Universally Anonymizable Public-Key Encryption

Ryotaro Hayashi and Keisuke Tanaka

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

Abstract. We first propose the notion of universally 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 anonymizability. If we use a universally anonymizable public-key encryption scheme, not only the person who made the ciphertexts, but also anyone can anonymize the encrypted data without using the corresponding secret key. We then propose universally anonymizable public-key encryption schemes based on the ElGamal encryption scheme, the Cramer-Shoup encryption scheme, and RSA-OAEP, and prove their security.

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

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.

In addition to the notion of key-privacy, they provided the RSA-based anonymous 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 [10] proposed the RSA-based anonymous encryption scheme by using the RSACD function. Hayashi and Tanaka [11] constructed

	RSA-OAEP	Sampling Twice [11]	RSA-RAEP [1]	RSACD [10]	Expanding
anonymity	No	Yes	Yes	Yes	Yes
# of mod. exp. to encrypt (average / worst)	1 / 1	2 / 2	1.5 / k_1	1.5 / 2	1 / 1
# of random bits to encrypt (average / worst)	k_0	$2k_0 + k + 3$ / $2k_0 + k + 3$	$1.5k_0$ / k_1k_0	$1.5k_0$ / $1.5k_0$	$k_0 + 160$ / $k_0 + 160$
size of ciphertexts	k	k	k	k	$k + 160$

Fig. 1. The costs of the encryption schemes.

the RSA-based anonymous encryption scheme by using the sampling twice technique. In [11], they also mentioned the scheme with the expanding technique for comparison, however, there is no security proof.

With respect to the discrete-log based schemes, Bellare, Boldyreva, Desai, and Pointcheval [1] proved that the ElGamal and the Cramer-Shoup encryption schemes provide the anonymity property when all of the users use a common group.

In this paper, we consider the following situation. In order to send e-mails, all members of the company use the encryption scheme which does not provide the anonymity property. They consider that e-mails sent to the inside of the company do not have to be anonymized and it is sufficient to be encrypted the data. However, when e-mails are sent to the outside of the company, they want to anonymize them for preventing the eavesdropper on the public network.

A trivial answer for this problem is that all members use the encryption scheme with the anonymity property. However, generally speaking, we require some computational costs to create ciphertexts with the anonymity property. In fact, the RSA-based anonymous encryption schemes proposed in [1, 10, 11], which are based on RSA-OAEP, are not efficient with respect to the encryption cost or the size of ciphertexts, compared with RSA-OAEP (See Figure 1. Here, k, k_0, k_1 are security parameters and we assume that N is uniformly distributed in $(2^{k-1}, 2^k)$.). Since the members do not require to anonymize the e-mails, it would be better to use the standard encryption scheme within the company.

We propose another way to solve this. Consider the situation that not only the person who made the ciphertexts, but also anyone can transform the encrypted data to those with the anonymity property without decrypting these encrypted data. If we have this situation, we can make an e-mail gateway which can transform encrypted e-mails to those with the anonymity property without using the corresponding secret key when they are sent to the outside of the company.

Furthermore, we can use this e-mail gateway in order to guarantee the anonymity property for e-mails sent to the outside of the company. The president of the company may consider that all e-mails sent to the outside of the company should be anonymized. In this case, even if someone tries to send e-mails to the outside of the company without anonymization, the e-mails passing through the e-mail gateway are always anonymized.

In this paper, in order to formalize this idea, we propose a special type of public-key encryption scheme called a *universally anonymizable public-key encryption scheme*. A universally anonymizable public-key encryption scheme consists of a standard public-key encryption scheme $\mathcal{PE}$ and two 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 it 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 universally 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 universally anonymizable public-key encryption schemes based on the ElGamal encryption scheme, the Cramer-Shoup encryption scheme, and RSA-OAEP, and prove their security.

We show the key-privacy property of our schemes by applying an argument in [1] with modification. 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 discrete-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. We also employ the expanding technique. With this 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.

The organization of this paper is as follows. In Section 2, we review the definitions of the Decisional Diffie-Hellman problem, the families of hash functions, and the RSA family of trap-door permutations. In Section 3, we formulate the notion of universally anonymizable public-key encryption and its security properties. We propose the universally anonymizable public-key encryption scheme based on the ElGamal encryption scheme in Section 4, that based on the Cramer-Shoup encryption scheme in Section 5, and that based on RSA-OAEP in Section 6.

2 Preliminaries

2.1 The Decisional Diffie-Hellman Problem

In this section, we review the decisional Diffie-Hellman Problem.

Definition 1 (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:*

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

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

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

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 any algorithm D whose time-complexity is polynomial in k.

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

2.2 Families of Hash Functions

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

Definition 2 (Families of Hash Functions). *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 3 (Universal One-Wayness). *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:*

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

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

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

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

2.3 The RSA Family of Trap-Door Permutations

In this section, we describe the definitions of the RSA family of trap-door permutations denoted by RSA and θ-partial one-wayness of RSA.

Definition 4 (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* $I_{N,d,k}(y) = y^d \bmod N$.

Definition 5 (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 experiment:*

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

Here, " $||$ *" denotes concatenation. We define the advantage 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, $x \xleftarrow{R} \mathbb{Z}^*_N$, *and* A. *We say that* RSA *is* θ*-partial one-way if the function* $\mathbf{Adv}^{\theta\text{-pow-fnc}}_{\mathsf{RSA},A}(k)$ *is negligible for any adversary* A *whose time complexity is polynomial in* k.

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 $\theta > 0.5$.

3 Universally Anonymizable Public-Key Encryption

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

3.1 The Definition of Universally Anonymizable Public-Key Encryption Schemes

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

Definition 6. *A universally 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 *and returns 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 *and returns 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.*

We require the standard correctness condition. That is, for any (pk, sk) *outputted by* $\mathcal{K}$ *and* $m \in \mathcal{M}(pk)$ *where* $\mathcal{M}(pk)$ *denotes the message space of* pk*, we have* $m = \mathcal{D}_{sk}(\mathcal{E}_{pk}(m))$ *and* $m = \mathcal{DA}_{sk}(\mathcal{UA}_{pk}(\mathcal{E}_{pk}(m)))$*.*

In the universally 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 it 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 Universally Anonymizable Public-Key Encryption Schemes

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

Data-Privacy We define the security property called *data-privacy* of universally 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. We first describe the definition of the data-privacy on standard ciphertexts.

Definition 7 (Data-Privacy on Standard Ciphertexts). *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, m_0, m_1, *and so on. For* $\mathrm{atk} \in \{\mathrm{cpa}, \mathrm{cca}\}$, *we consider the following experiment:*

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

Note that $m_0, m_1 \in \mathcal{M}(pk)$. *Above it is mandated that* A^2_{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_{cca} *never queries either the anonymized ciphertext* $\tilde{c} \in \{\mathcal{UA}_{pk_0}(c)\}$ *to* $\mathcal{DA}_{sk_0}(\cdot)$ *or* $\tilde{c} \in \{\mathcal{UA}_{pk_1}(c)\}$ *to* $\mathcal{DA}_{sk_1}(\cdot)$. *For* $\mathrm{atk} \in \{\mathrm{cpa}, \mathrm{cca}\}$, *we define the advantage via*

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

We say that the universally 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* $\mathbf{Adv}^{\text{dataS-cpa}}_{\mathcal{UAPE},A_{\mathrm{cpa}}}(k)$ *(resp.* $\mathbf{Adv}^{\text{dataS-cca}}_{\mathcal{UAPE},A_{\mathrm{cca}}}(k)$*) is negligible for any adversary* A *whose time complexity is polynomial in* k.

In the above experiment, if the challenge is c, then anyone can compute $\mathcal{UA}_{pk_0}(c)$. Therefore, in the CCA setting, we restrict the oracle access to $\mathcal{DA}$ as described above.

We next describe the definition of the data-privacy on anonymized ciphertexts.

Definition 8 (Data-Privacy on Anonymized Ciphertexts). *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* $\mathcal{DA}_{sk_1}(\cdot)$. *For* $\mathrm{atk} \in \{\mathrm{cpa}, \mathrm{cca}\}$, *we consider the following experiment:*

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

Note that $m_0, m_1 \in \mathcal{M}(pk)$. *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* $\mathrm{atk} \in \{\mathrm{cpa}, \mathrm{cca}\}$, *we define the advantage via*

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

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

Remark 1. In the CPA setting, if there exists an algorithm which breaks the data-privacy on anonymized ciphertexts, then we can break that on standard ciphertexts by applying the anonymizing algorithm to the standard ciphertexts and passing the resulting anonymized ciphertexts to the adversary which breaks the data-privacy on anonymized ciphertexts. Therefore, in the CPA setting, it is sufficient that the universally anonymizable public-key encryption scheme provides the data-privacy of standard ciphertexts.

On the other hand, in the CCA setting, the data privacy on standard ciphertexts does not always imply that on anonymized ciphertexts, since the oracle access of the adversary attacking the data privacy on standard ciphertexts is restricted more strictly than that on anonymized ciphertexts.

Key-Privacy We define the security property called *key-privacy* of universally anonymizable public-key encryption schemes. If the scheme provides the key-privacy, the adversary cannot know under which key the anonymized ciphertext was created.

Definition 9 (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* $\mathcal{DA}_{sk_1}(\cdot)$. *For* atk $\in$ {cpa, cca}, *we consider the following experiment:*

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

Note that $m_0 \in \mathcal{M}(pk_0)$ *and* $m_1 \in \mathcal{M}(pk_1)$. *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* atk $\in$ {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 the universally anonymizable public-key encryption scheme $\mathcal{UAPE}$ *provides the key-privacy against the chosen plaintext attack (resp. the adaptive chosen ciphertext attack) if* $\mathbf{Adv}^{\text{key-cpa}}_{\mathcal{UAPE},A_{\mathrm{cpa}}}(k)$ *(resp.* $\mathbf{Adv}^{\text{key-cca}}_{\mathcal{UAPE},A_{\mathrm{cca}}}(k)$*) is negligible for any adversary* A *whose time complexity is polynomial in* k.

Bellare, Boldyreva, Desai, and Pointcheval [1] proposed a security requirement of 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 universally 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 and the message spaces for users may be different even if the security parameter is fixed. In fact, in Sections 4 and 5, 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.

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

4 ElGamal and its Universal Anonymizability

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

4.1 The ElGamal Encryption Scheme

Definition 10 (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 a 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*.*

$\mathtt{Algorithm}\ \mathcal{K}^{\mathsf{EG}}(k)$	$\mathtt{Algorithm}\ \mathcal{E}^{\mathsf{EG}}_{pk}(m)$	$\mathtt{Algorithm}\ \mathcal{D}^{\mathsf{EG}}_{sk}(c_1, c_2)$
$(q, g) \leftarrow \mathcal{Q}(k)$	$r \xleftarrow{R} \mathbb{Z}_q$	$m \leftarrow c_2 \cdot c_1^{-x}$
$x \xleftarrow{R} \mathbb{Z}_q;\ y \leftarrow g^x$	$c_1 \leftarrow g^r$	$\mathtt{return}\ m$
$\mathtt{return}\ pk = (q, g, y)\ \mathtt{and}\ sk = x$	$c_2 \leftarrow m \cdot y^r$	
	$\mathtt{return}\ (c_1, c_2)$	

The ElGamal encryption scheme is secure in the sense of IND-CPA if the DDH problem for $\mathcal{Q}$ is hard.

4.2 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 anonymizing algorithm.

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

We describe the encoding function and the expanding technique.

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 $QR_p \subset \mathbb{Z}_p^*$ 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 $\bar{F}_{q,t}^{-1}$.

The Expanding Technique 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.

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

Then, for any q where $|q| = k$, if $\bar{c}$ is uniformly chosen from $\mathbb{Z}_q$, then the statistical distance between the distribution of the output c' by the expanding technique and the uniform distribution over $\{0,1\}^{k+k_b}$ is less than $1/2^{k_b-1}$. In the following, we set $k_b = 160$.

Our Scheme We now propose our universally 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 11. *Our universally 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.*

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

4.3 Security

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

We can easily see that our scheme provides the data-privacy on standard ciphertexts against the chosen plaintext attack if the DDH problem for $\mathcal{Q}$ is hard. More precisely, we can prove that if there exists a CPA-adversary attacking the data-privacy on standard ciphertexts of our scheme with advantage ϵ, then there exists a CPA-adversary attacking the indistinguishability of the ElGamal encryption scheme with the same advantage ϵ.

Note that this implies our scheme provides the data-privacy on anonymized ciphertexts against the chosen plaintext attack if the DDH problem for $\mathcal{Q}$ is hard.

We now prove our scheme provides the key-privacy against the chosen plaintext attack. To prove this, we use the idea of Halevi [9].

Lemma 1 (Halevi [9]). *Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a (standard) encryption scheme that is CCA secure (resp. CPA secure) for the indistinguishability (data-privacy). Then a sufficient condition for $\mathcal{PE}$ to be also CCA secure (resp. CPA secure) for*

the key-privacy (defined by Bellare, Boldyreva, Desai, and Pointcheval) if the statistical distance between the two distributions

$$D_0 = \{(pk_0, pk_1, \mathcal{E}_{pk_0}(m)) : (pk_0, sk_0), (pk_1, sk_1) \leftarrow \mathcal{K}(k);\ m \xleftarrow{R} \mathcal{M}(pk_0)\}$$
$$D_1 = \{(pk_0, pk_1, \mathcal{E}_{pk_1}(m)) : (pk_0, sk_0), (pk_1, sk_1) \leftarrow \mathcal{K}(k);\ m \xleftarrow{R} \mathcal{M}(pk_1)\}$$

is negligible.

This lemma shows the relation between the indistinguishability and the key-privacy for *standard* encryption scheme. We can apply this lemma to our universally anonymizable encryption scheme. That is, if the universally anonymizable encryption scheme $\mathcal{UAPE} = ((\mathcal{K}, \mathcal{E}, \mathcal{D}), \mathcal{UA}, \mathcal{DA})$ provides the data-privacy on *anonymized* ciphertexts against CCA (resp. CPA) and the statistical distance between the two distributions

$$D'_0 = \{(pk_0, pk_1, \mathcal{UA}_{pk_0}(\mathcal{E}_{pk_0}(m))) : (pk_0, sk_0), (pk_1, sk_1) \leftarrow \mathcal{K}(k);\ m \xleftarrow{R} \mathcal{M}(pk_0)\}$$
$$D'_1 = \{(pk_0, pk_1, \mathcal{UA}_{pk_1}(\mathcal{E}_{pk_1}(m))) : (pk_0, sk_0), (pk_1, sk_1) \leftarrow \mathcal{K}(k);\ m \xleftarrow{R} \mathcal{M}(pk_1)\}$$

is negligible, then $\mathcal{UAPE}$ provides the key-privacy against CCA (resp. CPA).

By using this, in order to prove that our scheme provides the key-privacy against the chosen plaintext attack, all we have to do is to see that the two distributions D'_0 and D'_1 derived by our scheme satisfy the property defined above. It is easy to see that the statistical distance between D'_0 and D'_1 is less than $2 \times (1/2^{159})^2$.

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

5 Cramer-Shoup and its Universal Anonymizability

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

5.1 The Cramer-Shoup Encryption Scheme

Definition 12 (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. Let* $\mathcal{H} = (\mathcal{GH}, \mathcal{EH})$ *be a family of hash functions. Note that* $\mathcal{Q}$ *is a QR-group generator with a safe prime.*

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

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

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

Cramer and Shoup [5] proved that the Cramer-Shoup encryption scheme is secure in the sense of IND-CCA2 assuming that $\mathcal{H}$ is universal one-way and the DDH problem for $\mathcal{Q}$ 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.

5.2 Universal Anonymizability of the Cramer-Shoup Encryption Scheme

We propose our universally 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 encoding function and the expanding technique appeared in Section 4.

Definition 13. *Our universally 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.*

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

5.3 Security

In this section, we prove that our universally anonymizable Cramer-Shoup encryption scheme $\mathcal{UAPE}^{\mathsf{EG}}$ is CCA-secure assuming that the DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is universal one-way.

We can prove that our scheme provides the data-privacy on standard ciphertexts against the adaptive chosen ciphertext attack if the DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is universal one-way. More precisely, we can prove that if there exists a CCA-adversary A attacking the data-privacy on standard ciphertexts of our scheme with advantage ϵ, then there exists a CCA2-adversary B attacking the indistinguishability of the Cramer-Shoup encryption scheme with the same 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 $\boldsymbol{c}' = (u'_1, u'_2, e', v')$ to

$\mathcal{DA}_{sk_0}(\cdot)$, we simply compute $\boldsymbol{c} = (u'_1 \bmod q_0, u'_2 \bmod q_0, e' \bmod q_0, v' \bmod q_0)$ and decrypt $\boldsymbol{c}$ 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.

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

We define the set of ciphertexts $EC_{\mathsf{CS}}((u'_1, u'_2, e', v'), pk)$ called "equivalence class" as

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

If $\boldsymbol{c}' = (u'_1, u'_2, e', v') \in (\{0,1\}^{k+160})^4$ is an anonymized ciphertext of m under $pk = (q, g_1, g_2, c, d, h, K)$ then any element $\check{\boldsymbol{c}} = (\check{u}_1, \check{u}_2, \check{e}, \check{v}) \in EC_{\mathsf{CS}}(\boldsymbol{c}', pk)$ is also an anonymized ciphertext of m under pk. Therefore, when $\boldsymbol{c}'$ is a challenge anonymized ciphertext, the adversary can ask an anonymized ciphertext $\check{\boldsymbol{c}} \in EC_{\mathsf{CS}}(\boldsymbol{c}', pk_0)$ to the decryption oracle $\mathcal{DA}^{\mathsf{CS}}_{sk_0}$ for anonymized ciphertexts, and if the answer of $\mathcal{DA}^{\mathsf{CS}}_{sk_0}$ is m_0 then the adversary knows that $\boldsymbol{c}'$ is encrypted by pk_0 and the plaintext of $\boldsymbol{c}'$ is m_0.

Furthermore, the adversary can ask $(u'_1 \bmod q_0, u'_2 \bmod q_0, e' \bmod q_0, v' \bmod q_0)$ to the decryption oracle $\mathcal{D}^{\mathsf{CS}}_{sk_0}$ for standard ciphertexts. If the answer of $\mathcal{D}^{\mathsf{CS}}_{sk_0}$ is m_0, then the adversary knows that $\boldsymbol{c}'$ is encrypted by pk_0 and the plaintext of $\boldsymbol{c}'$ is m_0.

To prevent these attacks, 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 $\check{\boldsymbol{c}} \in EC_{\mathsf{CS}}(\boldsymbol{c}', pk_0)$ to $\mathcal{DA}^{\mathsf{CS}}_{sk_0}$ or $\check{\boldsymbol{c}} \in EC_{\mathsf{CS}}(\boldsymbol{c}', pk_1)$ to $\mathcal{DA}^{\mathsf{CS}}_{sk_1}$. It is also mandated that the adversary never queries either $(u'_1 \bmod q_0, u'_2 \bmod q_0, e' \bmod q_0, v' \bmod q_0)$ to $\mathcal{D}^{\mathsf{CS}}_{sk_0}$ or $(u'_1 \bmod q_1, u'_2 \bmod q_1, e' \bmod q_1, v' \bmod q_1)$ to $\mathcal{D}^{\mathsf{CS}}_{sk_1}$.

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 [11], Hayashi and Tanaka also employed the same restriction in order to prove the anonymity of their encryption scheme. Incidentally, Canetti, Krawczyk, and Nielsen [4] proposed a relaxed notion of CCA security, called Replayable CCA (RCCA). In their security model, the schemes which require restriction such as equivalence class for proving their CCA security satisfy a variant of RCCA, pd-RCCA (publicly-detectable replayable-CCA) secure.

If we add these restrictions then we can prove that our scheme provides the data-privacy 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. More precisely, we can prove that if there exists a CCA-adversary attacking the data-privacy on anonymized ciphertexts of our scheme with advantage ϵ, then there exists a CCA-adversary attacking the data-privacy on standard ciphertexts of our scheme with the same advantage ϵ.

We now prove our scheme provides the key-privacy against the adaptive chosen ciphertext attack. If we add the restrictions described above, we can

prove this in a similar way as that for our universally anonymizable ElGamal encryption scheme. Note that the statistical distance between D'_0 and D'_1 (See Section 4.3.) is less than $2 \times (1/2^{159})^4$.

In conclusion, our universally anonymizable Cramer-Shoup encryption scheme is CCA-secure assuming that the DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is universal one-way.

6 RSA-OAEP and its Universal Anonymizability

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

6.1 RSA-OAEP

Definition 14 (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* RSA *to get* N, e, d. *It outputs the public key* $pk = (N, e)$ *and the secret key* $sk = d$. *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* $[x]^{\ell}$ *denotes the* ℓ *most significant bits of* x, *and* $[x]_{\ell'}$ *denotes the* ℓ' *least significant bits of* x.

$\mathtt{Algorithm}\ \mathcal{E}^{\mathsf{RO}}_{pk}(m)$	$\mathtt{Algorithm}\ \mathcal{D}^{\mathsf{RO}}_{sk}(c)$
$r \xleftarrow{R} \{0,1\}^{k_0}$	$s \leftarrow [c^d \bmod N]^{n+k_1};\ t \leftarrow [c^d \bmod N]_{k_0}$
$s \leftarrow (m \Vert 0^{k_1}) \oplus G(r)$	$r \leftarrow t \oplus H(s)$
$t \leftarrow r \oplus H(s)$	$m \leftarrow [s \oplus G(r)]^n;\ p \leftarrow [s \oplus G(r)]_{k_1}$
$c \leftarrow (s \Vert t)^e \bmod N$	$\mathtt{if}\ (p = 0^{k_1})\ z \leftarrow m\ \mathtt{else}\ z \leftarrow \perp$
$\mathtt{return}\ c$	$\mathtt{return}\ z$

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

6.2 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.

To anonymize ciphertexts of RSA-OAEP, we do not have to employ the encoding function and we only use the expanding technique.

Definition 15. *Our universally 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.*

$\mathtt{Algorithm}\ \mathcal{UA}^{\mathsf{RO}}_{pk}(c)$	$\mathtt{Algorithm}\ \mathcal{DA}^{\mathsf{RO}}_{sk}(c')$
$\alpha \xleftarrow{R} \{0, 1, 2, \cdots, \lfloor (2^{k+160} - c)/N \rfloor\}$	$c \leftarrow c' \bmod N$
$c' \leftarrow c + \alpha N$	$z \leftarrow \mathcal{D}^{\mathsf{RO}}_{sk}(c)$
$\mathtt{return}\ c'$	$\mathtt{return}\ z$

6.3 Security

In this section, we prove that our universally anonymizable RSA-OAEP scheme $\mathcal{UAPE}^{\mathsf{RO}}$ is CCA-secure in the random oracle model assuming RSA is one-way.

We can prove that our scheme provides the data-privacy on standard ciphertexts against the adaptive chosen ciphertext attack in the random oracle model assuming RSA is θ-partial one-way for $\theta > 0.5$. More precisely, if RSA-OAEP is secure in the sense of IND-CCA2 then our scheme provides the data-privacy on standard ciphertexts against the adaptive chosen ciphertext attack. The proof is similar to that for our universally anonymizable Cramer-Shoup encryption scheme.

In order to prove that our scheme provides the key-privacy and the data-privacy on anonymized ciphertexts against the adaptive chosen ciphertext attack, we need the restrictions similar to those for our universally anonymizable Cramer-Shoup encryption scheme. We define the equivalence class for our universally anonymizable RSA-OAEP scheme as

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

where $pk = (N, e)$ and 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 $\mathcal{D}^{\mathsf{RO}}_{sk_1}$.

If we add these restrictions then 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 RSA is θ-partial one-way for $\theta > 0.5$ in a similar way as that for our universally anonymizable Cramer-Shoup encryption scheme.

Furthermore, if we add the restrictions described above, then we can prove that our scheme provides the key-privacy against the adaptive chosen ciphertext attack in the random oracle model assuming RSA is θ-partial one-way for $\theta > 0.5$. More precisely, we show the following theorem [1].

Theorem 1. *For any adversary A attacking the key-privacy of our scheme under the adaptive chosen ciphertext attack, and making at most* q_{dec} *queries to decryption oracle for standard ciphertexts,* q'_{dec} *queries to decryption oracle for*

[1] Halevi [9] noted that we cannot apply Lemma 1 directly to the schemes analyzed in the random oracle model.

anonymized ciphertexts, q_{gen} G-oracle queries, and q_{hash} H-oracle queries, there exists a θ-partial inverting adversary B for RSA*, such that for any k, k_0, k_1, and $\theta = \frac{k-k_0}{k}$,*

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

where $\epsilon_1 = \frac{2}{2^{k/2-3}-1} + \frac{1}{2^{159}}$, $\epsilon_2 = \frac{2q_{\mathrm{gen}}+q_{\mathrm{dec}}+q'_{\mathrm{dec}}+2q_{\mathrm{gen}}(q_{\mathrm{dec}}+q'_{\mathrm{dec}})}{2^{k_0}} + \frac{2(q_{\mathrm{dec}}+q'_{\mathrm{dec}})}{2^{k_1}} + \frac{2q_{\mathrm{hash}}}{2^{k-k_0}}$, *and the running time of B is that of A plus $q_{\mathrm{gen}} \cdot q_{\mathrm{hash}} \cdot O(k^3)$.*

In conclusion, since RSA is θ-partial one-way if and only if RSA is one-way for $\theta > 0.5$, our universally anonymizable RSA-OAEP scheme is CCA-secure in the random oracle model assuming RSA is one-way.

6.4 Proof of Theorem 1

The proof is similar to that for RSA-RAEP. We construct the partial inverting algorithm M for the RSA function using a CCA-adversary A attacking the key-privacy of our encryption scheme. We describe the partial inverting algorithm M for RSA using a CCA-adversary A attacking the 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 $\mu \xleftarrow{R} \{0, 1, 2, \ldots, \lfloor (2^{k+160} - y)/N \rfloor\}$ and sets $Y \leftarrow y + \mu N$.
2) M runs the key generation algorithm of RSA with security parameter k to obtain $pk' = (N', e', k)$ and $sk' = (N', d', k)$. Then it picks a bit $b \xleftarrow{R} \{0, 1\}$, and 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 four 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 A's oracles G, H, $\mathcal{D}_{sk_0}$, and $\mathcal{D}_{sk_1}$ 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).

In order to analyze the advantage of M, we define some events. For $i \in \{0,1\}$, let $w_i = y^{d_i} \bmod N_i$, $s_i = [w_i]^{n+k_1}$, and $t_i = [w_i]_{k_0}$.

– 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.
– 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.
– $\mathsf{DBad} = \mathsf{DSBad} \vee \mathsf{DABad}$.
– YBad denotes the event that $y \notin (\mathbb{Z}_{N_0}^* \cap \mathbb{Z}_{N_1}^*)$.
– 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.

We let $\Pr[\cdot]$ denote the probability distribution in the game defining advantage and $\Pr_1[\cdot]$ 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 the 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 $\epsilon = \mathbf{Adv}^{\text{key-cca}}_{\mathcal{UAPE}^{\mathsf{RO}},A}(k)$. The proof of the following lemma is similar to that for RSA-RAEP.

Lemma 2.

$$\Pr_1[\mathsf{AskR} \wedge \mathsf{AskS} | \neg\mathsf{DBad}] \geq \frac{\epsilon}{2} \cdot \left(1 - 2q_{\text{gen}} \cdot 2^{-k_0} - 2q_{\text{hash}} \cdot 2^{-n-k_1}\right) - 2q_{\text{gen}} \cdot 2^{-k}.$$

We next bound $\Pr_1[\neg\mathsf{DBad} | \neg\mathsf{AskS}]$. It is easy to see that $\Pr_1[\neg\mathsf{DBad} | \neg\mathsf{AskS}] \leq \Pr_1[\neg\mathsf{DSBad} | \neg\mathsf{AskS}] + \Pr_1[\neg\mathsf{DABad} | \neg\mathsf{AskS}]$, and the proof of the following lemma is similar to that for RSA-RAEP.

Lemma 3.

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

By applying Lemmas 2 and 3, we can bound $\Pr_1[\mathsf{AskS}]$ as

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

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

Lemma 4.

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

Proof (Lemma 4). Let $N = pq$ and $N' = p'q'$. We define a set $S[N]$ as $\{\tilde{Y} | \tilde{Y} \in [0, 2^{k+160}) \wedge (\tilde{Y} \bmod N) \in \mathbb{Z}_N^*\}$. Then, we have

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

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

Since $2^{160} \cdot \phi(N) \le |S[N]| \le 2^{k+160}$, we have

$$\Pr[Y' \xleftarrow{R} S[N] :\ Y' \notin S[N']] \le \tfrac{2^{k+160} - |S[N']|}{|S[N]|} \le \tfrac{2^{k+160} - |S[N']|}{2^{160} \cdot \phi(N)}.$$

Furthermore, we have

$$\begin{aligned}
2^{k+160} - |S[N']| &= \left|\{Y' | Y' \in [0, 2^{k+160}) \wedge (Y' \bmod N') \notin \mathbb{Z}_{N'}^*\}\right| \\
&\le \left|\{Y' | Y' \in [0, 2N' \cdot 2^{160}) \wedge (Y' \bmod N') \notin \mathbb{Z}_{N'}^*\}\right| \\
&= 2^{161} \times |\{Y' | Y' \in [0, N') \wedge Y' \notin \mathbb{Z}_{N'}^*\}| \\
&= 2^{161}(N' - \phi(N')).
\end{aligned}$$

Noticing 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 have

$$\begin{aligned}
&\Pr[Y' \xleftarrow{R} S[N] :\ Y' \notin S[N']] \\
&\quad \le \tfrac{2^{161}(N' - \phi(N'))}{2^{160} \cdot \phi(N)} \le \tfrac{2(p' + q')}{N - p - q} \le \tfrac{2(2^{\lceil k/2 \rceil} + 2^{\lceil k/2 \rceil})}{2^{k-1} - 2^{\lceil k/2 \rceil} - 2^{\lceil k/2 \rceil}} \le \tfrac{2}{2^{k/2-3} - 1}.
\end{aligned}$$

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

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

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 $q_{\mathrm{gen}} \cdot q_{\mathrm{hash}} \cdot O(k^3)$.

References

1. M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval. Key-Privacy in Public-Key Encryption. In Boyd [3], pages 566–582. Full version of this paper, available via `http://www-cse.ucsd.edu/users/mihir/`.
2. M. Bellare and P. Rogaway. Optimal Asymmetric Encryption – How to Encrypt with RSA. In A. De Santis, editor, *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *LNCS*, pages 92–111, 1994. Springer-Verlag.
3. C. Boyd, editor. *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *LNCS*, 2001. Springer-Verlag.
4. R. Canetti, H. Krawczyk, and J. B. Nielsen. Relaxing Chosen-Ciphertext Security. In D. Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *LNCS*, pages 565–582, 2003. Springer-Verlag.
5. R. Cramer and V. Shoup. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack. In H. Krawczyk, editor, *Advances in Cryptology – CRYPTO '98*, volume 1462 of *LNCS*, pages 13–25, 1998. Springer-Verlag.
6. Y. Desmedt. Securing traceability of ciphertexts: Towards a secure software escrow scheme. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology – EUROCRYPT '95*, volume 921 of *LNCS*, pages 147–157, 1995. Springer-Verlag.
7. E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP is Secure under the RSA Assumption. In J. Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *LNCS*, pages 260–274, 2001. Springer-Verlag.
8. S. D. Galbraith and W. Mao. Invisibility and Anonymity of Undeniable and Confirmer Signatures. In M. Joye, editor, *Topics in Cryptology – CT-RSA 2003*, volume 2612 of *LNCS*, pages 80–97, 2003. Springer-Verlag.
9. S. Halevi. A Sufficient Condition for Key-Privacy. IACR Cryptology ePrint Archive, `http://eprint.iacr.org/2005/005.pdf`, 2005.
10. R. Hayashi, T. Okamoto, and K. Tanaka. An RSA Family of Trap-door Permutations with a Common Domain and its Applications. In F. Bao, R. H. Deng, and J. Zhou, editors, *Public Key Cryptography – PKC 2004*, volume 2947 of *LNCS*, pages 291–304, 2004. Springer-Verlag.
11. R. Hayashi and K. Tanaka. The Sampling Twice Technique for the RSA-based Cryptosystems with Anonymity. In S. Vaudenay, editor, *Public Key Cryptography – PKC 2005*, volume 3386 of *LNCS*, pages 216–233, 2005. Springer-Verlag.
12. S. Lucks. A Variant of the Cramer-Shoup Cryptosystem for Groups of Unknown Order. In Y. Zheng, editor, *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 27–45, 2002. Springer-Verlag.
13. R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In Boyd [3], pages 552–565.