ISSN 1342-2812

Research Reports on
Mathematical and
Computing Sciences

Universal Anonymizable Public-Key Encryption

Ryotaro Hayashi and Keisuke Tanaka

February 2005, C–208

Department of
Mathematical and
Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

Universal Anonymizable Public-Key Encryption

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

February 15, 2005

Abstract

We first propose the notion of universal anonymizable public-key encryption. Suppose that we have the encrypted data made with the same security parameter, and that these data do not satisfy the anonymity property. Consider the situation that we would like to transform these encrypted data to those with the anonymity property without decrypting these encrypted data. In this paper, in order to formalize this situation, we propose a new property for public-key encryption called universal anonymoizablity. We then propose the universal anonymizable public-key encryption schemes based on RSA-OAEP, the ElGamal encryption, and the Cramer-Shoup encryption schemes, and prove their security.

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

1 Introduction

The classical security requirement of public-key encryption schemes is that it provides privacy of the encrypted data. Popular formalizations such as indistinguishability or non-malleability, under either the chosen-plaintext or the chosen-ciphertext attacks are directed at capturing various data-privacy requirements.

Bellare, Boldyreva, Desai, and Pointcheval [1] proposed a new security requirement of encryption schemes called "key-privacy" or "anonymity." It asks that an encryption scheme provides (in addition to privacy of the data being encrypted) privacy of the key under which the encryption was performed. That is, if an encryption scheme provides the key-privacy, then the receiver is anonymous from the point of view of the adversary.

Anonymous encryption schemes have various applications such as anonymous authenticated key exchange protocol (Krawczyk [11]), anonymous credential system (Camenisch and Lysyanskaya [4]), and auction protocols (Sako [14]).

In addition to the notion of key-privacy, they provided the RSA-based key-privacy encryption scheme, RSA-RAEP, which is a variant of RSA-OAEP (Bellare and Rogaway [2], Fujisaki, Okamoto, Pointcheval, and Stern [7]). Recently, Hayashi, Okamoto, and Tanaka [9] proposed the RSA-based key-privacy encryption scheme by using the RSACD function, and Hayashi and Tanaka [10] also constructed the RSA-based key-privacy encryption scheme by using the sampling twice technique. With respect to the discrete-log based schemes, Bellare, Boldyreva, Desai, and Pointcheval [1] proved

*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.

that the ElGamal and the Cramer-Shoup encryption schemes provide the anonymity property when all of the users use a common group.

Suppose that we have the encrypted data made with the same security parameter, and that these data do not satisfy the anonymity property. Consider the situation that we would like to transform these encrypted data to those with the anonymity property without decrypting these encrypted data. In this paper, in order to formalize this situation, we propose a special type of public-key encryption scheme called a *universal anonymizable public-key encryption scheme*. The universal anonymizable public-key encryption scheme consists of a standard public-key encryption scheme $\mathcal{PE}$ and two other additional algorithms, that is, an anonymizing algorithm $\mathcal{UA}$ and a decryption algorithm $\mathcal{DA}$ for anonymized ciphertexts. We can use $\mathcal{PE}$ as a standard encryption scheme which is not necessary to have the anonymity property. Furthermore, in this scheme, by using the anonymizing algorithm $\mathcal{UA}$, anyone who has a standard ciphertext can anonymize the ciphertext with its public key whenever she wants to do that. The receiver can decrypt the anonymized ciphertext by using the decryption algorithm $\mathcal{DA}$ for anonymized ciphertexts. Then, the adversary cannot know under which key the anonymized ciphertext was created.

To formalize the security properties for universal anonymizable public-key encryption, we define three requirements, the key-privacy, the data-privacy on standard ciphertexts, and that on anonymized ciphertexts.

We then propose the universal anonymizable public-key encryption schemes based on RSA-OAEP, the ElGamal encryption, and the Cramer-Shoup encryption schemes, and prove their security.

We show the key-privacy property of our schemes by a similar argument as in [1]. The argument in [1] for the discrete-log based scheme depends heavily on the situation where all of the users employ a common group. However, in our descrete-log based schemes, we do not use the common group for obtaining the key-privacy property. Therefore, we cannot straightforwardly apply their argument to our schemes. To prove the key-privacy property of our schemes, we employ the idea described in [5] by Cramer and Shoup, where we encode the elements of QR_p (a group of quadratic residues modulo p) where $p = 2q + 1$ and p, q are prime to those of $\mathbb{Z}_q$. This encoding plays an important role in our schemes.

The organization of this paper is as follows. In Section 2, we describe the definitions of the RSA family of trap-door permutations, the DDH problem, and the paired DDH problem. In Section 3, we formulate the notion of universal anonymizable public-key encryption and its security properties. We propose the universal anonymizable public-key encryption scheme based on RSA-OAEP in Section 4, that based on the ElGamal encryption scheme in Section 5, and that based on the Cramer-Shoup encryption scheme in Section 6. We conclude in Section 7.

2 Preliminaries

In this section, we describe the definitions of the RSA family of trap-door permutations, the DDH problem, and the paired DDH problem. Our schemes are based on these family and problems.

2.1 The RSA Family of Trap-Door Permutations

Definition 1 (the RSA family of trap-door permutations)**.** *The RSA family of trap-door permutations* $\mathsf{RSA} = (K, E, I)$ *is described as follows. The key generation algorithm* K *takes as input a security parameter* k *and picks random, distinct primes* p, q *in the range* $2^{\lceil k/2 \rceil - 1} < p, q < 2^{\lceil k/2 \rceil}$ *and* $2^{k-1} < pq < 2^k$*. It sets* $N = pq$ *and picks* $e, d \in \mathbb{Z}^*_{\phi(N)}$ *such that* $ed = 1 \pmod{\phi(N)}$*. The public key is* N, e, k *and the secret key is* N, d, k*. The evaluation algorithm is* $E_{N,e,k}(x) = x^e \bmod N$ *and the inversion algorithm is* $I_{N,d,k}(y) = y^d \bmod N$*.*

We describe the definition of partial one-wayness of RSA.

Definition 2 (θ-partial one-wayness of RSA). *Let $k \in \mathbb{N}$ be a security parameter. Let $0 < \theta \leq 1$ be a constant. Let A be an adversary. We consider the following experiments:*

```
Experiment $\mathbf{Exp}^{\theta\text{-pow-fnc}}_{\mathsf{RSA},A}(k)$
  $((N,e,k),(N,d,k)) \leftarrow K(k);\ x \overset{R}{\leftarrow} \mathbb{Z}_N^*;\ y \leftarrow x^e \bmod N$
  $x_1 \leftarrow A(pk,y)$ where $|x_1| = \lceil \theta \cdot |x| \rceil$
  if $((x_1||x_2)^e \bmod N = y$ for some $x_2)$ return $1$ else return $0$
```

Here "$||$" denotes concatenation, and "$x \overset{R}{\leftarrow} \mathbb{Z}_N^*$" is the operation of picking an element x uniformly from $\mathbb{Z}_N^*$. We define the advantages of the adversary via

$$\mathbf{Adv}^{\theta\text{-pow-fnc}}_{\mathsf{RSA},A}(k) = \Pr[\mathbf{Exp}^{\theta\text{-pow-fnc}}_{\mathsf{RSA},A}(k) = 1]$$

where the probability is taken over K, $x \overset{R}{\leftarrow} \mathbb{Z}_N^*$, and A. We say that the RSA family RSA is θ-partial one-way if the function $\mathbf{Adv}^{\theta\text{-pow-fnc}}_{\mathsf{RSA},A}(\cdot)$ is negligible for any adversary A 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.

Note that when $\theta = 1$ the notion of θ-partial one-wayness coincides with the standard notion of one-wayness. Fujisaki, Okamoto, Pointcheval, and Stern [7] showed that the θ-partial one-wayness of RSA is equivalent to the (1-partial) one-wayness of RSA for $\theta > 0.5$.

2.2 The Decisional Diffie-Hellman Problem

Definition 3 (DDH). *Let $\mathcal{G}$ be a group generator which takes as input a security parameter k and returns (q,g) where q is a k-bit integer 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 $\mathbf{Exp}^{\text{ddh-real}}_{\mathcal{G},D}(k)$
  $(q,g) \leftarrow \mathcal{G}(k);\ x,y \overset{R}{\leftarrow} \mathbb{Z}_q$
  $X \leftarrow g^x;\ Y \leftarrow g^y;\ T \leftarrow g^{xy}$
  $d \leftarrow D(q,g,X,Y,T)$
  return $d$
```

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

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

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

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

2.3 The Paired Decisional Diffie-Hellman Problem

We now define the paired DDH problem. In order to prove the securities of our schemes based on the ElGamal and Cramer-Shoup schemes, we use this problem for reductions.

Definition 4 (paired DDH). *Let $\mathcal{G}$ be a group generator. Let D be an adversary. We consider the* *following experiments:*

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

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

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

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

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

We prove the following theorem, and its proof is in Appendix A.

Theorem 1. *The paired DDH problem for $\mathcal{G}$ is hard if and only if the DDH problem for $\mathcal{G}$ is hard.*

3 Universal Anonymizable Public-Key Encryption

In this section, we propose the definition of universal anonymizable public-key encryption schemes and its security properties.

3.1 The Definition of Universal Anonymizable Public-Key Encryption Schemes

We formalize the notion of universal anonymizable public-key encryption schemes as follows.

Definition 5. *A universal anonymizable public-key encryption scheme $\mathcal{UAPE} = ((\mathcal{K}, \mathcal{E}, \mathcal{D}), \mathcal{UA}, \mathcal{DA})$ consists of a public-key encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ and two other algorithms.*

- *The key generation algorithm $\mathcal{K}$ is a randomized algorithm that takes as input a security parameter k and returns a pair (pk, sk) of keys, a 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 m to return a standard ciphertext c.*
- *The decryption algorithm $\mathcal{D}$ for standard ciphertexts is a deterministic algorithm that takes the secret key sk and a standard ciphertext c to return the corresponding plaintext m or a special symbol $\perp$ to indicate that the standard ciphertext is invalid.*
- *The anonymizing algorithm $\mathcal{UA}$ is a randomized algorithm that takes the public key pk and a standard ciphertext c, and returns an anonymized ciphertext c'.*
- *The decryption algorithm $\mathcal{DA}$ for anonymized ciphertexts is a deterministic algorithm that takes the secret key sk and an anonymized ciphertext c' and returns the corresponding plaintext m or a special symbol $\perp$ to indicate that the anonymized ciphertext is invalid.*

In the universal anonymizable public-key encryption scheme, we can use $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ as a standard encryption scheme. Furthermore, in this scheme, by using the anonymizing algorithm $\mathcal{UA}$, anyone who has a standard ciphertext can anonymize the ciphertext whenever she wants to do that. The receiver can decrypt the anonymized ciphertext by using the decryption algorithm $\mathcal{DA}$ for anonymized ciphertexts.

3.2 Security Properties of Universal Anonymizable Public-Key Encryption Scheme

We now define two security properties with respect to universal anonymizable public-key encryption schemes.

3.2.1 Key-Privacy

First, we define the security property called *key-privacy* of universal anonymizable public-key encryption schemes. If the scheme provides the key-privacy, the adversary cannot know under which key the anonymized ciphertext was encrypted.

Definition 6 (Key-Privacy)**.** *Let $b \in \{0,1\}$ and $k \in \mathbb{N}$. Let $A_{\mathrm{cpa}} = (A^1_{\mathrm{cpa}}, A^2_{\mathrm{cpa}})$, $A_{\mathrm{cca}} = (A^1_{\mathrm{cca}}, A^2_{\mathrm{cca}})$ be adversaries that run in two stages and where A_{cca} has access to the oracles $\mathcal{D}_{sk_0}(\cdot)$, $\mathcal{D}_{sk_1}(\cdot)$, $\mathcal{DA}_{sk_0}(\cdot)$, and $\mathcal{DA}_{sk_1}(\cdot)$. Note that* si *is the state information. It contains pk_0, pk_1, and so on. For* $\mathrm{atk} \in \{\mathrm{cpa, cca}\}$*, we consider the following experiment:*

```
Experiment $\mathbf{Exp}^{\text{key-atk-}b}_{\mathcal{UAPE},A_{\mathrm{atk}}}(k)$
    $(pk_0, sk_0) \leftarrow \mathcal{K}(k);\ (pk_1, sk_1) \leftarrow \mathcal{K}(k)$
    $(m_0, m_1, \mathsf{si}) \leftarrow A^1_{\mathrm{atk}}(pk_0, pk_1);\ c \leftarrow \mathcal{E}_{pk_b}(m_b);\ c' \leftarrow \mathcal{UA}_{pk_b}(c);\ d \leftarrow A^2_{\mathrm{atk}}(c', \mathsf{si})$
    return $d$
```

Note that m_0 and m_1 are chosen from the message spaces for pk_0 and pk_1, respectively. Above it is mandated that A^2_{cca} never queries the challenge c' to either $\mathcal{DA}_{sk_0}(\cdot)$ or $\mathcal{DA}_{sk_1}(\cdot)$. For $\mathrm{atk} \in \{\mathrm{cpa, cca}\}$*, we define the advantage via*

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

We say that a universal anonymizable public-key encryption scheme $\mathcal{UAPE}$ provides the the key-privacy against the chosen plaintext attack (respectively the adaptive chosen ciphertext attack) if the function $\mathbf{Adv}^{\text{key-cpa}}_{\mathcal{UAPE},A_{\mathrm{cpa}}}(\cdot)$ (resp. $\mathbf{Adv}^{\text{key-cca}}_{\mathcal{UAPE},A_{\mathrm{cca}}}(\cdot)$) is negligible for any adversary A whose time complexity is polynomial in k.

Bellare, Boldyreva, Desai, and Pointcheval [1] proposed a security requirement of the encryption schemes called "key-privacy." Similar to the above definition, it asks that the encryption provides privacy of the key under which the encryption was performed. In addition to the property of the universal anonymizability, there are two differences between their definition and ours.

In [1], they defined the encryption scheme with some *common-key* which contains the common parameter for all users to obtain the key-privacy property. For example, in the discrete-log based schemes such that the ElGamal and the Cramer-Shoup encryption schemes, the common key contains a common group G, and the encryption is performed over the common group for all uses.

On the other hand, in our definition, we do not prepare any common key for obtaining the key-privacy property. In the universal anonymizable public-key encryption scheme, we can use the standard encryption scheme which is not necessary to have the key-privacy property. In addition to it, anyone can anonymize the ciphertext by using its public key whenever she want to do that, and the adversary cannot know under which key the anonymized ciphertext was created.

The definition in [1], they considered the situation that the message space was common to each user. Therefore, in the experiment of their definition, the adversary chooses only one message m from the common message space and receives a ciphertext of m encrypted with one of two keys pk_0 and pk_1.

In our definition, we do not use common parameter, the message spaces for users may be different even if the security parameter is fixed. In fact, in Sections 5 and 6, we propose the encryption schemes whose message spaces for users are different. Therefore, in the experiment of our definition, the adversary chooses two messages m_0 and m_1 where m_0 and m_1 are in the message spaces for pk_0

and pk_1, respectively, and receives either a ciphertext of m_0 encrypted with pk_0 or a ciphertext of m_1 encrypted with pk_1. The ability of the adversary with two messages m_0 and m_1 might be stronger than that with one message m.

3.2.2 Data-Privacy

Second, we define the security property called *data-privacy* of universal anonymizable public-key encryption schemes. The definition is based on the indistinguishability for standard public-key encryption schemes.

We can consider two types of data-privacy, that is, the data-privacy on standard ciphertexts and that on anonymized ciphertexts.

Definition 7 (Data-Privacy of Standard Ciphertexts). *Let $b \in \{0,1\}$ and $k \in \mathbb{N}$. Let $A_{\rm cpa} = (A^1_{\rm cpa}, A^2_{\rm cpa})$, $A_{\rm cca} = (A^1_{\rm cca}, A^2_{\rm cca})$ be adversaries that run in two stages and where $A_{\rm cca}$ has access to the oracles $\mathcal{D}_{sk_0}(\cdot)$, $\mathcal{D}_{sk_1}(\cdot)$, $\mathcal{DA}_{sk_0}(\cdot)$, and $\mathcal{DA}_{sk_1}(\cdot)$. For* atk $\in$ {cpa, cca}*, we consider the following experiment:*

```
Experiment $\mathbf{Exp}^{\text{dataS-atk-}b}_{\mathcal{UAPE},A_{\rm atk}}(k)$
    $(pk, sk) \leftarrow \mathcal{K}(k)$
    $(m_0, m_1, \mathsf{si}) \leftarrow A^1_{\rm atk}(pk)$;  $c \leftarrow \mathcal{E}_{pk}(m_b)$;  $d \leftarrow A^2_{\rm atk}(c, \mathsf{si})$
    return $d$
```

Note that m_0 and m_1 are chosen from the message space for pk. Above it is mandated that $A^2_{\rm cca}$ never queries the challenge c to either $\mathcal{D}_{sk_0}(\cdot)$ or $\mathcal{D}_{sk_1}(\cdot)$. It is also mandated that $A^2_{\rm cca}$ never queries either the anonymized ciphertexts $\tilde{c} \in \{\mathcal{UA}_{pk_0}(c)\}$ to $\mathcal{DA}_{sk_0}(\cdot)$ or $\tilde{c} \in \{\mathcal{UA}_{pk_1}(c)\}$ to $\mathcal{DA}_{sk_1}(\cdot)$. For atk $\in$ {cpa, cca}*, we define the advantage via*

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

We say that a universal anonymizable public-key encryption scheme $\mathcal{UAPE}$ provides the data-privacy on standard ciphertexts against the chosen plaintext attack (respectively the adaptive chosen ciphertext attack) if the function $\mathbf{Adv}^{\text{dataS-cpa}}_{\mathcal{UAPE},A_{\rm cpa}}(\cdot)$ (resp. $\mathbf{Adv}^{\text{dataS-cca}}_{\mathcal{UAPE},A_{\rm cca}}(\cdot)$) is negligible for any adversary A whose time complexity is polynomial in k.

Definition 8 (Data-Privacy of Anonymized Ciphertexts). *Let $b \in \{0,1\}$ and $k \in \mathbb{N}$. Let $A_{\rm cpa} = (A^1_{\rm cpa}, A^2_{\rm cpa})$, $A_{\rm cca} = (A^1_{\rm cca}, A^2_{\rm cca})$ be adversaries that run in two stages and where $A_{\rm cca}$ has access to the oracles $\mathcal{D}_{sk_0}(\cdot)$, $\mathcal{D}_{sk_1}(\cdot)$, $\mathcal{DA}_{sk_0}(\cdot)$, and $\mathcal{DA}_{sk_1}(\cdot)$. For* atk $\in$ {cpa, cca}*, we consider the following experiment:*

```
Experiment $\mathbf{Exp}^{\text{dataA-atk-}b}_{\mathcal{UAPE},A_{\rm atk}}(k)$
    $(pk, sk) \leftarrow \mathcal{K}(k)$
    $(m_0, m_1, \mathsf{si}) \leftarrow A^1_{\rm atk}(pk)$;  $c \leftarrow \mathcal{E}_{pk}(m_b)$;  $c' \leftarrow \mathcal{UA}_{pk}(c)$;  $d \leftarrow A^2_{\rm atk}(c', \mathsf{si})$
    return $d$
```

Note that m_0 and m_1 are chosen from the message space for pk. Above it is mandated that $A^2_{\rm cca}$ never queries the challenge c' to either $\mathcal{DA}_{sk_0}(\cdot)$ or $\mathcal{DA}_{sk_1}(\cdot)$. For atk $\in$ {cpa, cca}*, we define the advantage via*

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

We say that the universal anonymizable public-key encryption scheme $\mathcal{UAPE}$ provides the data-privacy on anonymized ciphertexts against the chosen plaintext attack (respectively the adaptive chosen ciphertext attack) if the function $\mathbf{Adv}^{\text{dataA-cpa}}_{\mathcal{UAPE},A_{\rm cpa}}(\cdot)$ (resp. $\mathbf{Adv}^{\text{dataA-cca}}_{\mathcal{UAPE},A_{\rm cca}}(\cdot)$) is negligible for any adversary A whose time complexity is polynomial in k.

We say that a universal anonymizable public-key encryption scheme $\mathcal{UAPE}$ is CPA-secure (respectively CCA-secure) if the scheme $\mathcal{UAPE}$ provides the key-privacy, the data-privacy on standard ciphertexts, and that on anonymized ciphertexts, against the chosen plaintext attack (resp. the adaptive chosen ciphertext attack).

4 RSA-OAEP and its Universal Anonymizability

In this section, we propose a universal anonymizable RSA-OAEP scheme.

4.1 RSA-OAEP

Definition 9 (RSA-OAEP)**.** *RSA-OAEP $\mathcal{PE}^{\mathsf{RO}} = (\mathcal{K}^{\mathsf{RO}}, \mathcal{E}^{\mathsf{RO}}, \mathcal{D}^{\mathsf{RO}})$ is as follows. Let k, k_0 and k_1 be security parameters such that $k_0 + k_1 < k$. This defines an associated plaintext-length $n = k - k_0 - k_1$. The key generation algorithm $\mathcal{K}^{\mathsf{RO}}$ takes as input a security parameter k and runs the key generation algorithm of the RSA family to get N, e, d. The public key pk is $(N, e), k, k_0, k_1$ and the secret key sk is $(N, d), k, k_0, k_1$. The other algorithms are depicted below. Let $G : \{0,1\}^{k_0} \to \{0,1\}^{n+k_1}$ and $H : \{0,1\}^{n+k_1} \to \{0,1\}^{k_0}$ be hash functions. Note that $[x]^n$ denotes the n most significant bits of x and $[x]_m$ denotes the m least significant bits of x.*

```
Algorithm $\mathcal{E}^{\mathsf{RO}}_{pk}(m)$
  $r \overset{R}{\leftarrow} \{0,1\}^{k_0}$
  $s \leftarrow (m || 0^{k_1}) \oplus G(r)$
  $t \leftarrow r \oplus H(s)$
  $c \leftarrow (s||t)^e \bmod N$
  return $c$
```

```
Algorithm $\mathcal{D}^{\mathsf{RO}}_{sk}(c)$
  $s \leftarrow [c^d]^{n+k_1}$; $t \leftarrow [c^d]_{k_0}$
  $r \leftarrow t \oplus H(s)$
  $m \leftarrow [s \oplus G(r)]^n$; $p \leftarrow [s \oplus G(r)]_{k_1}$
  if $(p = 0^{k_1})$ $z \leftarrow m$ else $z \leftarrow \perp$
  return $z$
```

Fujisaki, Okamoto, Pointcheval, and Stern [7] proved that OAEP with partial one-way permutation is secure in the sense of IND-CCA2. They also showed that the RSA family is one-way if and only if the RSA family is θ-partial one-way for $\theta > 0.5$. Thus, RSA-OAEP is secure in the sense of IND-CCA2 assuming the RSA family is one-way.

4.2 Universal Anonymizability of RSA-OAEP

A simple observation that seems to be folklore is that if one publishes the ciphertext of the RSA-OAEP scheme directly (without anonymization) then the scheme does not provide the key-privacy. Suppose an adversary knows that the ciphertext c is created under one of two keys (N_0, e_0) or (N_1, e_1), and suppose $N_0 \leq N_1$. If $c \geq N_0$ 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. In order to construct the schemes with anonymity, it is necessary that the space of ciphertexts is common to each user.

To anonymize ciphertexts of RSA-OAEP, we use the expanding technique. In the expanding technique, if we get the ciphertext, we expand it to the common domain. This technique was proposed by Desmedt [6]. In [8], Galbraith and Mao used this technique for the undeniable signature scheme. In [13], Rivest, Shamir, and Tauman also used this technique for the ring signature scheme.

Definition 10. *Our universal anonymizable RSA-OAEP scheme $\mathcal{UAPE}^{\mathsf{RO}} = ((\mathcal{K}^{\mathsf{RO}}, \mathcal{E}^{\mathsf{RO}}, \mathcal{D}^{\mathsf{RO}}), \mathcal{UA}^{\mathsf{RO}}, \mathcal{DA}^{\mathsf{RO}})$ consists of RSA-OAEP $\mathcal{PE}^{\mathsf{RO}} = (\mathcal{K}^{\mathsf{RO}}, \mathcal{E}^{\mathsf{RO}}, \mathcal{D}^{\mathsf{RO}})$ and two algorithms described as follows.*

```
Algorithm $\mathcal{UA}^{\mathsf{RO}}_{pk}(c)$
  $\alpha \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor (2^{k+160} - c)/N \rfloor\}$
  $c' \leftarrow c + \alpha N$
  return $c'$
```

```
Algorithm $\mathcal{DA}^{\mathsf{RO}}_{sk}(c')$
  $c \leftarrow c' \bmod N$
  $z \leftarrow \mathcal{D}^{\mathsf{RO}}_{sk}(c)$
  return $z$
```

4.3 Security

In this section, we prove that our universal anonymizable RSA-OAEP scheme $\mathcal{UAPE}^{\mathsf{RO}}$ is CCA-secure.

In order to prove that our scheme provides the key-privacy and the data-privacy on anonymized ciphertexts, we need the restriction as follows.

We define the set of ciphertexts $EC_{\mathsf{RO}}(c', pk)$ called "equivalence class" as

$$EC_{\mathsf{RO}}(c', pk) = \{\check{c} \in \{0,1\}^{k+160} | \check{c} = c' \pmod{N}\}.$$

If $c' \in \{0,1\}^{k+160}$ is an anonymized ciphertext of m_0 for $pk_0 = (N_0, e_0, k)$ then any element $\check{c} \in EC_{\mathsf{RO}}(c', pk_0)$ is also an anonymized ciphertext of m_0 under pk_0. Therefore, when c' is a challenge anonymized ciphertext, the adversary can ask an anonymized ciphertext $\check{c} \in EC_{\mathsf{RO}}(c', pk_0)$ to the decryption oracle $\mathcal{DA}^{\mathsf{RO}}_{sk_0}$ for anonymized ciphertexts, and if the answer of $\mathcal{DA}^{\mathsf{RO}}_{sk_0}$ is m_0 then the adversary knows that c' is encrypted by pk_0 and the plaintext of c' is m_0.

Furthermore, since the adversary can compute the standard ciphertext c as $c' \bmod N_0$, the adversary can ask c to the decryption oracle $\mathcal{D}^{\mathsf{RO}}_{sk_0}$ and if the answer of $\mathcal{D}^{\mathsf{RO}}_{sk_0}$ is m_0, then the adversary knows that c' is encrypted by pk_0 and the plaintext of c' is m_0.

To prevent this attack, we add some natural restriction to the adversaries in the definitions of the key-privacy and the data-privacy on anonymized ciphertexts. That is, it is mandated that the adversary never queries either $\check{c} \in EC_{\mathsf{RO}}(c', pk_0)$ to $\mathcal{DA}^{\mathsf{RO}}_{sk_0}$ or $\check{c} \in EC_{\mathsf{RO}}(c', pk_1)$ to $\mathcal{DA}^{\mathsf{RO}}_{sk_1}$. It is also mandated that the adversary never queries either $c' \bmod N_0$ to $\mathcal{D}^{\mathsf{RO}}_{sk_0}$ or $c' \bmod N_1$ to $\mathcal{D}^{\mathsf{RO}}_{sk_1}$.

We think these restrictions are natural and reasonable. Actually, in the case of undeniable and confirmer signature schemes, Galbraith and Mao [8] defined the anonymity on undeniable signature schemes with the above restriction. In [10], Hayashi and Tanaka also employed the same restriction in order to prove anonymity of their encryption scheme.

If we add these restrictions then we can prove that our scheme provides the key-privacy against the adaptive chosen ciphertext attack in the random oracle model assuming RSA family is θ-partial one-way for $\theta > 0.5$. More precisely, we show the following theorem, the proof is in Appendix B.

Theorem 2. *If the RSA family is partial one-way then our scheme $\mathcal{UAPE}^{\mathsf{RO}}$ provides the key-privacy against the adaptive chosen ciphertext attack in the random oracle model. More precisely, for any adversary A attacking the key-privacy of our scheme under the adaptive chosen ciphertext attack, and making at most $q_{\rm dec}$ queries to decryption oracle for standard ciphertexts, $q'_{\rm dec}$ queries to decryption oracle for anonymized ciphertexts, $q_{\rm gen}$ G-oracle queries, and $q_{\rm hash}$ H-oracle queries, there exists a θ-partial inverting adversary B for the RSA family, such that for any $k, k_0(k), k_1(k)$, and $\theta = \frac{k-k_0(k)}{k}$,*

$$\begin{aligned}\mathbf{Adv}^{\text{key-cca}}_{\mathcal{UAPE}^{\mathsf{RO}},A}(k) \le 8q_{\rm hash} \cdot ((1-\epsilon_1)\cdot(1-\epsilon_2))^{-1} \cdot \mathbf{Adv}^{\theta\text{-pow-fnc}}_{\mathsf{RSA},B}(k) \\ + q_{\rm gen} \cdot q_{\rm hash} \cdot (1-\epsilon_2)^{-1} \cdot 2^{-k+2}\end{aligned}$$

where

$$\epsilon_1 = \frac{1}{2^{k/2-3}-1} + \frac{1}{2^{159}}\ ; \quad \epsilon_2 = \frac{2q_{\rm gen} + q_{\rm dec} + q'_{\rm dec} + 2q_{\rm gen}(q_{\rm dec} + q'_{\rm dec})}{2^{k_0}} + \frac{2q_{\rm gen}}{2^{k_1}} + \frac{2q_{\rm hash}}{2^{k-k_0}},$$

and the running time of B is that of A plus $q_{\rm gen} \cdot q_{\rm hash} \cdot O(k^3)$.

We can also prove that our scheme provides the data-privacy on standard ciphertexts against the adaptive chosen ciphertext attack in the random oracle model assuming the RSA family is θ-partial one-way for $\theta > 0.5$. More precisely, we can prove that if there exists a CCA-adversary A attacking the data-privacy on standard ciphertexts of our scheme with advantage ϵ, then there exists a CCA2-adversary B attacking indistinguishability of RSA-OAEP with advantage ϵ. In the reduction of the proof, we have to simulate the decryption oracles for anonymized ciphertexts for A. If A makes a query c' to $\mathcal{DA}_{sk_0}(\cdot)$, we simply compute $c \leftarrow c' \bmod N_0$ and decrypt c by using the decryption algorithm $\mathcal{D}_{sk_0}(\cdot)$ for standard ciphertexts for B. We can simulate $\mathcal{DA}_{sk_1}(\cdot)$ in a similar way.

Furthermore, if we add the restrictions described above, we can prove that our scheme provides the data-privacy on anonymized ciphertexts against the adaptive chosen ciphertext attack in the random oracle model assuming the RSA family is θ-partial one-way for $\theta > 0.5$. More precisely, we can prove that if there exists a CCA-adversary C attacking the data-privacy on anonymized ciphertexts of our scheme with advantage ϵ, then there exists a CCA-adversary A attacking the data-privacy on standard ciphertexts of our scheme with the same advantage ϵ.

In conclusion, since the RSA family is θ-partial one-way if and only if the RSA family is one-way for $\theta > 0.5$, our universal anonymizable RSA-OAEP scheme $\mathcal{UAPE}^{\mathsf{RO}}$ is CCA-secure in the random oracle model assuming the RSA family is one-way.

5 ElGamal and its Universal Anonymizability

In this section, we propose a universal anonymizable ElGamal encryption scheme.

5.1 The ElGamal Encryption Scheme

Definition 11 (ElGamal)**.** *The ElGamal encryption scheme* $\mathcal{PE}^{\mathsf{EG}} = (\mathcal{K}^{\mathsf{EG}}, \mathcal{E}^{\mathsf{EG}}, \mathcal{D}^{\mathsf{EG}})$ *is as follows. Note that* $\mathcal{Q}$ *is 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 *(a group of quadratic residues modulo* p*) of order* q*.*

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

```
Algorithm $\mathcal{E}^{\mathsf{EG}}_{pk}(m)$
  $r \xleftarrow{R} \mathbb{Z}_q$
  $c_1 \leftarrow g^r$
  $c_2 \leftarrow m \cdot y^r$
  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 ElGamal encryption scheme is secure in the sense of IND-CPA if the DDH problem for $\mathcal{Q}$ is hard.

5.2 Universal Anonymizability of the ElGamal Encryption Scheme

We now consider the situation that there exists no common key, and in the above definition of the ElGamal encryption scheme, 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. Therefore, each user U_i uses a different groups G_i for her encryption scheme and if she publishes the ciphertext directly (without anonymization) then the scheme does not provide the key-privacy. In fact, 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. To anonymize the standard ciphertext of the ElGamal encryption scheme, we consider the following strategy in the universal anonymizing algorithm.

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).

We have already used the expanding technique in Section 4. We now describe the encoding function.

The Encoding Function Generally speaking, it is not easy to encode the elements of a prime-order group of order q to those of $\mathbb{Z}_q$. We employ the idea described in [5] by Cramer and Shoup. We can encode the elements of QR_p where $p = 2q + 1$ and p, q are prime to those 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 $\bar{F}_{q,t}^{-1}$.

Our Scheme. We now propose our universal anonymizable ElGamal encryption scheme. Our scheme provides the key-privacy against the chosen plaintext attack 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.

Definition 12. *Our universal anonymizable ElGamal encryption scheme* $\mathcal{UAPE}^{\mathsf{EG}} = ((\mathcal{K}^{\mathsf{EG}}, \mathcal{E}^{\mathsf{EG}}, \mathcal{D}^{\mathsf{EG}}), \mathcal{UA}^{\mathsf{EG}}, \mathcal{DA}^{\mathsf{EG}})$ *consists of the ElGamal encryption scheme* $\mathcal{PE}^{\mathsf{EG}} = (\mathcal{K}^{\mathsf{EG}}, \mathcal{E}^{\mathsf{EG}}, \mathcal{D}^{\mathsf{EG}})$ *and two algorithms described as follows.*

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

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

5.3 Security

In this section, we prove that our universal anonymizable ElGamal encryption scheme $\mathcal{UAPE}^{\mathsf{EG}}$ is CPA-secure.

In order to prove that our scheme provides the key-privacy and the data-privacy on anonymized ciphertexts against the chosen plaintext attack, we need the restrictions similar to those for our universal anonymizable RSA-OAEP scheme. We define the equivalence class for our universal anonymizable ElGamal encryption scheme as follows:

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

It is mandated that the adversary never queries either $(\check{c}_1, \check{c}_2) \in EC_{\mathsf{EG}}((c'_1, c'_2), pk_0)$ to $\mathcal{DA}_{sk_0}$ or $(\check{c}_1, \check{c}_2) \in EC_{\mathsf{EG}}((c'_1, c'_2), pk_1)$ to $\mathcal{DA}_{sk_1}$. It is also mandated that the adversary never queries either $\bar{F}_{q_0,2}^{-1}(c'_1 \bmod q_0, c'_2 \bmod q_0)$ to $\mathcal{D}_{sk_0}$ or $\bar{F}_{q_1,2}^{-1}(c'_1 \bmod q_1, c'_2 \bmod q_1)$ to $\mathcal{D}_{sk_1}$.

We prove the following theorem with the above restrictions. The proof of the following theorem is in Appendix C.

Theorem 3. *Our universal anonymizable ElGamal encryption scheme provides the key-privacy against the chosen plaintext attack if the DDH problem for $\mathcal{Q}$ is hard.*

We can also prove that our scheme provides the data-privacy on standard ciphertexts and that on anonymized ciphertexts against the chosen plaintext attack if the DDH problem for $\mathcal{Q}$ is hard. The reductions in these proofs are similar to those in the proofs for our universal anonymizable RSA-OAEP scheme.

In conclusion, our universal anonymizable ElGamal encryption scheme $\mathcal{UAPE}^{\mathsf{EG}}$ is CPA-secure assuming that the DDH problem for $\mathcal{Q}$ is hard.

6 Cramer-Shoup and its Universal Anonymizability

In this section, we propose a universal anonymizable Cramer-Shoup encryption scheme.

6.1 The Cramer-Shoup Encryption Scheme

Definition 13 (Cramer-Shoup)**.** *The Cramer-Shoup encryption scheme $\mathcal{PE}^{\mathsf{CS}} = (\mathcal{K}^{\mathsf{CS}}, \mathcal{E}^{\mathsf{CS}}, \mathcal{D}^{\mathsf{CS}})$ is defined as follows. Note that $\mathcal{Q}$ is a QR-group generator with safe prime and $\mathcal{H} = (\mathcal{GH}, \mathcal{EH})$ be a family of hash functions (See Appendix D for families of hash functions.).*

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

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

```
Algorithm $\mathcal{D}_{sk}^{\mathsf{CS}}(u_1, u_2, e, v)$
  $\alpha \leftarrow \mathcal{EH}_K(u_1, u_2, e)$
  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 [5] proved that the Cramer-Shoup encryption scheme is secure in the sense of IND-CCA2 assuming that $\mathcal{H}$ is universal one-way (See Appendix D for universal one-way.) and the DDH problem for $\bar{\mathcal{Q}}$ is hard. Lucks [12] recently proposed a variant of the Cramer-Shoup encryption scheme for groups of unknown order. This scheme is secure in the sense of IND-CCA2 assuming that the family of hash functions in the scheme is universal one-way, and both the Decisional Diffie-Hellman problem in QR_N (a set of quadratic residues modulo N) and factoring N are hard.

6.2 Universal Anonymizability of the Cramer-Shoup Encryption Scheme

We propose our universal anonymizable Cramer-Shoup encryption scheme. Our scheme provides the key-privacy against the adaptive chosen ciphertext attack 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 our scheme we employ the expanding technique in Section 4 and the encoding function in Section 5.

Definition 14. *Our universal anonymizable Cramer-Shoup encryption scheme $\mathcal{UAPE}^{\mathsf{CS}} = ((\mathcal{K}^{\mathsf{CS}}, \mathcal{E}^{\mathsf{CS}}, \mathcal{D}^{\mathsf{CS}}), \mathcal{UA}^{\mathsf{CS}}, \mathcal{DA}^{\mathsf{CS}})$ consists of the Cramer-Shoup encryption scheme $\mathcal{PE}^{\mathsf{CS}} = (\mathcal{K}^{\mathsf{CS}}, \mathcal{E}^{\mathsf{CS}}, \mathcal{D}^{\mathsf{CS}})$ and* *two algorithms described as follows.*

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

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

6.3 Security

In this section, we prove that our universal anonymizable Cramer-Shoup encryption scheme $\mathcal{UAPE}^{\mathsf{EG}}$ is CCA-secure.

In order to prove that our scheme provides the key-privacy against the adaptive chosen ciphertext attack, we need to add restrictions similar to those for our universal anonymizable ElGamal encryption scheme. We define the equivalence class for our universal anonymizable Cramer-Shoup scheme as follows:

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

We can prove the following theorem with the above restrictions. The proof of the following theorem is in Appendix E and see Appendix D for collision resistant.

Theorem 4. *Our universal anonymizable Cramer-Shoup encryption scheme provides the key-privacy against the adaptive chosen ciphertext attack if the DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is collision resistant.*

We can also prove that our scheme provides the data-privacy on standard ciphertexts and that on anonymized ciphertexts against the adaptive chosen ciphertext attack if the DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is universal one-way. The reductions in these proofs are similar to those in the proofs for our universal anonymizable RSA-OAEP scheme.

In conclusion, since if $\mathcal{H}$ is collision resistant then $\mathcal{H}$ is universal one-way, our universal anonymizable Cramer-Shoup encryption scheme $\mathcal{UAPE}^{\mathsf{CS}}$ is CCA-secure assuming that the DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is collision resistant.

7 Conclusion

We have proposed the notion of universal anonymizable public-key encryption. We have also proposed the universal anonymizable public-key encryption schemes based on RSA-OAEP, the ElGamal encryption, and the Cramer-Shoup encryption schemes, and prove their security.

References

[1] Bellare, M., Boldyreva, A., Desai, A., and Pointcheval, D. Key-Privacy in Public-Key Encryption. In Boyd [3], pp. 566–582. Full version of this paper, available via `http://www-cse.ucsd.edu/users/mihir/`.

[2] Bellare, M., and Rogaway, P. Optimal Asymmetric Encryption – How to Encrypt with RSA. In *Advances in Cryptology – EUROCRYPT '94* (Perugia, Italy, May 1994), A. De Santis, Ed., vol. 950 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 92–111.

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

[4] 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.

[5] 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.

[6] 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.

[7] Fujisaki, E., Okamoto, T., Pointcheval, D., and Stern, J. RSA-OAEP is Secure under the RSA Assumption. In *Advances in Cryptology – CRYPTO 2001* (Santa Barbara, California, USA, August 2001), J. Kilian, Ed., vol. 2139 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 260–274.

[8] 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.

[9] 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, 7th International Workshop on Theory and Practice in Public Key Cryptography* (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.

[10] Hayashi, R., and Tanaka, K. The Sampling Twice Technique for the RSA-based Cryptosystems with Anonymity. In *Public Key Cryptography – PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography* (Les Diablerets, Switzerland, January 2005), S. Vaudenay, Ed., vol. 3386 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 216–233.

[11] 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.

[12] Lucks, S. A Variant of the Cramer-Shoup Cryptosystem for Groups of Unknown Order. In *Advances in Cryptology – ASIACRYPT 2002* (Queenstown, New Zealand, December 2002), Y. Zheng, Ed., vol. 2501 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 27–45.

[13] Rivest, R. L., Shamir, A., and Tauman, Y. How to Leak a Secret. In Boyd [3], pp. 552–565.

[14] Sako, K. An Auction Protocol Which Hides Bids of Losers. In *Public Key Cryptography – PKC 2000, 3rd International Workshop on Theory and Practice in Public Key Cryptography* (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

It is easy to see that if the paired DDH problem for $\mathcal{G}$ is hard then the DDH problem for $\mathcal{G}$ is hard.

We now consider the opposite direction. We assume that there exists an algorithm D for the paired-DDH problem such that the advantage $\mathbf{Adv}^{\text{pddh}}_{\mathcal{G},D}(k)$ is non-neglibigle. By using the algorithm D, we construct an algorithm D' for the DDH problem as follows:

```
Algorithm $D'(q,g,X,Y,T)$
  $i \overset{R}{\leftarrow} \{0,1\}$
  if $(i=0)$
    $(q_0,g_0) \leftarrow \mathcal{G}(k)$; $x_0,y_0 \overset{R}{\leftarrow} \mathbb{Z}_{q_0}$; $X_0 \leftarrow g_0^{x_0}$; $Y_0 \leftarrow g_0^{y_0}$; $T_0 \leftarrow g_0^{x_0y_0}$
    $(q_1,g_1,X_1,Y_1,T_1) \leftarrow (q,g,X,Y,T)$
    $d \leftarrow D((q_0,g_0,X_0,Y_0,T_0),(q_1,g_1,X_1,Y_1,T_1))$
  else
    $(q_0,g_0,X_0,Y_0,T_0) \leftarrow (q,g,X,Y,T)$
    $(q_1,g_1) \leftarrow \mathcal{G}(k)$; $x_1,y_1,z_1 \overset{R}{\leftarrow} \mathbb{Z}_{q_1}$; $X_1 \leftarrow g_1^{x_1}$; $Y_1 \leftarrow g_1^{y_1}$; $T_1 \leftarrow g_1^{z_1}$
    $d \leftarrow D((q_0,g_0,X_0,Y_0,T_0),(q_1,g_1,X_1,Y_1,T_1))$
  return $d$
```

Furthermore, we consider the additional experiment as follows:

```
Experiment $\mathbf{Exp}^{\text{pddh-temp}}_{\mathcal{G},D}(k)$
  $(q_0,g_0) \leftarrow \mathcal{G}(k)$; $x_0,y_0 \overset{R}{\leftarrow} \mathbb{Z}_{q_0}$; $X_0 \leftarrow g_0^{x_0}$; $Y_0 \leftarrow g_0^{y_0}$; $T_0 \leftarrow g_0^{x_0y_0}$
  $(q_1,g_1) \leftarrow \mathcal{G}(k)$; $x_1,y_1 \overset{R}{\leftarrow} \mathbb{Z}_{q_1}$; $X_1 \leftarrow g_1^{x_1}$; $Y_1 \leftarrow g_1^{y_1}$; $T_1 \overset{R}{\leftarrow} G_{q_1}$
  $d \leftarrow D((q_0,g_0,X_0,Y_0,T_0),(q_1,g_1,X_1,Y_1,T_1))$
  return $d$
```

Then, we have

$$\begin{aligned}
\mathbf{Adv}^{\text{ddh}}_{\mathcal{G},D'}(k) &= |\Pr[\mathbf{Exp}^{\text{ddh-real}}_{\mathcal{G},D'}(k)=1] - \Pr[\mathbf{Exp}^{\text{ddh-rand}}_{\mathcal{G},D'}(k)=1]| \\
&= |\tfrac{1}{2}(\Pr[\mathbf{Exp}^{\text{ddh-real}}_{\mathcal{G},D'}(k)=1|i=0] + \Pr[\mathbf{Exp}^{\text{ddh-real}}_{\mathcal{G},D'}(k)=1|i=1]) \\
&\quad - \tfrac{1}{2}(\Pr[\mathbf{Exp}^{\text{ddh-rand}}_{\mathcal{G},D'}(k)=1|i=0] + \Pr[\mathbf{Exp}^{\text{ddh-rand}}_{\mathcal{G},D'}(k)=1|i=1])| \\
&= |\tfrac{1}{2}(\Pr[\mathbf{Exp}^{\text{pddh-real}}_{\mathcal{G},D}(k)=1] + \Pr[\mathbf{Exp}^{\text{pddh-temp}}_{\mathcal{G},D}(k)=1]) \\
&\quad - \tfrac{1}{2}(\Pr[\mathbf{Exp}^{\text{pddh-temp}}_{\mathcal{G},D}(k)=1] + \Pr[\mathbf{Exp}^{\text{pddh-rand}}_{\mathcal{G},D}(k)=1])| \\
&= \tfrac{1}{2}|\Pr[\mathbf{Exp}^{\text{pddh-real}}_{\mathcal{G},D}(k)=1] - \Pr[\mathbf{Exp}^{\text{pddh-rand}}_{\mathcal{G},D}(k)=1]|. \\
&= \tfrac{1}{2}\mathbf{Adv}^{\text{pddh}}_{\mathcal{G},D}(k).
\end{aligned}$$

Therefore, the advantage of D' is non-negligible.

B Proof of Theorem 2

We first describe the RSA partial inverting algorithm M using a CCA-adversary A attacking anonymity of our encryption scheme. M is given $pk=(N,e,k)$ and a point $y \in \mathbb{Z}_N^*$ where $|y| = k = n+k_0+k_1$. Let $sk=(N,d,k)$ be the corresponding secret key. The algorithm is trying to find the $n+k_1$ most significant bits of the e-th root of y modulo N.

1) M picks a bit $\mu \overset{R}{\leftarrow} \{0,1,2,\ldots,\lfloor(2^{k+160}-y)/N\rfloor\}$ and sets $Y \leftarrow y+\mu N$.

2) M runs the key generation algorithm of the RSA family with security parameter k to obtain $pk'=(N',e',k)$ and $sk'=(N',d',k)$. Then it picks a bit $b \overset{R}{\leftarrow} \{0,1\}$, sets $pk_b \leftarrow (N,e)$ and $pk_{1-b} \leftarrow (N',e')$. If the above y does not satisfy $y \in (\mathbb{Z}^*_{N_0} \cap \mathbb{Z}^*_{N_1})$ then M outputs Fail and halts; else it continues.

3) M initializes for lists, called G-list, H-list, Y_0-list, and Y_1-list to empty. It then runs A as follows. Note that M simulates A's oracles G, H, $\mathcal{D}_{sk_0}$, and $\mathcal{D}_{sk_1}$ as described below.

   3-1) M runs $A_1(pk_0, pk_1)$ and gets (m_0, m_1, si) which is the output of A_1.

   3-2) M runs $A_2(Y, \mathsf{si})$ and gets a bit $d \in \{0, 1\}$ which is the output of A_2.

4) M chooses a random element on the H-list and outputs it as its guess for the $n + k_1$ most significant bits of the e-th root of y modulo N.

M simulates the random oracles G and H, and the decryption oracle as follows:

- When A makes an oracle query g to G, then for each (h, H_h) on the H-list, M builds $z = h||(g \oplus H_h)$, and computes $y_{h,g,0} = z^{e_0} \bmod N_0$ and $y_{h,g,1} = z^{e_1} \bmod N_1$. For $i \in \{0, 1\}$, M checks whether $y = y_{h,g,i}$. If for some h and i such a relation holds, then we have inverted y under pk_i, and we can still correctly simulate G by answering $G_g = h \oplus (m_i||0^{k_1})$. Otherwise, M outputs a random value G_g of length $n + k_1$. In both cases, M adds (g, G_g) to the G-list. Then, for all h, M checks if the k_1 least significant bits of $h \oplus G_g$ are all 0. If they are, then it adds $y_{h,g,0}$ and $y_{h,g,1}$ to the Y_0-list and the Y_1-list, respectively.

- When A makes an oracle query h to H, M provides A with a random string H_h of length k_0 and adds (h, H_h) to the H-list. Then for each (g, G_g) on the G-list, M builds $z = h||(g \oplus H_h)$, and computes $y_{h,g,0} = z^{e_0} \bmod N_0$ and $y_{h,g,1} = z^{e_1} \bmod N_1$. M checks if the k_1 least significant bits of $h \oplus G_g$ are all 0. If they are, then it adds $y_{h,g,0}$ and $y_{h,g,1}$ to the Y_0-list and the Y_1-list, respectively.

- When for $i \in \{0, 1\}$, A makes an oracle query $\hat{y} \in \mathbb{Z}_{N_i}^*$ to $\mathcal{D}_{sk_i}$, M checks if there exists some $y_{h,g,i}$ in the Y_i-list such that $\hat{y} = y_{h,g,i}$. If there is, then it returns the n most significant bits of $h \oplus G_g$ to A. Otherwise it returns $\perp$ (indicating that $\hat{y}$ is an invalid ciphertext).

- When for $i \in \{0, 1\}$, A makes an oracle query $\hat{Y} \in \{0, 1\}^{k+160}$ to $\mathcal{DA}_{sk_i}$, M checks if there exists some $y_{h,g,i}$ in the Y_i-list such that $\hat{Y} \bmod N_i = y_{h,g,i}$. If there is, then it returns the n most significant bits of $h \oplus G_g$ to A. Otherwise it returns $\perp$ (indicating that $\hat{Y}$ is an invalid anonymized ciphertext).

Now, we analyze the advantage of M. For $i \in \{0, 1\}$, let $w_i = y^{d_i} \bmod N_i$, $s_i = [w_i]^{n+k_1}$, and $t_i = [w_i]_{k_0}$. Let r_i be the random variable $t_i \oplus H(s_i)$. We consider the following events.

- FBad denotes the event that
  - A G-oracle query r_0 was made by A_1 in step 3-1, and $G_{r_0} \neq s_0 \oplus (x||0^{k_1})$, or
  - A G-oracle query r_1 was made by A_1 in step 3-1, and $G_{r_1} \neq s_1 \oplus (x||0^{k_1})$.

- GBad denotes the event that
  - A G-oracle query r_0 was made by A_2 in step 3-2, and at the point in time that it was made, the H-oracle query s_0 was not on the H-list, and $G_{r_0} \neq s_0 \oplus (x||0^{k_1})$, or
  - A G-oracle query r_1 was made by A_2 in step 3-2, and at the point in time that it was made, the H-oracle query s_1 was not on the H-list, and $G_{r_1} \neq s_1 \oplus (x||0^{k_1})$.

- DABad denotes the event that
  - A $\mathcal{DA}_{sk_0}$ query is not correctly answered, or
  - A $\mathcal{DA}_{sk_1}$ query is not correctly answered.

- DSBad denotes the event that

  - A $\mathcal{D}_{sk_0}$ query is not correctly answered, or
  - A $\mathcal{D}_{sk_1}$ query is not correctly answered.

- $\mathsf{DBad} = \mathsf{DABad} \vee \mathsf{DSBad}$.
- $\mathsf{G} = \neg\mathsf{FBad} \wedge \neg\mathsf{GBad} \wedge \neg\mathsf{DBad}$.

We let $\Pr[\cdot]$ denote the probability distribution in the game defining advantage. We introduce the following additional events:

- YBad denotes the event that $y \in (\mathbb{Z}_{N_0}^* \cap \mathbb{Z}_{N_1}^*)$.
- FAskS denotes the event that H-oracle query s_0 or s_1 was made by A_1 in step 3-1.
- AskR denotes the event that (r_0, G_{r_0}) or (r_1, G_{r_1}) is on the G-list at the end of step 3-2.
- AskS denotes the event that (s_0, H_{s_0}) or (s_1, H_{s_1}) is on the H-list at the end of step 3-2.

Let $\Pr_1[\cdot]$ denote the probability distribution in the simulated game where $\neg\mathsf{YBad}$ occurs.

We can bound $\Pr_1[\mathsf{AskS}]$ in a similar way as in the proof of anonymity for RSA-RAEP [1], and we have

$$\Pr_1[\mathsf{AskS}] \geq \frac{1}{2} \cdot \Pr_1[\mathsf{AskR} \wedge \mathsf{AskS} | \neg\mathsf{DBad}] \cdot \Pr_1[\neg\mathsf{DBad} | \neg\mathsf{AskS}].$$

We next bound $\Pr_1[\mathsf{AskR} \wedge \mathsf{AskS} | \neg\mathsf{DBad}]$. Let $\Pr_2[\cdot]$ denote the probability distribution in the simulated game where $\neg\mathsf{DBad} \wedge \neg\mathsf{YBad}$ occurs.

The proof of the following lemma is similar to that for RSA-RAEP.

Lemma 1.

$$\Pr_2[\mathsf{AskR} \wedge \mathsf{AskS}] \geq \frac{\epsilon}{2} \cdot \left(1 - 2q_{\text{gen}} \cdot 2^{-k_0} - 2q_{\text{hash}} \cdot 2^{-n-k_1}\right) - 2q_{\text{gen}} \cdot 2^{-k}.$$

We next bound $\Pr_1[\neg\mathsf{DBad} | \neg\mathsf{AskS}]$. It is easy to see that

$$\Pr_1[\neg\mathsf{DBad} | \neg\mathsf{AskS}] \leq \Pr_1[\neg\mathsf{DABad} | \neg\mathsf{AskS}] + \Pr_1[\neg\mathsf{DSBad} | \neg\mathsf{AskS}].$$

The proof of the following lemma is similar to that for RSA-RAEP.

Lemma 2.

$$\Pr_1[\mathsf{DSBad} | \neg\mathsf{AskS}] \leq q_{\text{dec}} \cdot \left(2 \cdot 2^{-k_1} + (2q_{\text{gen}} + 1) \cdot 2^{-k_0}\right).$$

Furthermore, we can prove the following lemma in a similar way as that for Lemma 2.

Lemma 3.

$$\Pr_1[\mathsf{DABad} | \neg\mathsf{AskS}] \leq q'_{\text{dec}} \cdot \left(2 \cdot 2^{-k_1} + (2q_{\text{gen}} + 1) \cdot 2^{-k_0}\right).$$

By applying Lemmas 1, 2, and 3, we have

$$\begin{aligned} \Pr_1[\mathsf{AskS}] &\geq \frac{1}{2} \cdot \left(\frac{\epsilon}{2} \cdot \left(1 - \frac{2q_{\text{gen}}}{2^{k_0}} - \frac{2q_{\text{hash}}}{2^{n+k_1}}\right) - \frac{2q_{\text{gen}}}{2^k}\right) \cdot \left(1 - (q_{\text{dec}} + q'_{\text{dec}}) \cdot \left(\frac{2}{2^{k_1}} + \frac{2q_{\text{gen}} + 1}{2^{k_0}}\right)\right) \\ &\geq \frac{\epsilon}{4} \cdot \left(\frac{2q_{\text{gen}} + q_{\text{dec}} + q'_{\text{dec}} + 2q_{\text{gen}}(q_{\text{dec}} + q'_{\text{dec}})}{2^{k_0}} + \frac{2q_{\text{gen}}}{2^{k_1}} + \frac{2q_{\text{hash}}}{2^{k-k_0}}\right) - \frac{q_{\text{gen}}}{2^k}. \end{aligned}$$

Assuming $\neg\mathsf{YBad}$, we have by the random choice of b and symmetry, that the probability of M outputting s is at least $\frac{1}{2q_{\text{hash}}} \cdot \Pr_1[\mathsf{AskS}]$.

We next bound the probabilities that $\neg\mathsf{YBad}$ occurs.

Lemma 4.

$$\Pr[\mathsf{YBad}] \leq \frac{2}{2^{k/2-3}-1} + \frac{1}{2^{159}}.$$

Proof of Lemma 4. Let $N = pq$ and $N' = p'q'$. Note that $2^{\lceil k/2 \rceil -1} < p, q, p', q' < 2^{\lceil k/2 \rceil}$ and $2^{k-1} < N, N' < 2^k$. We define a set $S[N]$ as $\{\tilde{Y} | \tilde{Y} \in [0, 2^{k+160}) \wedge (\tilde{Y} \bmod N) \in S[N]\}$. Then, we have

$$\begin{aligned}\Pr[\mathsf{YBad}] &= \Pr[y \overset{R}{\leftarrow} \mathbb{Z}_N^*;\ \mu \overset{R}{\leftarrow} \{0,1,2,\ldots,\lfloor (2^{k+160}-y)/N \rfloor\};\ Y \leftarrow y + \mu N :\ Y \notin S[N']] \\ &\leq \Pr[Y' \overset{R}{\leftarrow} S[N] :\ Y' \notin S[N']] + 1/2^{159}\end{aligned}$$

since the distribution of Y' is statistically indistinguishable from that of Y, and the statistically distance is less than $1/2^{159}$.

Since $\phi(N) \leq |S[N]| \leq 2^k$, we have

$$\Pr[Y' \overset{R}{\leftarrow} S[N] :\ Y' \notin S[N']] \leq \frac{|S[N]| - |S[N']|}{|S[N]|} \leq \frac{2^k - |S[N']|}{\phi(N)}.$$

Furthermore, we have

$$\begin{aligned}2^k - |S[N']| &= \left|\{Y' | Y' \in [0, 2^k) \wedge (Y' \bmod N') \notin \mathbb{Z}_{N'}^*\}\right| \\ &\leq \left|\{Y' | Y' \in [0, 2N') \wedge (Y' \bmod N') \notin \mathbb{Z}_{N'}^*\}\right| \\ &= 2 \times \left|\{Y' | Y' \in [0, N') \wedge Y' \notin \mathbb{Z}_{N'}^*\}\right| \\ &= 2(N' - \phi(N')).\end{aligned}$$

Therefore, we can bound $\Pr[Y' \overset{R}{\leftarrow} S[N] :\ Y' \notin S[N']]$ as

$$\begin{aligned}\Pr[Y' \overset{R}{\leftarrow} S[N] :\ Y' \notin S[N']] &\leq \frac{2^k - |S[N']|}{\phi(N)} \leq \frac{2(N' - \phi(N'))}{\phi(N)} = \frac{2(p'+q'-1)}{N-p-q+1} \leq \frac{2(p'+q')}{N-p-q} \\ &\leq \frac{2(2^{\lceil k/2 \rceil} + 2^{\lceil k/2 \rceil})}{2^{k-1} - 2^{\lceil k/2 \rceil} - 2^{\lceil k/2 \rceil}} = \frac{2(1+1)}{2^{k-1-\lceil k/2 \rceil} - 1 - 1} \leq \frac{4}{2^{k/2-2} - 2} = \frac{2}{2^{k/2-3}-1}.\end{aligned}$$

□

We have that

$$\mathbf{Adv}_{\mathsf{RSA},B}^{\theta\text{-pow-fnc}}(k) \geq (1 - \Pr[\mathsf{YBad}]) \cdot \left(\frac{\Pr_1[\mathsf{AskS}]}{2q_{\text{hash}}} \right).$$

Substituting the bounds for the above probabilities and re-arranging the terms, we get the claimed result.

Finally, we estimate the time complexity of M. It is the time complexity of A plus the time for simulating the random oracles. In the random oracle simulation, for each pair $((g, G_g), (h, H_h))$, it is sufficient to compute $y_{h,g,0} = z^{e_0} \bmod N_0$ and $y_{h,g,1} = z^{e_1} \bmod N_1$. Therefore, the time complexity of M is that of A plus $q_{\text{gen}} \cdot q_{\text{hash}} \cdot O(k^3)$.

C Proof of Theorem 3

Since the DDH problem is hard if and only if the paired DDH problem is hard, we construct a distinguisher D for the paired DDH problem for $\mathcal{Q}$ in Figure 1. In this algorithm, we employ an adversary A attacking the key-privacy of our universal anonymizable ElGamal encryption scheme.

Now we analyze D. First we consider $\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-real}}(k)$. 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

```
Algorithm $D((q_0,g_0,X_0,Y_0,T_0),(q_1,g_1,X_1,Y_1,T_1))$
  $pk_0 \leftarrow (q_0,g_0,X_0)$; $pk_1 \leftarrow (q_1,g_1,X_1)$
  $(m_0,m_1,\mathsf{si}) \leftarrow A^1_{\rm cpa}(pk_0,pk_1)$
  $b \overset{R}{\leftarrow} \{0,1\}$
  $(\bar{c}_1,\bar{c}_2) \leftarrow \bar{F}_{q_b,2}(Y_b,T_b \cdot m_b)$
  $t_1 \leftarrow \{0,1,2,\cdots,\lfloor(2^{k+160}-\bar{c}_1)/q_b\rfloor\}$;   $t_2 \leftarrow \{0,1,2,\cdots,\lfloor(2^{k+160}-\bar{c}_2)/q_b\rfloor\}$
  $c'_1 \leftarrow \bar{c}_1 + t_1 q_b$; $c'_2 \leftarrow \bar{c}_2 + t_2 q_b$
  $d \leftarrow A^2_{\rm cpa}((c'_1,c'_2),\mathsf{si})$
  if $(b = d)$ then return 1 else return 0
```

Figure 1: Distinguisher for Theorem 3

the proper distribution of public keys for our universal anonymizable ElGamal encryption scheme. Furthermore, the challenge ciphertext has the right form under the public key pk_b. Hence,

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

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 universal anonymizable ElGamal encryption scheme. 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 $(\{0,1\}^{k+160})^2$. 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, and 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

$$\mathbf{Adv}^{\text{pddh}}_{\mathcal{Q},D}(k) \geq \frac{1}{2}\mathbf{Adv}^{\text{key-cpa}}_{\mathcal{UAPE}^{\mathsf{EG}},A}(k) - \frac{1}{2^{2(k-2)}} - \left(\frac{1}{2^{159}}\right)^2.$$

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

D Families of Hash Functions

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

Definition 15. *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 16. *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 17. *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.

E Proof of Theorem 4

Since the DDH problem is hard if and only if the paired DDH problem is hard, we construct a distinguisher D for the paired DDH problem for $\mathcal{Q}$ in Figure 2. In this algorithm, we employ an adversary A attacking the key-privacy of our universal anonymizable Cramer-Shoup encryption scheme. 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 $\mathcal{DA}_{sk_i}$ $(i \in \{0, 1\})$, 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 $\tilde{m} \leftarrow \perp$
```

Similarly, 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:

```
$\tilde{\alpha} \leftarrow \mathcal{EH}_{K_i}(\tilde{u}_1, \tilde{u}_2, \tilde{e})$
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 5.

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

```
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
    $g_{1,j} \leftarrow g_j;\ \ g_{2,j} \leftarrow X_j;\ \ u_{1,j} \leftarrow Y_j;\ \ u_{2,j} \leftarrow T_j$
    $x_{1,j},\ x_{2,j},\ y_{1,j},\ y_{2,j},\ z_{1,j},\ z_{2,j} \overset{R}{\leftarrow} \mathbb{Z}_{q_j}$
    $c_j \leftarrow (g_{1,j})^{x_{1,j}}(g_{2,j})^{x_{2,j}};\ \ d_j \leftarrow (g_{1,j})^{y_{1,j}}(g_{2,j})^{y_{2,j}};\ \ h_j \leftarrow (g_{1,j})^{z_{1,j}}(g_{2,j})^{z_{2,j}}$
    $K_j \leftarrow \mathcal{GH}(k)$
    $pk_j \leftarrow (g_{1,j}, g_{2,j}, c_j, d_j, h_j, K_j)$
    $sk_j \leftarrow (x_{1,j}, x_{2,j}, y_{1,j}, y_{2,j}, z_{1,j}, z_{2,j})$
  $(m_0, m_1, \mathsf{si}) \leftarrow A^1_{\mathrm{cca}}(pk_0, pk_1)$
  $b \overset{R}{\leftarrow} \{0, 1\}$
  $e \leftarrow (u_{1,b})^{z_{1,b}}(u_{2,b})^{z_{2,b}} m_b$
  $\alpha \leftarrow \mathcal{EH}_{K_b}(u_{1,b}, u_{2,b}, e)$
  $v \leftarrow (u_{1,b})^{x_{1,b}+\alpha y_{1,b}}(u_{2,b})^{x_{2,b}+\alpha y_{2,b}}$
  $(\bar{u_1}, \bar{u_2}, \bar{e}, \bar{v}) \leftarrow \bar{F}_{q_b,4}(u_{1,b}, u_{2,b}, e, v)$
  $t_1 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{u_1})/q_b\rfloor\};\quad t_2 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{u_2})/q_b\rfloor\}$
  $t_3 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{e})/q_b\rfloor\};\quad t_4 \overset{R}{\leftarrow} \{0, 1, 2, \cdots, \lfloor(2^{k+160} - \bar{v})/q_b\rfloor\}$
  $u'_1 \leftarrow \bar{u_1} + t_1 q_b;\ \ u'_2 \leftarrow \bar{u_2} + t_2 q_b;\ \ e' \leftarrow \bar{e} + t_3 q_b;\ \ v' \leftarrow \bar{v} + t_4 q_b$
  $d \leftarrow A^2_{\mathrm{cca}}((u'_1, u'_2, e', v'), \mathsf{si})$
  if $(b = d)$ then return 1 else return 0
```

Figure 2: Distinguisher for Theorem 4

Lemma 6. *There exists an adversary C attacking the collision-resistance of $\mathcal{H}$ such that*

$$\Pr[\mathbf{Exp}^{\text{pddh-rand}}_{\mathcal{Q},D}(k) = 1] \leq \frac{1}{2} + \frac{q_d(k) + q'_d(k) + 2}{2^{k-4}} + 4\mathbf{Adv}^{\text{cr}}_{\mathcal{H},C}(k) + \left(\frac{1}{2^{159}}\right)^4,$$

where $q_d(k)$ is the number of decryption query to $\mathcal{DA}_{sk}$ and $q'_d(k)$ is the number of decryption query to $\mathcal{D}_{sk}$, and whose time-complexity is bounded by that of A plus $O(k^3)$.

Proof of Theorem 4. The statement follows from the above two lemmas. More concretely, we have

$$\mathbf{Adv}^{\text{pddh}}_{\mathcal{Q},D}(k) \geq \frac{1}{2}\mathbf{Adv}^{\text{key-cca}}_{\mathcal{UAPE}^{\mathsf{CS}},A}(k) - \frac{q_d(k) + q'_d(k) + 2}{2^{k-4}} - 4\mathbf{Adv}^{\text{cr}}_{\mathcal{H},C}(k) - \left(\frac{1}{2^{159}}\right)^4.$$

□

E.1 Proof of Lemma 5

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 $e = g_{1,b}^{r_{1,b}\bar{z}_b} m_b$ 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 $M = e/g_{1,i}^{r_{1,i}\tilde{z}_i} = e/h_i^{r_{1,i}}$, the output of decryption oracle in the simulation demonstrates that of the actual decryption oracle.

E.2 Proof of Lemma 6

In the experiment $\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k)$, the distribution of challenge ciphertexts is statistically indistinguishable from the uniform distribution over $(\{0,1\}^{k+160})^4$, and the statistically distance is less than $(1/2^{159})^4$.

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 $\log_{g_{1,i}} \tilde{u}_1 \neq \log_{g_{2,i}} \tilde{u}_2$. Furthermore, we say the anonymized ciphertext $\mathcal{UA}_{pk}(\tilde{u}_1, \tilde{u}_2, \tilde{e}, \tilde{v})$ is invalid when $(\tilde{u}_1, \tilde{u}_2, \tilde{e}, \tilde{v})$ is invalid. 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 anonymized ciphertext to the oracle $\mathcal{DA}_{sk_0}$ or $\mathcal{DA}_{sk_1}$ and does not get $\perp$, or submits an invalid ciphertext to the oracle $\mathcal{D}_{sk_0}$ or $\mathcal{D}_{sk_1}$ and does not get $\perp$.

Lemma 7. $\Pr[\mathsf{NR}] \leq 1/2^{k-3}$.

Lemma 8. *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 9. *There exists a polynomial-time adversary C such that*

$$\Pr[\mathsf{Inv} | \neg\mathsf{NR}] \leq 4\mathbf{Adv}_{\mathcal{H},C}^{\text{cr}}(k) + \frac{q_d(k) + q_d'(k)}{2^{k-3}}.$$

Proof of Lemma 6.

$$\begin{aligned}
&\Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1] \\
&\quad = \frac{1}{2}\Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 0] + \frac{1}{2}\Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 1] \\
&\quad \leq \Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 0 \wedge \neg\mathsf{NR} \wedge \neg\mathsf{Inv}] \\
&\qquad + \Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 1 \wedge \neg\mathsf{NR} \wedge \neg\mathsf{Inv}] + \Pr[\mathsf{NR}] + \Pr[\mathsf{Inv}] + \left(\frac{1}{2^{159}}\right)^4 \\
&\quad \leq \Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 0 \wedge \neg\mathsf{NR} \wedge \neg\mathsf{Inv}] \\
&\qquad + \Pr[\mathbf{Exp}_{\mathcal{Q},D}^{\text{pddh-rand}}(k) = 1 | b = 1 \wedge \neg\mathsf{NR} \wedge \neg\mathsf{Inv}] + 2\Pr[\mathsf{NR}] + \Pr[\mathsf{Inv} | \neg\mathsf{NR}] + \left(\frac{1}{2^{159}}\right)^4 \\
&\quad \leq \frac{1}{2} + \frac{1}{2^{k-4}} 4\mathbf{Adv}_{\mathcal{H},C}^{\text{cr}}(k) + \frac{q_d(k) + q_d'(k)}{2^{k-3}} + \left(\frac{1}{2^{159}}\right)^4 \\
&\quad = \frac{1}{2} + \frac{q_d(k) + q_d'(k) + 2}{2^{k-4}} + 4\mathbf{Adv}_{\mathcal{H},C}^{\text{cr}}(k) + \left(\frac{1}{2^{159}}\right)^4
\end{aligned}$$

where 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. □

E.2.1 Proof of Lemma 7

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 $\Pr[\mathsf{NR}] \leq 2/q_0 + 2/q_1 \leq 1/2^{k-3}$.

E.2.2 Proof of Lemma 8

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

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

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 $\mathbf{Exp}^{\text{pddh-rand}}_{Q,D}(k)$. 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 $\mathbf{Exp}^{\text{pddh-rand}}_{Q,D}(k)$ 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 10. *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 8. Lemma 10 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 10. 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:

$$\begin{aligned} e &= u_{1,0}^{z_{1,0}} u_{2,0}^{z_{2,0}} m_0 && \pmod{p_0} \\ v &= u_{1,0}^{x_{1,0}+\alpha y_{2,0}} u_{2,0}^{x_{2,0}+\alpha y_{2,0}} && \pmod{p_0} \end{aligned}$$

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 $E_0 \subseteq S_0$.):

$$\begin{array}{rcllr}
g_{1,0} & = & \hat{g}_{1,0} & \pmod{p_0} & (1) \\
g_{2,0} & = & \hat{g}_{2,0} & \pmod{p_0} & (2) \\
x_{1,0} + \hat{\omega}_0 x_{2,0} & = & \log_{\hat{g}_{1,0}} \hat{c}_0 & \pmod{q_0} & (3) \\
y_{1,0} + \hat{\omega}_0 y_{2,0} & = & \log_{\hat{g}_{1,0}} \hat{d}_0 & \pmod{q_0} & (4) \\
z_{1,0} + \hat{\omega}_0 z_{2,0} & = & \log_{\hat{g}_{1,0}} \hat{h}_0 & \pmod{q_0} & (5) \\
g_{1,1} & = & \hat{g}_{1,1} & \pmod{p_1} & (6) \\
g_{2,1} & = & \hat{g}_{2,1} & \pmod{p_1} & (7) \\
x_{1,1} + \hat{\omega}_1 x_{2,1} & = & \log_{\hat{g}_{1,1}} \hat{c}_1 & \pmod{q_1} & (8) \\
y_{1,1} + \hat{\omega}_1 y_{2,1} & = & \log_{\hat{g}_{1,1}} \hat{d}_1 & \pmod{q_1} & (9) \\
z_{1,1} + \hat{\omega}_1 z_{2,1} & = & \log_{\hat{g}_{1,1}} \hat{h}_1 & \pmod{q_1} & (10) \\
F_{q_0}(u_{1,0}) + t_1 q_0 & = & \hat{u}'_{1,0} & & (11) \\
F_{q_0}(u_{2,0}) + t_2 q_0 & = & \hat{u}'_{2,0} & & (12) \\
F_{q_0}(e) + t_3 q_0 & = & \hat{e}' & & (13) \\
F_{q_0}(v) + t_4 q_0 & = & \hat{v}' & & (14) \\
r_{1,0} z_{1,0} + r_{2,0} \hat{\omega}_0 z_{2,0} & = & \log_{\hat{g}_{1,0}} \frac{e}{m_0} & \pmod{q_0} & (15) \\
r_{1,0} x_{1,0} + r_{1,0} \alpha_0 x_{2,0} + r_{2,0} \hat{\omega}_0 x_{2,0} + r_{2,0} \hat{\omega}_0 \alpha_0 y_{2,0} & = & \log_{\hat{g}_{1,0}} v & \pmod{q_0} & (16)
\end{array}$$

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_0 denote the known constants whereas the variables without hats except p_0, p_1, q_0, q_1, m_0 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 $F_{q_0} : G_{q_0} \to \mathbb{Z}_{q_0}$ 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.

$$\begin{aligned}
F_{q_1}(u_{1,1}) + t_1 q_1 &= \hat{u}'_{1,1} && (11') \\
F_{q_1}(u_{2,1}) + t_2 q_1 &= \hat{u}'_{2,1} && (12') \\
F_{q_1}(e) + t_3 q_1 &= \hat{e}' && (13') \\
F_{q_1}(v) + t_4 q_1 &= \hat{v}' && (14') \\
r_{1,1} z_{1,0} + r_{2,1}\hat{\omega}_1 z_{2,0} &= \log_{\hat{g}_{1,1}} \tfrac{e}{m_1} \pmod{q_1} && (15') \\
r_{1,1} x_{1,1} + r_{1,1}\alpha_1 x_{2,1} + r_{2,1}\hat{\omega}_1 x_{2,1} + r_{2,1}\hat{\omega}_1 \alpha_1 y_{2,1} &= \log_{\hat{g}_{1,1}} v \pmod{q_1} && (16')
\end{aligned}$$

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

E.2.3 Proof of Lemma 9

We first define the events InvA_0 and InvA_1. The event InvA_0 (respectively InvA_1) is true if during the execution of D the adversary A submits an invalid anonymized ciphertext to its decryption oracle $\mathcal{DA}_{sk_0}$ (resp. $\mathcal{DA}_{sk_1}$) for anonymized ciphertexts and does not get $\perp$. We also define the events InvS_0 and InvS_1. The event InvS_0 (respectively InvS_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. $\mathcal{D}_{sk_1}$) for standard ciphertexts and does not get $\perp$.

It is clear that

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

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

Then, we have

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

and

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

Note that $F_{q_0,4}^{-1}$ 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 $(\tilde{u}'_1, \tilde{u}'_2, \tilde{e}', \tilde{v}') \notin EC_{\mathsf{CS}}((u'_{1,b}, u'_{2,b}, e', v'), pk_0)$, $\tilde{v} \neq v$ 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

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

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

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

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

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

Let us define the following events:

- $\mathsf{InvA}_{i,0}$ 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 $\mathcal{DA}_{sk_0}$ 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 $\mathcal{DA}_{sk_0}$. 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,

$$\begin{aligned}
&\Pr[\mathsf{InvA}_{1,0}|\neg\mathsf{NR}] \\
&= \frac{1}{2}\Pr[E_0^{\mathrm{inv}}|E_0] + \frac{1}{2}\Pr[E_0^{\mathrm{inv}}|E_1] \leq \frac{\Pr[E_0^{\mathrm{inv}} \wedge E_0]}{\Pr[E_0]} + \frac{\Pr[E_0^{\mathrm{inv}} \wedge E_1]}{\Pr[E_1]} \\
&\leq \frac{|E_0^{\mathrm{inv}} \wedge E_0| \cdot |S|}{2|S||E_0|} + \frac{|E_0^{\mathrm{inv}} \wedge E_1| \cdot |S|}{2|S||E_1|} = \frac{|E_0^{\mathrm{inv}} \wedge E_0|}{2q_0 q_1^5} + \frac{|E_0^{\mathrm{inv}} \wedge E_1|}{2q_1 q_0^5}.
\end{aligned}$$

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

In the case of $|E_0^{\mathrm{inv}} \wedge E_0|$, 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 $|E_0^{\mathrm{inv}} \wedge E_0| = q_1^5$.

In the case of $|E_0^{\mathrm{inv}} \wedge E_1|$, 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 $|E_0^{\mathrm{inv}} \wedge E_1| = q_1 q_0^4$.

Therefore,

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

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

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

Therefore, we have

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

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

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

We now consider $\Pr[\mathsf{InvS}_0|\neg\mathsf{NR}]$ and $\Pr[\mathsf{InvS}_1|\neg\mathsf{NR}]$. We can define the event $\mathsf{InvS}_{i,0}$ in a similar way as that for $\mathsf{InvA}_{i,0}$. It is easy to see that if the adversary A can submit an invalid ciphertext to its decryption oracle $\mathcal{D}_{sk_i}$ for standard ciphertexts then A can submit an invalid anonymized ciphertext to its decryption oracle $\mathcal{DA}_{sk_i}$ for anonymized ciphertexts. Thus, we have

$$\Pr[\mathsf{InvS}_{1,0}|\neg\mathsf{NR} \wedge \text{Case 3}] \leq \Pr[\mathsf{InvA}_{1,0}|\neg\mathsf{NR} \wedge \text{Case 3}],$$

and

$$\Pr[\mathsf{InvS}_0|\neg\mathsf{NR}] \leq \mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},C}(k) + \frac{q'_d(k)}{2^{k-2}}.$$

Similarly, we can evaluate

$$\Pr[\mathsf{InvS}_1|\neg\mathsf{NR}] \leq \mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},C}(k) + \frac{q'_d(k)}{2^{k-2}}.$$

In conclusion, we have

$$\Pr[\mathsf{Inv}|\neg\mathsf{NR} \wedge \text{Case 3}] \leq 4\mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},C}(k) + \frac{q_d(k) + q'_d(k)}{2^{k-3}}.$$