2 q_b$
  $d \leftarrow A^2_{\rm cpa}((c'_1, c'_2), \mathsf{si})$
  if $(b = d)$ then return $1$ else return $0$
```

Figure 3: Distinguisher for Theorem 1

$(\{0,1\}^{k+160})^2$. This means that the challenge ciphertext gives A no information about b. Therefore, we have

$$\Pr[\mathbf{Exp}^{\text{pddh-rand}}_{\mathcal{Q},D}(k) = 1] \leq \frac{1}{2} + \frac{1}{2^{2(k-2)}} + \left(\frac{1}{2^{159}}\right)^2.$$

Above, the second term accounts for the maximum probability that the random inputs to D happen to have the distribution of the valid paired-DDH tuple, The last term is the advantage of the decision problem between the distribution of the output by the expanding technique and that of the uniform distribution.

In conclusion, we have

$$\mathbf{Adv}^{\rm ddh}_{\mathcal{G},D}(k) \geq \frac{1}{2}\mathbf{Adv}^{\text{ik-cpa}}_{\mathcal{PE}^{\mathsf{EGE}},A}(k) - \frac{1}{2^{2(k-2)}} - \left(\frac{1}{2^{159}}\right)^2.$$

The time-complexity of D is bounded by $T_A + O(k^3)$ where T_A is the time-complexity of A.

B Proof of Theorem 3

We construct a distinguisher D for the paired DDH problem for $\mathcal{Q}$ in Figure 4. In this algorithm, we employ an adversary A attacking the anonymity of our Cramer-Shoup variant with expanding. First of all, the time-complexity of D is bounded by $T_A + O(k^3)$ where T_A is the time-complexity of A.

Note that if A makes a decryption query $(\tilde{u}'_1, \tilde{u}'_2, \tilde{e}', \tilde{v}')$ to $\mathcal{D}_{sk_i}$ $(i \in \{0,1\})$, D makes its answer $\tilde{m}$ as follows:

```
$(\tilde{u}_1, \tilde{u}_2, \tilde{e}, \tilde{v}) \leftarrow \bar{F}^{-1}_{q_i,4}(\tilde{u}'_1 \bmod q_i, \tilde{u}'_2 \bmod q_i, \tilde{e}' \bmod q_i, \tilde{v}' \bmod q_i)$
$\tilde{\alpha} \leftarrow \mathcal{EH}_{K_i}(\tilde{u}_1, \tilde{u}_2, \tilde{e})$
if $(\tilde{v} = (\tilde{u}_1)^{x_{1,i}+y_{1,i}\tilde{\alpha}} + (\tilde{u}_2)^{x_{2,i}+y_{2,i}\tilde{\alpha}})$ then $\tilde{m} \leftarrow \tilde{e}/(\tilde{u}_1^{z_{1,i}}\tilde{u}_2^{z_{2,i}})$ else $\tilde{m} \leftarrow \perp$
```

Lemma 1.

$$\Pr[\mathbf{Exp}^{\text{pddh-real}}_{\mathcal{Q},D}(k) = 1] = \frac{1}{2} + \frac{1}{2}\mathbf{Adv}^{\text{ik-cca}}_{\mathcal{PE}^{\mathsf{CSE}},A}(k)$$

Lemma 2. *There exists an adversary C attacking the collision-resistance of $\mathcal{H}$ such that*

$$\Pr[\mathbf{Exp}^{\text{pddh-rand}}_{\mathcal{Q},D}(k) = 1] \leq \frac{1}{2} + \frac{q_d(k) + 2}{2^{k-4}} + 2\mathbf{Adv}^{\rm cr}_{\mathcal{H},C}(k),$$

```
Algorithm $D((q_0, g_0, X_0, Y_0, T_0), (q_1, g_1, X_1, Y_1, T_1))$
  for each $j \in \{0, 1\}$ do
    $g_{1,j} \leftarrow g_j$;  $g_{2,j} \leftarrow X_j$;  $u_{1,j} \leftarrow Y_j$;  $u_{2,j} \leftarrow T_j$
    $x_{1,j},\ x_{2,j},\ y_{1,j},\ y_{2,j},\ z_{1,j},\ z_{2,j} \overset{R}{\leftarrow} \mathbb{Z}_{q_j}$
    $c_j \leftarrow (g_{1,j})^{x_{1,j}}(g_{2,j})^{x_{2,j}}$;  $d_j \leftarrow (g_{1,j})^{y_{1,j}}(g_{2,j})^{y_{2,j}}$;  $h_j \leftarrow (g_{1,j})^{z_{1,j}}(g_{2,j})^{z_{2,j}}$
    $K_j \leftarrow \mathcal{GH}(k)$
    $pk_j \leftarrow (g_{1,j}, g_{2,j}, c_j, d_j, h_j, K_j)$
    $sk_j \leftarrow (x_{1,j}, x_{2,j}, y_{1,j}, y_{2,j}, z_{1,j}, z_{2,j})$

  $(m, \mathsf{si}) \leftarrow A^1_{\mathrm{cca}}(pk_0, pk_1)$

  $b \overset{R}{\leftarrow} \{0, 1\}$

  $e \leftarrow (u_{1,b})^{z_{1,b}}(u_{2,b})^{z_{2,b}}m$
  $\alpha \leftarrow \mathcal{EH}_{K_b}(u_{1,b}, u_{2,b}, e)$
  $v \leftarrow (u_{1,b})^{x_{1,b}+\alpha y_{1,b}}(u_{2,b})^{x_{2,b}+\alpha y_{2,b}}$

  $(\bar{u_1}, \bar{u_2}, \bar{e}, \bar{v}) \leftarrow \bar{F}_{q_b,4}(u_{1,b}, u_{2,b}, e, v)$
  $t_1 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{u}_1)/q_b\rfloor\}$;   $t_2 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{u}_2)/q_b\rfloor\}$
  $t_3 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{e})/q_b\rfloor\}$;   $t_4 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{v})/q_b\rfloor\}$
  $u_1' \leftarrow \bar{u_1} + t_1 q_b$;  $u_2' \leftarrow \bar{u_2} + t_2 q_b$;  $e' \leftarrow \bar{e} + t_3 q_b$;  $v' \leftarrow \bar{v} + t_4 q_b$

  $d \leftarrow A^2_{\mathrm{cca}}(u_1', u_2', e', v'), \mathsf{si})$

  if $(b = d)$ then return 1 else return 0
```

Figure 4: Distinguisher for Theorem 3

and whose time-complexity is bounded by that of A plus $O(k^3)$.

Proof of Theorem 3. The statement follows from the above two lemmas. More concretely, we have

$$\mathbf{Adv}^{\mathrm{ddh}}_{\mathcal{Q},D}(k) \geq \frac{1}{2}\mathbf{Adv}^{\text{ik-cca}}_{\mathcal{PE}^{\mathsf{CSE}},A}(k) - \frac{q_d(k)+2}{2^{k-4}} - 2\mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},C}(k).$$

□

B.1 Proof of Lemma 1

To prove this lemma, we show that the view of the adversary A in the experiment $\mathbf{Exp}^{\text{pddh-real}}_{\mathcal{Q},D}(k)$ is the same as that in the actual experiment.

It is easy to see that c_i, d_i have the right distribution. Furthermore, we can rewrite h_i as $h_i = g_{1,i}^{z_{1,i}+\omega_i z_{2,i}}$ where $\omega_i = \log_{g_{1,i}} g_{2,i}$, and $\bar{z}_i = z_{1,i} + \omega_i z_{2,i}$ is uniformly distributed over $\mathbb{Z}_{q_i}$. Therefore, the public-key in the simulation has the right distribution.

We can rewrite the challenge ciphertext $(u_{1,b}, u_{2,b}, e, v)$ which D computes as $e = g_{1,b}^{r_{1,b}\bar{z}_b}M$ and $v = c_b^{r_{1,b}} d_b^{r_{1,b}\alpha_b}$ where $r_{1,b} = \log_{g_{1,b}} u_{1,b}$ and $\alpha_b = \mathcal{EH}_{K_b}(u_{1,b}, u_{2,b}, e)$. Hence, the challenge ciphertext has the right distribution since $r_{1,b}$ is randomly distributed over $\mathbb{Z}_{q_b}$.

Finally, since we can rewrite the response M of the decryption query in the simulation as $M = e/g_{1,i}^{r_{1,i}\bar{z}_i} = e/h_i^{r_{1,i}}$, the output of decryption oracle in the simulation demonstrates that of the actual decryption oracle.

B.2 Proof of Lemma 2

In the experiment $\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k)$, for $i \in \{0,1\}$, we can see the input $(q_i, g_i, X_i, Y_i, T_i)$ as $(q_i, g_{1,i}, g_{2,i},\ u_{1,i}, u_{2,i})$ where $u_{1,i} = (g_{1,i})^{r_{1,i}}$, $u_{2,i} = (g_{2,i})^{r_{2,i}} = (g_{1,i})^{\omega_i r_{1,i}}$, $\omega_i = \log_{g_{1,i}} g_{2,i}$, where $r_{1,i}, r_{2,i}$ are random element in $\mathbb{Z}_{q_i}$. When the adversary A makes a decryption query $(\tilde{u}_1, \tilde{u}_2, \tilde{e}, \tilde{v})$ for $\mathcal{D}_{sk_i}$, we say the ciphertext is invalid when $\log_{g_{1,i}} \tilde{u}_1 \neq \log_{g_{2,i}} \tilde{u}_2$. We define the following events associated to D:

- NR is true if $r_{1,0} = r_{2,0}$ or $r_{1,1} = r_{2,1}$ or $g_{2,0} = 1$ or $g_{2,1} = 1$,
- Inv is true if during the execution of D the adversary A submits an invalid ciphertext to a decryption oracle $\mathcal{D}_{sk_0}$ or $\mathcal{D}_{sk_1}$ and does not get $\perp$.

Lemma 3. $\Pr[\mathsf{NR}] \leq 1/2^{k-3}$.

Lemma 4. *We have*

$$\Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 0 \wedge \neg\mathsf{NR} \wedge \neg\mathsf{Inv}] = \frac{1}{2},$$

$$\Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 1 \wedge \neg\mathsf{NR} \wedge \neg\mathsf{Inv}] = \frac{1}{2}.$$

Lemma 5. *There exists a polynomial-time adversary C such that*

$$\Pr[\mathsf{Inv} | \neg\mathsf{NR}] \leq 2\mathbf{Adv}_{\mathcal{H},C}^{\text{cr}}(k) + \frac{q_d(k)}{2^{k-3}}.$$

Proof of Lemma 2.

$$\begin{aligned}
&\Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1] \\
&= \frac{1}{2}\Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 0] + \frac{1}{2}\Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 1] \\
&\leq \Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 0 \wedge \neg\mathsf{NR} \wedge \neg\mathsf{Inv}] \\
&+ \Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 1 \wedge \neg\mathsf{NR} \wedge \neg\mathsf{Inv}] + \Pr[\mathsf{NR}] + \Pr[\mathsf{Inv}] \\
&\leq \Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 0 \wedge \neg\mathsf{NR} \wedge \neg\mathsf{Inv}] \\
&+ \Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 1 \wedge \neg\mathsf{NR} \wedge \neg\mathsf{Inv}] + 2\Pr[\mathsf{NR}] + \Pr[\mathsf{Inv} | \neg\mathsf{NR}] \\
&\leq \frac{1}{2} + \frac{1}{2^{k-4}} + 2\mathbf{Adv}_{\mathcal{H},C}^{\text{cr}}(k) + \frac{q_d(k)}{2^{k-3}} = \frac{1}{2} + \frac{q_d(k)+2}{2^{k-4}} + 2\mathbf{Adv}_{\mathcal{H},C}^{\text{cr}}(k).
\end{aligned}$$

□

B.2.1 Proof of Lemma 3

We have $\Pr[r_{1,0} = r_{2,0}], \Pr[g_{2,0} = 1] \leq 1/q_0$ and $\Pr[r_{1,1} = r_{2,1}], \Pr[g_{2,1} = 1] \leq 1/q_1$. Since $2^{k-1} < q_0, q_1 < 2^k$, we have $\Pr[\mathsf{NR}] \leq 2/q_0 + 2/q_1 \leq 1/2^{k-3}$.

B.2.2 Proof of Lemma 4

We consider a sample space S from which the random choice is uniformly chosen in the experiment $\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k)$. It consists of the values chosen at random in $\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k)$. We will denote an element of S as

$$\begin{aligned}\vec{s} = (&x_{1,0}, x_{2,0}, y_{1,0}, y_{2,0}, z_{1,0}, z_{2,0}, x_{1,1}, x_{2,1}, y_{1,1}, y_{2,1}, z_{1,1}, z_{2,1}, \\ &g_{1,0}, g_{2,0}, u_{1,0}, u_{2,0}, g_{1,1}, g_{2,1}, u_{1,1}, u_{2,1}, t_1, t_2, t_3, t_4, b).\end{aligned}$$

and S is a subset of

$$\mathbb{Z}_{q_0}^6 \times \mathbb{Z}_{q_1}^6 \times G_{q_0}^4 \times G_{q_1}^4 \times (\{0,1\}^{160})^4 \times \{0,1\}.$$

To evaluate the space S, we consider two spaces $S_0 = \{\vec{s} \in S | b = 0\}$ and $S_1 = \{\vec{s} \in S | b = 1\}$. When $b = 0$ (respectively $b = 1$), the random choice is uniformly chosen from S_0 (resp. S_1) in the Experiment $\mathbf{Exp}^{\text{pddh-rand}}_{\mathcal{Q},D}(k)$. It is clear that $S = S_0 \cup S_1$ and $|S| = |S_0| + |S_1|$ since $S_0 \cap S_1 = \emptyset$. We evaluate S_0, S_1, and S later on.

We let View be the function which has the domain S and associates to any $\vec{s} \in S$ the view of the adversary A in the experiment $\mathbf{Exp}^{\text{pddh-rand}}_{\mathcal{Q},D}(k)$ when the random choice in that experiment is chosen from S. For simplicity, we assume the adversary is deterministic. The argument can simply be made for each choice of its coins. The view then includes the inputs that the adversary receives in its two stages, and the answers to all its oracle queries. The adversary's output is a deterministic function of its view.

Lemma 6. *Fix a specific view $\hat{V}$ of the adversary A simulated by D. Assume that the event $\neg\mathsf{NR} \wedge \neg\mathsf{Inv}$ occurs for this view. Then*

$$\Pr[\mathsf{View} = \hat{V} \mid b = 0] = \Pr[\mathsf{View} = \hat{V} \mid b = 1].$$

Proof of Lemma 4. Lemma 6 means that, if $\neg\mathsf{NR} \wedge \neg\mathsf{Inv}$ occurs then A's view is independent of the hidden bit b. Therefore A can output its guess of b correctly only with the probability 1/2. □

Proof of Lemma 6. For simplicity of the analysis, we will exclude the keys $\hat{K_0}$ and $\hat{K_1}$, because they are clearly independent of the bit b. We do not consider the answers of the decryption oracles to the valid ciphertext queries as a part of the view of the adversary since we show below that this does not give the adversary any information about the hidden bit b. We have

$$\hat{V} = (\hat{g}_{1,0}, \hat{g}_{2,0}, \hat{c}_0, \hat{d}_0, \hat{h}_0, \hat{g}_{1,1}, \hat{g}_{2,1}, \hat{c}_1, \hat{d}_1, \hat{h}_1, \hat{u}'_1, \hat{u}'_2, \hat{e}', \hat{v}').$$

We evaluate $\Pr[\mathsf{View} = \hat{V} \wedge b = 0]$. We first compute $|S_0|$. Note that we now consider the situation that $\neg\mathsf{NR}$. We let $b = 0$ and fix four values $(u'_1, u'_2, e', v') \in (\{0,1\}^{k+160})^4$. Then $t_1 \in \{0, 1, 2, \cdots, \lfloor (2^{k+160} - \bar{u}_1)/q_0 \rfloor\}$ and $\bar{u}_1 \in \mathbb{Z}_{q_0}$ are fixed uniquely since $u'_1 = \bar{u}_1 + t_1 q_0$.

Similarly, $t_2, t_3, t_4, \bar{u_2}, \bar{e}, \bar{v}$ are also fixed uniquely. Furthermore, $u_1 = F^{-1}_{q_0}(\bar{u}_1)$ is fixed uniquely since F is bijective. Similarly, u_2, e, v are fixed uniquely.

We now consider the following equations:

$$\begin{array}{rcll} e & = & u_{1,0}^{z_{1,0}} u_{2,0}^{z_{2,0}} m & \pmod{p_0} \\ v & = & u_{1,0}^{x_{1,0}+\alpha y_{2,0}} u_{2,0}^{x_{2,0}+\alpha y_{2,0}} & \pmod{p_0} \end{array}$$

where $\alpha = \mathcal{EH}(u_1, u_2, e)$. For any $(u_1, u_2, e, v) \in G_{q_0}^4$, the number of vectors $(x_{1,0}, x_{2,0}, y_{1,0}, y_{2,0}, z_{1,0}, z_{2,0})$ which satisfy the above two equations is q_0^4. Furthermore, the other values of $\vec{s}$, that is, $g_{1,0}, g_{1,1}, x_{1,0}, x_{2,0}$, $y_{1,0}, y_{2,0}, z_{1,0}, z_{2,0}, g_{1,0}, g_{1,1}, u_{1,1}, u_{2,1}$, are not restricted in S_0. Therefore,

$$|S_0| = (2^{k+160})^4 \cdot q_0^4 \cdot q_0^2 \cdot q_1^6 \cdot q_1^4 = (2^{k+160})^4 \cdot q_0^6 \cdot q_1^{10}.$$

We next define $E_0 \subseteq S_0$ as the set of all $\vec{s} \in S_0$ such that $\vec{s}$ gives rise to $b = 0$ and $\mathsf{View}(\vec{s}) = \hat{V}$ and $\neg\mathsf{NR}$ is true when the random choice in the experiment is $\vec{s}$. Then

$$\Pr[\mathsf{View} = \hat{V} | b = 0] = \frac{|E_0|}{|S_0|}.$$

We next compute $|E_0|$. This is the number of solutions to the following system of 16 equations in 24 unknowns – $x_{1,0}, x_{2,0}, y_{1,0}, y_{2,0}, z_{1,0}, z_{2,0}, x_{1,1}, x_{2,1}, y_{1,1}$, $y_{2,1}, z_{1,1}, z_{2,1}, g_{1,0}, g_{2,0}, u_{1,0}, u_{2,0}, g_{1,1}, g_{2,1}$, $u_{1,1}, u_{2,1}$, t_1, t_2, t_3, t_4 (Note that b is fixed to 0 since we now consider $E_0 \subseteq S_0$.):

$$
\begin{array}{rcll r}
g_{1,0} & = & \hat{g}_{1,0} & \pmod{p_0} & (1) \\
g_{2,0} & = & \hat{g}_{2,0} & \pmod{p_0} & (2) \\
x_{1,0} + \hat{\omega}_0 x_{2,0} & = & \log_{\hat{g}_{1,0}} \hat{c}_0 & \pmod{q_0} & (3) \\
y_{1,0} + \hat{\omega}_0 y_{2,0} & = & \log_{\hat{g}_{1,0}} \hat{d}_0 & \pmod{q_0} & (4) \\
z_{1,0} + \hat{\omega}_0 z_{2,0} & = & \log_{\hat{g}_{1,0}} \hat{h}_0 & \pmod{q_0} & (5) \\
g_{1,1} & = & \hat{g}_{1,1} & \pmod{p_1} & (6) \\
g_{2,1} & = & \hat{g}_{2,1} & \pmod{p_1} & (7) \\
x_{1,1} + \hat{\omega}_1 x_{2,1} & = & \log_{\hat{g}_{1,1}} \hat{c}_1 & \pmod{q_1} & (8) \\
y_{1,1} + \hat{\omega}_1 y_{2,1} & = & \log_{\hat{g}_{1,1}} \hat{d}_1 & \pmod{q_1} & (9) \\
z_{1,1} + \hat{\omega}_1 z_{2,1} & = & \log_{\hat{g}_{1,1}} \hat{h}_1 & \pmod{q_1} & (10) \\
F_{q_0}(u_{1,0}) + t_1 q_0 & = & \hat{u}'_{1,0} & & (11) \\
F_{q_0}(u_{2,0}) + t_2 q_0 & = & \hat{u}'_{2,0} & & (12) \\
F_{q_0}(e) + t_3 q_0 & = & \hat{e}' & & (13) \\
F_{q_0}(v) + t_4 q_0 & = & \hat{v}' & & (14) \\
r_{1,0} z_{1,0} + r_{2,0} \hat{\omega}_0 z_{2,0} & = & \log_{\hat{g}_{1,0}} \frac{e}{M} & \pmod{q_0} & (15) \\
r_{1,0} x_{1,0} + r_{1,0} \alpha_0 x_{2,0} + r_{2,0} \hat{\omega}_0 x_{2,0} + r_{2,0} \hat{\omega}_0 \alpha_0 y_{2,0} & = & \log_{\hat{g}_{1,0}} v & \pmod{q_0} & (16)
\end{array}
$$

In the above equations, $\hat{\omega}_0 = \log_{\hat{g}_{1,0}} \hat{g}_{2,0}$, $\hat{\omega}_1 = \log_{\hat{g}_{1,1}} \hat{g}_{2,1}$ $r_{1,0} = \log_{\hat{g}_{1,0}} u_{1,0}$, $r_{2,0} = \log_{\hat{g}_{1,0}} u_{2,0}$, and $\alpha_0 = \mathcal{EH}_{\hat{K}_0}(u_{1,0}, u_{2,0}, e)$. The variables with hats, and p_0, p_1, q_0, q_1, M denote the known constants whereas the variables without hats except p_0, p_1, q_0, q_1, M denote unknowns.

In the following, we evaluate the number of solutions of the above 16 equations. Note that we consider the situation that $\neg\mathsf{NR}$.

From equations 1, 2, 6, and 7, the values $g_{1,0}, g_{2,0}, g_{1,1}, g_{2,1}$ are fixed uniquely. Noticing that $F_{q_0} : G_{q_0} \rightarrow \mathbb{Z}_{q_0}$ is bijective, from equations 11, 12, 13, and 14, the values $t_1, t_2, t_3, t_4 \in \mathbb{N}$ and $u_{1,0}, u_{2,0}, e, v \in QR_{p_0}$ are fixed uniquely.

Since the values $u_{1,0}, u_{2,0}, e$ are fixed, $r_{1,0}, r_{2,0}, \alpha_0$ are also fixed. In the following, we consider the situation such that $g_{1,0}, g_{2,0}, g_{1,1}, g_{2,1}, t_1, t_2, t_3, t_4, u_{1,0}, u_{2,0}, e, v$, $r_{1,0}, r_{2,0}, \alpha_0$ are fixed.

From equations 5 and 15, the values $z_{1,0}, z_{2,0}$ are fixed uniquely.

The values $x_{1,0}, x_{2,0}, y_{1,0}, y_{2,0}$ are restricted only by equations 3, 4, and 16, and the number of vectors $(x_{1,0}, x_{2,0}, y_{1,0}, y_{2,0})$ which satisfy these three equations is q_0.

The values $x_{1,1}, x_{2,1}, y_{1,1}, y_{2,1}, z_{1,1}, z_{2,1}$ are restricted only by equations 8, 9, and 10, and the number of vectors $(x_{1,1}, x_{2,1}, y_{1,1}, y_{2,1}, z_{1,1}, z_{2,1})$ which satisfy these three equations is q_1^3.

Finally, $u_{1,1}, u_{2,1}$ are not restricted by the above 16 equations, therefore the number of vectors $(u_{1,1}, u_{2,1})$ which satisfy these above equations is q_1^2.

Hence, the number of solutions is $q_0 \cdot q_1^5$, which is $|E_0|$, and

$$
\Pr[\mathsf{View} = \hat{V} | b = 0] = \frac{|E_0|}{|S_0|} = \frac{q_0 \cdot q_1^5}{(2^{k+160})^4 \cdot q_0^6 \cdot q_1^{10}} = \frac{1}{(2^{k+160})^4 \cdot q_0^5 \cdot q_1^5}.
$$

In the case of $b = 1$, the equations 11–16 are replaced by the following equations $11'$–$16'$ respectively.

$$
\begin{aligned}
F_{q_1}(u_{1,1}) + t_1 q_1 &= \hat{u}'_{1,1} && && (11') \\
F_{q_1}(u_{2,1}) + t_2 q_1 &= \hat{u}'_{2,1} && && (12') \\
F_{q_1}(e) + t_3 q_1 &= \hat{e}' && && (13') \\
F_{q_1}(v) + t_4 q_1 &= \hat{v}' && && (14') \\
r_{1,1} z_{1,0} + r_{2,1}\hat{\omega}_1 z_{2,0} &= \log_{\hat{g}_{1,1}} \tfrac{e}{M} && \pmod{q_1} && (15') \\
r_{1,1}x_{1,1} + r_{1,1}\alpha_1 x_{2,1} + r_{2,1}\hat{\omega}_1 x_{2,1} + r_{2,1}\hat{\omega}_1\alpha_1 y_{2,1} &= \log_{\hat{g}_{1,1}} v && \pmod{q_1} && (16')
\end{aligned}
$$

where $r_{1,1} = \log_{\hat{g}_{1,1}} u_{1,1}$, $r_{2,1} = \log_{\hat{g}_{1,1}} u_{2,1}$, and $\alpha_1 = \mathcal{EH}_{\hat{K}_1}(u_{1,1}, u_{2,1}, e)$.

By a similar observation as that in the case of $b = 0$, we have $|S_1| = (2^{k+160})^4 \cdot q_1^6 \cdot q_0^{10}$ and $|E_1| = q_1 \cdot q_0^5$. Therefore,

$$\Pr[\mathsf{View} = \hat{V} | b = 1] = \frac{|E_1|}{|S_1|} = \frac{q_1 \cdot q_0^5}{(2^{k+160})^4 \cdot q_1^6 \cdot q_0^{10}} = \frac{1}{(2^{k+160})^4 \cdot q_1^5 \cdot q_0^5}.$$

In conclusion, we have $\Pr[\mathsf{View} = \hat{V} | b = 0] = \Pr[\mathsf{View} = \hat{V} | b = 1]$. □

B.2.3 Proof of Lemma 5

We first define the events Inv_0 and Inv_1. The event Inv_0 (respectively Inv_1) is true if during the execution of D the adversary A submits an invalid ciphertext to its decryption oracle $\mathcal{D}_{sk_0}$ (resp. $\mathcal{D}_{sk_1}$) and does not get $\perp$. It is clear that

$$\Pr[\mathsf{Inv} | \neg\mathsf{NR}] \le \Pr[\mathsf{Inv}_0 | \neg\mathsf{NR}] + \Pr[\mathsf{Inv}_1 | \neg\mathsf{NR}].$$

We now evaluate $\Pr[\mathsf{Inv}_0 | \neg\mathsf{NR}]$. Assume the adversary A submits an invalid ciphertext $(\tilde{u}'_1, \tilde{u}'_2, \tilde{e}', \tilde{v}')$ to its decryption oracle $\mathcal{D}_{sk_0}$. Let $(u'_{1,b}, u'_{2,b}, e', v')$ denote the challenge ciphertext.

Then, we have

$$(u_{1,b}, u_{2,b}, e, v) = F^{-1}_{q_0,4}(u'_{1,b} \bmod q_0, u'_{2,b} \bmod q_0, e' \bmod q_0, v' \bmod q_0)$$

and

$$(\tilde{u}_1, \tilde{u}_2, \tilde{e}, \tilde{v}) = F^{-1}_{q_0,4}(\tilde{u}'_1 \bmod q_0, \tilde{u}'_2 \bmod q_0, \tilde{e}' \bmod q_0, \tilde{v}' \bmod q_0).$$

Note that $F^{-1}_{q_0,4}$ is bijective. Furthermore, we have $\tilde{\alpha}_0 = \mathcal{EH}_{K_0}(\tilde{u}_1, \tilde{u}_2, \tilde{e})$ and $\alpha_{0,b} = \mathcal{EH}_{K_0}(u_{1,b}, u_{2,b}, e)$.

We consider the following three cases.

- Case 1 : $(\tilde{u}_1, \tilde{u}_2, \tilde{e}) = (u_{1,b}, u_{2,b}, e)$
- Case 2 : $(\tilde{u}_1, \tilde{u}_2, \tilde{e}) \neq (u_{1,b}, u_{2,b}, e)$ and $\tilde{\alpha}_0 = \alpha_{0,b}$
- Case 3 : $(\tilde{u}_1, \tilde{u}_2, \tilde{e}) \neq (u_{1,b}, u_{2,b}, e)$ and $\tilde{\alpha}_0 \neq \alpha_{0,b}$

In Case 1, noticing that $(\tilde{u}'_1, \tilde{u}'_2, \tilde{e}', \tilde{v}') \notin EC((u'_{1,b}, u'_{2,b}, e', v'), pk_0)$, $\tilde{v} \neq v$ and the decryption oracle will reject. If Case 2 occurs, it implies that the adversary A can find a collision for $\mathcal{EH}_{K_0}$. Therefore, there exists an adversary C attacking the collision-resistance of $\mathcal{H}$ such that

$$
\begin{aligned}
\Pr[\mathsf{Inv}_0 | \neg\mathsf{NR}] &= \Pr[\mathsf{Inv}_0 | \text{Case } 1 \wedge \neg\mathsf{NR}] \cdot \Pr[\text{Case } 1] \\
&+ \Pr[\mathsf{Inv}_0 | \text{Case } 2 \wedge \neg\mathsf{NR}] \cdot \Pr[\text{Case } 2] + \Pr[\mathsf{Inv}_0 | \text{Case } 3 \wedge \neg\mathsf{NR}] \cdot \Pr[\text{Case } 3] \\
&\le 0 + \Pr[\text{Case } 2] + \Pr[\mathsf{Inv}_0 | \text{Case } 3 \wedge \neg\mathsf{NR}] \\
&\le 0 + \mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},C}(k) + \Pr[\mathsf{Inv}_0 | \text{Case } 3 \wedge \neg\mathsf{NR}].
\end{aligned}
$$

Note that the time-complexity of C is bounded by that of A plus $O(k^3)$.

We now bound $\Pr[\mathsf{Inv}_0 | \text{Case } 3 \wedge \neg\mathsf{NR}]$.

A ciphertext $(\tilde{u}'_1, \tilde{u}'_2, \tilde{e}', \tilde{v}')$ submitted to the $\mathcal{D}_{sk_0}$ is accepted when

$$(\tilde{u}_1)^{x_{1,0}+y_{1,0}\tilde{\alpha}_0}(\tilde{u}_2)^{x_{2,0}+y_{2,0}\tilde{\alpha}_0} = \tilde{v}.$$

Let $\tilde{u}_1 = g_{1,0}^{\tilde{r}_1}, \tilde{u}_2 = g_{2,0}^{\tilde{r}_2} = g_{1,0}^{\omega_0\tilde{r}_2}$. We can rewrite the above equation as

$$\tilde{r}_1 x_{1,0} + \tilde{r}_1\tilde{\alpha}x_{2,0} + \tilde{r}_2\hat{\omega}_0 x_{2,0} + \tilde{r}_2\hat{\omega}_0\tilde{\alpha}y_{2,0} = \log_{\hat{g}_{1,0}} \tilde{v} \pmod{q_0}. \qquad (17)$$

Let us define the following events:

- $\mathsf{Inv}_{i,0}$ is true if the adversary A during its i-th query submits an invalid ciphertext $(\tilde{u}'_1, \tilde{u}'_2, \tilde{e}', \tilde{v}')$ subject to Case 3 to the decryption oracle $\mathcal{D}_{sk_0}$ for $i \in \{1, 2, \cdots, q_d\}$ and does not get $\perp$.
- E_0^{inv} is a set $\{\vec{s} \in S | \vec{s}$ gives rise to equation 17 and $\neg\mathsf{NR}\}$ and Case 3.

We now consider the simulation of $\mathcal{D}_{sk_0}$. To submit a ciphertext which will not be rejected, the adversary should find the coefficients for Equation 17 which is consistent with its view, which with equal probability can contain a hidden bit $b = 0$ and $b = 1$. Therefore,

$$\begin{aligned}
&\Pr[\mathsf{Inv}_{1,0} | \neg\mathsf{NR}] \\
&= \frac{1}{2}\Pr[E_0^{\text{inv}} | E_0] + \frac{1}{2}\Pr[E_0^{\text{inv}} | E_1] \le \frac{\Pr[E_0^{\text{inv}} \wedge E_0]}{\Pr[E_0]} + \frac{\Pr[E_0^{\text{inv}} \wedge E_1]}{\Pr[E_1]} \\
&\le \frac{|E_0^{\text{inv}} \wedge E_0| \cdot |S|}{2|S||E_0|} + \frac{|E_0^{\text{inv}} \wedge E_1| \cdot |S|}{2|S||E_1|} = \frac{|E_0^{\text{inv}} \wedge E_0|}{2q_0q_1^5} + \frac{|E_0^{\text{inv}} \wedge E_1|}{2q_1q_0^5}.
\end{aligned}$$

where $|E_0^{\text{inv}} \wedge E_0|$ is the number of solutions to the system of equations 1–16 and 17 assuming $\neg\mathsf{NR}$, and $|E_0^{\text{inv}} \wedge E_1|$ is that of equations 1–10, 11′–16′, and 17 assuming $\neg\mathsf{NR}$.

In the case of $|E_0^{\text{inv}} \wedge E_0|$, adding equation 17 to the system of equations 1–16, $(x_{1,0}, x_{2,0}, y_{1,0}, y_{2,0})$ are fixed uniquely. The other values are not restricted by equation 17. Then, we have $|E_0^{\text{inv}} \wedge E_0| = q_1^5$.

In the case of $|E_0^{\text{inv}} \wedge E_1|$, adding equation 17 to the system of equations 1–10 and 11′–16′, the number of vectors $(x_{1,0}, x_{2,0}, y_{1,0}, y_{2,0})$ which satisfy the system of equations 1–10, 11′–16′, and 17 is reduced from q_0^2 to q_0^1. The other values are not restricted by equation 17. Hence, we have $|E_0^{\text{inv}} \wedge E_1| = q_1q_0^4$.

Therefore,

$$\Pr[\mathsf{Inv}_{1,0} | \neg\mathsf{NR}] \le \frac{q_1^5}{2q_0q_1^5} + \frac{q_1q_0^4}{2q_1q_0^5} = \frac{1}{q_0}.$$

Each time the adversary submits an invalid ciphertext and it gets rejected, this reduces the set of the next possible decryption oracle queries at most by one. Hence, we have

$$\Pr[\mathsf{Inv}_0 | \neg\mathsf{NR} \wedge \text{Case } 3] \le \sum_{i=1}^{q_d(k)} \Pr[\mathsf{Inv}_{i,0} | \neg\mathsf{NR}] \le \sum_{i=1}^{q_d(k)} \frac{1}{q_0 - i + 1} \le \frac{2q_d(k)}{q_0} \le \frac{q_d(k)}{2^{k-2}}.$$

Therefore, we have

$$\Pr[\mathsf{Inv}_0 | \neg\mathsf{NR}] \le \mathbf{Adv}_{\mathcal{H},C}^{\text{cr}}(k) + \frac{q_d(k)}{2^{k-2}}.$$

Similarly, we can evaluate $\Pr[\mathsf{Inv}_{1,1} | \neg\mathsf{NR} \wedge \text{Case } 3] \le 1/q_1$ and

$$\Pr[\mathsf{Inv}_1 | \neg\mathsf{NR}] \le \mathbf{Adv}_{\mathcal{H},C}^{\text{cr}}(k) + \frac{q_d(k)}{2^{k-2}}.$$

In conclusion, we have

$$\Pr[\mathsf{Inv} | \neg\mathsf{NR} \wedge \text{Case } 3] \le 2\mathbf{Adv}_{\mathcal{H},C}^{\text{cr}}(k) + \frac{q_d(k)}{2^{k-3}}.$$