ISSN 1342-2812

Research Reports on Mathematical and Computing Sciences

PA in the Two-Key Setting and
a Generic Conversion for Encryption with Anonymity

Ryotaro Hayashi and Keisuke Tanaka

April 2006, C–224

Department of
Mathematical and
Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

PA in the Two-Key Setting and a Generic Conversion for Encryption with Anonymity

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. Bellare, Boldyreva, Desai, and Pointcheval [2] proposed a new security requirement of encryption schemes called "key-privacy" or "anonymity." It asks that an encryption scheme provides 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. They formalized the property of anonymity, and this can be considered under either the chosen plaintext attack or the adaptive chosen ciphertext attack, yielding two notions of security, IK-CPA and IK-CCA. (IK means "indistinguishability of keys.")
In this paper, we propose the notion of plaintext awareness in the two-key setting, called PATK. We say that a public-key encryption scheme Π is secure in the sense of PATK if Π is secure in the sense of IK-CPA and there exists a knowledge extractor for PATK. There are some differences between the definition of knowledge extractor for PA in [3] and that for PATK. We also prove that if a public-key encryption scheme is secure in the sense of PATK, then it is also secure in the sense of IK-CCA. Since it looks much easier to prove that a public-key encryption scheme is secure in the sense of PATK than to prove directly that it is secure in the sense of IK-CCA, the notion of PATK is useful to prove the anonymity property of public-key encryption schemes.
We also propose the first generic conversion for the anonymity, that is, we prove that the public-key encryption scheme derived from the Fujisaki-Okamoto conversion scheme, where the basic public-key encryption scheme is secure in the sense of IK-CPA, is secure in the sense of IK-CCA in the random oracle model.

Keywords: anonymity, key-privacy, encryption, plaintext awareness in the two-key setting

1 Introduction

1.1 Background

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

The widely admitted appropriate security level for public-key encryption is the indistinguishability against the adaptive chosen ciphertext attack (IND-CCA). A promising way to construct such a public-key encryption scheme is to convert it from primitives which are secure in a weaker sense such as one-wayness (OW), IND-CPA, etc.

Bellare and Rogaway [5] proposed a generic and simple conversion scheme from a one-way trapdoor permutation into a public-key encryption scheme. The scheme created in this way is called OAEP. Fujisaki, Okamoto, Pointcheval, and Stern [16] proved that OAEP with a partial one-way trapdoor permutation is secure in the sense of IND-CCA. The OAEP conversion has several variants, such as SAEP [6], OAEP+ [26], etc.

Fujisaki and Okamoto [15] proposed a simple conversion scheme from weak public-key and symmetric-key encryption schemes into a public-key encryption scheme which is secure in the sense of IND-CCA. This scheme was used to construct the identity-based encryption scheme proposed by Boneh and Franklin [7]. Pointcheval [24] proposed a similar conversion scheme.

Recently, many conversion schemes which depend on gap problems [22], such as, REACT [21], GEM [9], and the schemes in [10], are proposed.

The public-key encryption schemes derived from the conversion schemes [5, 16, 6, 26, 15, 24, 21, 9, 10] described above meet not only IND-CCA, but also the notion of plaintext awareness (PA). The notion of PA is first proposed by Bellare and Rogaway [5] and refined by Bellare, Desai, Pointcheval, and Rogaway [3] which is, roughly speaking, that nobody can produce a *new* ciphertext without knowing the plaintext. We say that a public-key encryption scheme is secure in the sense of PA if it is secure in the sense of IND-CPA and there exists a knowledge extractor which is a formalization of the above property. In [3], they proved that PA implies IND-CCA. Since it looks much easier to prove that a public-key encryption scheme is secure in the sense of PA than to prove directly it is secure in the sense of IND-CCA, the notion of PA is useful to prove the security of public-key encryption schemes.

Recently, Bellare and Palacio [4] discussed the problem of defining the notion of plaintext-awareness without random oracles and of achieving its concrete schemes.

On the other hand, the notion of PA might be too strong. The schemes described above get a redundant construction. In [23, 11], the conversion schemes without redundancy were proposed. They are secure in the sense of IND-CCA, but does not meet PA. Fujisaki [14] introduced another security notion, called plaintext simulatability (PS). It implies IND-CCA, similar to PA, however, it is a properly weaker notion than PA.

In 2001, Bellare, Boldyreva, Desai, and Pointcheval [2] 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. They formalized the property of anonymity. This can be considered under either the chosen plaintext attack or the adaptive chosen ciphertext attack, yielding two notions of security, IK-CPA and IK-CCA. (IK means "indistinguishability of keys.")

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 [5], Fujisaki, Okamoto, Pointcheval, and Stern [16]). Recently, Hayashi, Okamoto, and Tanaka [17] proposed the RSA-based anonymous encryption scheme by using the RSACD function. Hayashi and Tanaka [18] constructed the RSA-based anonymous encryption scheme by using the sampling twice technique.

1.2 Our Contribution

In this paper, we propose the notion of plaintext awareness in the two-key setting, called PATK. We say that the public-key encryption scheme Π is secure in the sense of PATK if Π is secure in the sense of IK-CPA and there exists a knowledge extractor for PATK. There are some differences between the definition of a knowledge extractor for PA in [3] and that for PATK (See Section 4). We can see that if there exists a knowledge extractor K for PATK of Π, then we can use K as a knowledge extractor for PA of Π. That is, if the public-key encryption scheme Π is secure in the sense of PATK and IND-CPA, then Π is secure in the sense of PA. However, it is not clear that we can use the knowledge extractor for PA of Π as that for PATK of Π.

We also prove that if a public-key encryption scheme is secure in the sense of PATK, then it is also secure in the sense of IK-CCA. Since it looks much easier to prove that a public-key encryption scheme is secure in the sense of PATK than to prove directly that it is secure in the sense of IK-CCA, the notion of PATK is useful to prove the anonymity property of public-key encryption schemes.

We also propose the first generic conversion scheme for the anonymity from IK-CPA to IK-CCA. We employ the Fujisaki-Okamoto conversion scheme [15]. The public-key encryption scheme derived from their conversion scheme is secure in the sense of IND-CCA in the random oracle

model when it consists of a public-key encryption scheme Π^{pub} and a symmetric-key encryption scheme Π^{sym} where

- Π^{pub} is γ-uniform ($\gamma < 1$) and secure in the sense of OW, and
- Π^{sym} is secure in the sense of find-guess (FG).

We prove that the scheme derived from the Fujisaki-Okamoto conversion scheme with the above two and the following two assumptions is secure in the sense of IK-CCA in the random oracle model.

- In Π^{pub}, the message space and the randomness space are common to each user (each public-key).
- Π^{pub} is secure in the sense of IK-CPA.

We can get the public-key encryption scheme which is secure in the sense of IND-CCA and IK-CCA if we assume the above four conditions.

The organization of this paper is as follows. In Section 2, we review the definitions of public-key encryption and symmetric-key encryption. In Section 3 we review the security definitions for public-key encryption and symmetric-key encryption. In Section 4, we propose the notion of plaintext awareness in the two-key setting (PATK), and prove that PATK implies IK-CCA. In Section 5, we review the conversion scheme to IND-CCA proposed by Fujisaki and Okamoto [15]. In Section 6, we propose a generic conversion scheme for the anonymity. More precisely, we prove that the public-key encryption scheme derived from the Fujisaki-Okamoto conversion scheme, where the basic public-key encryption scheme is secure in the sense of IK-CPA, is secure in the sense of IK-CCA in the random oracle model. We conclude in Section 7.

2 Preliminaries

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

2.1 Public-Key Encryption

In this section, we review the definition of public-key encryption schemes.

In this paper, we mainly consider the anonymity property of encryption schemes proposed in [2]. It asks that the encryption provide (in addition to privacy of the data being encrypted) privacy of the key under which the encryption was performed. In a heterogeneous public-key environment, encryption will probably fail to be anonymous for trivial reasons. For example, different users might be using different cryptosystems, or, if the same cryptosystem, have keys of different lengths. To avoid this problem, we employ some common parameter called *common key* in the definition of encryption schemes, similar to that in [2]. Then, the public key pk includes the corresponding common key I and other information for each user.

Definition 1. *A public-key encryption scheme with common-key generation $\Pi = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of four algorithms.*

- *The common-key generation algorithm $\mathcal{G}(1^k)$ takes as input a security parameter 1^k and returns some common key I.*
- *The key generation algorithm $\mathcal{K}(I)$ is a randomized algorithm that takes as input a common key I and returns a pair (pk, sk) of keys, a public key and a matching secret key. For given pk, the message space $\mathtt{MSPC}(pk)$ and the randomness space $\mathtt{COINS}(pk)$ of Π are uniquely determined.*

– *The encryption algorithm* $\mathcal{E}_{pk}(m;r)$ *is a randomized algorithm that takes a public key* pk *and a plaintext* $m \in \mathtt{MSPC}(pk)$*, and returns a ciphertext* c*, using random coin* $r \in \mathtt{COINS}(pk)$*.*
– *The decryption algorithm* $\mathcal{D}_{sk}(c)$ *is a deterministic algorithm that takes a secret key* sk *and a ciphertext* c*, and returns the corresponding plaintext* m *or a special symbol* $\perp$ *to indicate that the ciphertext* c *is invalid.*

We require that, for any $k \in \mathbb{N}$*, if* $I \leftarrow \mathcal{G}(1^k)$*,* $(pk, sk) \leftarrow \mathcal{K}(I)$*,* $m \in \mathtt{MSPC}(pk)$*, and* $c \leftarrow \mathcal{E}_{pk}(m)$*, then* $m = \mathcal{D}_{sk}(c)$*.*

2.2 Symmetric-Key Encryption

In this section, we review the definition of symmetric-key encryption schemes.

Definition 2. *A symmetric-key encryption scheme* $\Pi = (\mathcal{E}, \mathcal{D})$ *consists of two algorithms.*

– *The encryption algorithm* $\mathcal{E}_x(m)$ *is a deterministic algorithm that takes a symmetric-key* $x \in \mathtt{KSPC}(k)$ *and a message* $m \in \mathtt{MSPC}(k)$*, and returns a ciphertext* c*. Note that* $\mathtt{KSPC}(k)$ *and* $\mathtt{MSPC}(k)$ *are the key space and the message space for* k*, respectively. They are uniquely determined by a security parameter* 1^k*.*
– *The decryption algorithm* $\mathcal{D}_x(c)$ *is a deterministic algorithm that takes a symmetric key* x *and a ciphertext* c*, and returns the corresponding plaintext* m*.*

We require that, for any $k \in \mathbb{N}$*, if* $x \in \mathtt{KSPC}(k)$*,* $m \in \mathtt{MSPC}(k)$*, and* $c \leftarrow \mathcal{E}_x(m)$*, then* $m = \mathcal{D}_x(c)$*.*

3 Security Definitions

In this section, we review the security definitions for public-key encryption and symmetric-key encryption schemes.

3.1 Public-Key Encryption

γ-uniformity We review a property of public-key encryption, called γ-uniformity, following [15].

Definition 3 (γ-uniformity). *Let* $\Pi = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *be a public-key encryption scheme. We say that* Π *is* γ*-uniform, if, for any* $I \leftarrow \mathcal{G}(1^k)$*,* $(pk, sk) \leftarrow K(I)$*,* $m \in \mathtt{MSPC}(pk)$*, and* $y \in \{0,1\}^*$*,*

$$\Pr[r \xleftarrow{R} \mathtt{COINS}(pk) \ : \ y = \mathcal{E}_{pk}(x;r)] < \gamma.$$

One-Wayness We review a weak security notion for public-key encryption, called one-wayness, following [15].

Definition 4 (OW). *Let* $\Pi = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *be a public-key encryption scheme. Let* A *be an adversary. We define the advantage of* A *via*

$$\mathbf{Adv}^{\mathrm{ow}}_{\Pi,A}(k) = \Pr[I \leftarrow \mathcal{G}(1^k);\ (pk, sk) \leftarrow \mathcal{K}(I);\ m \xleftarrow{R} \mathtt{MSPC}(pk);\ c \leftarrow \mathcal{E}_{pk}(m) \ : \ A(c, pk) = m].$$

We say that A *is a* (t, ϵ)*-adversary for* Π *in the sense of OW if* A *runs in at most time* t *and archives* $\mathbf{Adv}^{\mathrm{ow}}_{\Pi,A}(k) \geq \epsilon$*. We say that* Π *is* (t, ϵ)*-secure in the sense of OW if there is no* (t, ϵ)*-adversary for* Π *in that sense.*

Anonymity In 2001, Bellare, Boldyreva, Desai, and Pointcheval [2] 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 anonymity, then the receiver is anonymous from the point of view of the adversary. In [2], they also formalized the property of "anonymity." Similar notions had been proposed Abadi and Rogaway [1], Fischlin [13], Camenisch and Lysyanskaya [8], Sako [25], and Desai [12], however, the adaptive chosen ciphertext attack does not seem to have been considered before in the context of key-privacy. The definition by Bellare, Boldyreva, Desai, and Pointcheval [2] can be considered under either the chosen plaintext attack or the adaptive chosen ciphertext attack, yielding two notions of security, IK-CPA and IK-CCA. (IK means "indistinguishability of keys.") We describe the definition of the anonymity, following [2].

Definition 5 (IK-CPA, IK-CCA [2]). *Let $\Pi = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme. Let A_{cpa} and A_{cca} be adversaries that run in two stages,* find *and* guess*. The adversaries A_{cpa} and A_{cca} have access to some oracles $\mathcal{O}_{\mathrm{cpa}}$ and O_{cca}, respectively. For atk $\in \{$cpa, cca$\}$, we define the advantages of A_{atk} via*

$$\mathbf{Adv}^{\text{ik-atk}}_{\Pi, A_{\mathrm{atk}}}(k) = 2 \cdot \Pr[I \leftarrow \mathcal{G}(1^k);\ (pk_0, sk_0), (pk_1, sk_1) \leftarrow \mathcal{K}(I);\\ (m, \mathsf{si}) \leftarrow A^{\mathcal{O}_{\mathrm{atk}}}_{\mathrm{atk}}(\mathsf{find}, pk_0, pk_1);\ b \xleftarrow{R} \{0,1\};\ c \leftarrow \mathcal{E}_{pk_b}(m)\ :\ A^{\mathcal{O}_{\mathrm{atk}}}_{\mathrm{atk}}(\mathsf{guess}, c, \mathsf{si}) = b] - 1$$

where $\mathcal{O}_{\mathrm{cpa}} = \epsilon$ and $\mathcal{O}_{\mathrm{cca}} = (\mathcal{D}_{sk_0}, \mathcal{D}_{sk_1})$. Note that si *is the state information. It contains the public keys pk_0, pk_1, the message m, and so on. We require that $m \in \mathtt{MSPC}(pk_0) \cap \mathtt{MSPC}(pk_1)$. We also require that A_{cca} never queries the challenge c to either $\mathcal{D}_{sk_0}$ or $\mathcal{D}_{sk_1}$ in the guess stage.*

We say that A_{cpa} is a (t, ϵ)-adversary for Π in the sense of IK-CPA if A_{cpa} runs in at most time t and achieves $\mathbf{Adv}^{\text{ik-cpa}}_{\Pi, A_{\mathrm{cpa}}}(k) \geq \epsilon$.

Similarly, we say that A_{cca} is a (t, q_d, ϵ)-adversary for Π in the sense of IK-CCA if A_{cca} runs in at most time t, makes a total number of q_d queries to decryption oracles $\mathcal{D}_{sk_0}$ and $\mathcal{D}_{sk_1}$, and achieves $\mathbf{Adv}^{\text{ik-cca}}_{\Pi, A_{\mathrm{cca}}}(k) \geq \epsilon$.

We say that Π is (t, ϵ)-secure (respectively (t, q_d, ϵ)-secure) in the sense of IK-CPA (resp. IK-CCA) if there is no (t, ϵ)-adversary (resp. (t, q_d, ϵ)-adversary) for Π in the corresponding sense.

Anonymity in the Random Oracle Model. We can consider the definition of the anonymity in the random oracle model in a similar way as that in the standard model described above.

We define Ω as the map family from an appropriate range. The domain and range depend on the underlying encryption scheme. Even if we choose two random functions that have distinct domains and distinct ranges respectively, we just write the experiment, for convenience, as $G, H \leftarrow \Omega$, instead of preparing two map families.

In the random oracle model, we begin the experiment of A_{atk} described above (which defines advantage) by $H \leftarrow \Omega$. Then, we add the random oracle H to both $\mathcal{O}_{\mathrm{cpa}}$ and $\mathcal{O}_{\mathrm{cca}}$, and allow that for $i \in \{0,1\}$, $\mathcal{E}_{pk_i}$ and $\mathcal{D}_{sk_i}$ may depend on H (which we write $\mathcal{E}^H_{pk_i}$ and $\mathcal{D}^H_{sk_i}$, respectively).

We define the adversaries in a similar way as those in the standard model, that is, we define a (t, q_h, ϵ)-adversary in the sense of IK-CPA in the random oracle model and a (t, q_h, q_d, ϵ)-adversary in the sense of IK-CCA in the random oracle model where the adversary makes at most q_h queries to H.

We say that Π is (t, q_h, ϵ)-secure (respectively (t, q_h, q_d, ϵ)-secure) in the sense of IK-CPA (resp. IK-CCA) in the random oracle model if there is no (t, q_h, ϵ)-adversary (resp. (t, q_h, q_d, ϵ)-adversary) for Π in the corresponding sense in the random oracle model.

3.2 Symmetric-Key Encryption

Find-Guess We review a security notion for symmetric-key encryption, called find-guess (FG), following [15].

Definition 6 (FG). *Let $\Pi = (\mathcal{E}, \mathcal{D})$ be a symmetric-key encryption scheme. Let A be an adversary that runs in two stages,* find *and* guess*. We define the advantage of A via*

$$\mathbf{Adv}^{\mathrm{fg}}_{\Pi}(k) = 2 \cdot \Pr[x \xleftarrow{R} \mathtt{KSPC}(k);\ (m_0, m_1, \mathsf{si}) \leftarrow A(\mathsf{find}, k);\\ b \xleftarrow{R} \{0,1\};\ c \leftarrow \mathcal{E}_x(m_b)\ :\ A(\mathsf{guess}, c, \mathsf{si}) = b] - 1.$$

We require that $m_0 \neq m_1$ and $m_0, m_1 \in \mathtt{MSPC}(k)$.

We say that A is a (t, ϵ)-adversary for Π in the sense of FG if A runs in at most time t and achieves $\mathbf{Adv}^{\mathrm{fg}}_{\Pi,A}(k) \geq \epsilon$.

We say that Π is (t, ϵ)-secure in the sense of FG if there is no (t, ϵ)-adversary for Π in the sense of FG.

4 Plaintext Awareness in the Two-Key Setting

In this section, we propose the notion of plaintext awareness in the two-key setting (PATK), and prove that PATK implies IK-CCA.

We describe the definition of plaintext awareness in the two-key setting.

Definition 7 (Plaintext Awareness in the two-key setting and Knowledge Extractor for PATK). *Let $\Pi = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme. Let B and K be algorithms, called an adversary for PATK and a knowledge extractor for PATK, respectively. They work in the random oracle model as follows:*

- *B is a (q_h, q_e)-adversary for PATK that takes two public-keys pk_0, pk_1 and an index $i \in \{0,1\}$, and makes at most q_h queries to H and q_e queries to the encryption oracles, $\mathcal{E}^H_{pk_0}$ and $\mathcal{E}^H_{pk_1}$. B finally outputs $c \notin C$, where*
  - *T_H denotes the set of all pairs of a B's query and the corresponding answer from H, and*
  - *C denotes the set of all answers from $\mathcal{E}^H_{pk_0}$ and $\mathcal{E}^H_{pk_1}$. (Note that C does not contain an information of which encryption oracle responded.)*

  We write this experiment as $(T_H, C, c, pk_i) \leftarrow \mathtt{run}\ B^{H, \mathcal{E}^H_{pk_0}, \mathcal{E}^H_{pk_1}}(pk_0, pk_1, i)$.
- *Knowledge extractor K for PATK takes (T_H, C, c, pk_i) and outputs a string m.*

For any $k \in \mathbb{N}$ and $i \in \{0,1\}$, we define

$$\mathbf{Succ}^{\mathrm{patk}}_{K,B,\Pi,i}(k) = \Pr[H \leftarrow \Omega;\ I \leftarrow \mathcal{G}(1^k);\ (pk_0, sk_0), (pk_1, sk_1) \leftarrow \mathcal{K}(I);\\ (T_H, C, c, pk_i) \leftarrow \mathtt{run}\ B^{H, \mathcal{E}^H_{pk_0}, \mathcal{E}^H_{pk_1}}(pk_0, pk_1, i)\ :\ K(T_H, C, c, pk_i) = \mathcal{D}^H_{sk_i}(c)].$$

We say that K is a $(t_{\mathrm{KETK}}, \lambda, q_h, q_e)$-knowledge extractor for PATK of Π if for any (q_h, q_e)-adversary $B$and $i \in \{0,1\}$, K runs in at most time t_{KETK} and achieves $\mathbf{Succ}^{\mathrm{patk}}_{K,B,\Pi,i}(k) \geq \lambda$.

We say that Π is $(t_{\mathrm{cpa}}, t_{\mathrm{KETK}}, q_h, q_e, \epsilon, \lambda)$-secure in the sense of PATK if Π is $(t_{\mathrm{cpa}}, q_h, \epsilon)$-secure in the sense of IK-CPA, and there exists a $(t_{\mathrm{KETK}}, \lambda, q_h, q_e)$-knowledge extractor K for PATK of Π.

There are some differences between the definition of PA in [3] and that of PATK (For the comparison of the definitions, we describe the definitions of the indistinguishability and the plaintext awareness in Appendix **??**.). First, the adversary B in our definition receives two public keys and two encryption oracles, while the adversary in the definition of PA receives one public key and one encryption oracle. Second, we define the success probability of B for any index $i \in \{0,1\}$.

This indicates under which key, pk_0 or pk_1, the knowledge extractor K for PATK should decrypt c. Third, in the definition of PA, the list C contains the answers (ciphertexts) from only one encryption oracle $\mathcal{E}^H_{pk}$. When we prove that PA implies IND-CCA, C plays an important role, that is, C contains the challenge ciphertext of IND-CCA game to give it to the adversary B for PA. In our definition, if we use C to prove that PATK implies IK-CCA, C has to contain the challenge ciphertext of IK-CCA game and the challenge ciphertext is encrypted by either pk_0 or pk_1. Therefore, in our definition, we define that the list C consists of the answers (ciphertexts) from *both* $\mathcal{E}^H_{pk_0}$ *and* $\mathcal{E}^H_{pk_1}$.

It is easy to see that if there exists a knowledge extractor K for PATK of Π, then we can use K as a knowledge extractor for PA of Π. That is, if the public-key encryption scheme Π is secure in the sense of PATK and IND-CPA, then Π is secure in the sense of PA. However, it is not clear that we can use the knowledge extractor for PA of Π as that for PATK of Π. The difficulty of proving this seems to depend on the third difference described above.

We prove the following theorem.

Theorem 1. *If the public encryption scheme Π is $(t_{\mathrm{cpa}}, t_{\mathrm{KETK}}, q_h, 1, \epsilon, \lambda)$-secure in the sense of PATK, then Π is $(t_{\mathrm{cca}}, q_h, q_d, \epsilon')$-secure in the sense of IK-CCA where*

$$t_{\mathrm{cca}} = t_{\mathrm{cpa}} - q_d \cdot t_{\mathrm{KETK}} \text{ and } \epsilon' = \epsilon + 2q_d \cdot (1 - \lambda).$$

Proof. In [3], Bellare, Desai, Pointcheval, and Rogaway proved that PA implies IND-CCA. We prove Theorem 1 in a similar way.

Let A_{cca} be an $(t_{\mathrm{cca}}, q_h, q_d, \epsilon)$-adversary of Π in the sense of IK-CCA. We construct an adversary A_{cpa} of Π in the sense of IK-CPA by using A_{cca}.

We construct the algorithm A_{cpa} as follows. Note that A_{cpa} simulates A_{cca}'s oracles H, $\mathcal{D}_{sk_0}$, and $\mathcal{D}_{sk_1}$ as described below.

1. A_{cpa} initializes two lists, T_H and C to empty.
2. $A_{\mathrm{cpa}}(\mathsf{find}, pk_0, pk_1)$ runs A_{cca} as $(m, \mathsf{si}) \leftarrow A_{\mathrm{cca}}(\mathsf{find}, pk_0, pk_1)$ and outputs (m, si).
3. A_{cpa} receives a challenge ciphertext $\hat{c} = \mathcal{E}^H_{pk_b}(m)$ where $b \overset{R}{\leftarrow} \{0, 1\}$.
4. $A_{\mathrm{cpa}}(\mathsf{guess}, \hat{c})$ runs A_{cca} as $d \leftarrow A_{\mathrm{cca}}(\mathsf{guess}, \hat{c})$ and outputs d.

A_{cpa} simulates A_{cca}'s oracle as follows:

- When A_{cca} makes a query h to H, A_{cpa} makes a query h to *its* oracle H and obtains an answer $H(h)$. Then, A_{cpa} returns $H(h)$ to A_{cca} and puts $(h, H(h))$ into the list T_H.
- When A_{cca} makes a decryption query c to $\mathcal{D}^H_{sk_i}$, A_{cpa} runs the knowledge extractor K as follows.
  - In the find stage, A_{cpa} runs K as $m \leftarrow K(T_H, \epsilon, c, pk_i)$ and returns m to A_{cca}.
  - In the guess stage, A_{cpa} runs K as $m \leftarrow K(T_H, \hat{c}, c, pk_i)$ and returns m to A_{cca}.

To guarantee that the knowledge extractor K for PATK outputs a correct answer (a corresponding plaintext m or an invalid symbol $\perp$), for $j \in \{1, 2, \cdots, q_d\}$ we construct the adversary B_j for PATK as follows. Note that B_j simulates A_{cca}'s oracles H, $\mathcal{D}_{sk_0}$, and $\mathcal{D}_{sk_1}$ as described below. Note that $B_j(pk_0, pk_1, i)$ returns some value and halts when A_{cca} makes its j-th decryption query.

1. B_j initializes two lists, T_H and C to empty.
2. B_j runs A_{cca} as $(m, \mathsf{si}) \leftarrow A_{\mathrm{cca}}(\mathsf{find}, pk_0, pk_1)$.
3. B_j picks a random bit $b \overset{R}{\leftarrow} \{0, 1\}$ and makes an oracle query as $\hat{c} \leftarrow \mathcal{E}^H_{pk_b}(m)$.
4. B_j runs $A_{\mathrm{cca}}(\mathsf{guess}, \hat{c})$. (Note that B_j is sure to halt before A_{cca} outputs d. See below.)

$B_j(pk_0, pk_1, i)$ simulates A_{cca}'s oracle as follows:

– When A_{cca} makes a query h to H, A_{cpa} makes a query h to *its* oracle H and obtains an answer $H(h)$. Then, A_{cpa} returns $H(h)$ to A_{cca} and puts $(h, H(h))$ into the list T_H.
– When A_{cca} makes a j'-th decryption query c to $\mathcal{D}^H_{sk_i}$, A_{cpa} runs the knowledge extractor K as follows.
  • In the find stage, if $j' = j$ then B_j returns c and halts; otherwise, A_{cpa} runs K as $m \leftarrow K(T_H, \epsilon, c, pk_i)$ and returns m to A_{cca}.
  • In the guess stage, if $j' = j$ then B_j returns c and halts; otherwise, A_{cpa} runs K as $m \leftarrow K(T_H, \hat{c}, c, pk_i)$ and returns m to A_{cca}.

Since $j \leq q_d$ and A_{cca} makes at most q_d queries to the decryption oracles, B_j is sure to output c and halt before A_{cca} outputs d in the guess stage.

We analyze the success probability of A_{cpa}. We have that for any $j \in \{1, 2, \cdots, q_d\}$ the distribution of $(T_H, C, c, pk_i) \leftarrow \mathtt{run}\ B_j^{H, \mathcal{E}^H_{pk_0}, \mathcal{E}^H_{pk_1}}(pk_0, pk_1, i)$ where

$$H \leftarrow \Omega;\ I \leftarrow \mathcal{G}(1^k);\ (pk_0, sk_0), (pk_1, sk_1) \leftarrow \mathcal{K}(I)$$

and the distribution of the j-th input for K in the above adversary A_{cpa} is identical. Therefore,

$$\Pr[A_{\mathrm{cpa}}(\mathsf{find}, pk_0, pk_1) = A_{\mathrm{cca}}(\mathsf{find}, pk_0, pk_1)] \geq 1 - q_d^{\mathrm{find}} \cdot (1 - \lambda)$$

and

$$\begin{aligned}\Pr[&A_{\mathrm{cpa}}(\mathsf{guess}, c, (\mathsf{si}, T_H)) = A_{\mathrm{cca}}(\mathsf{guess}, c, \mathsf{si}) \\ &| A_{\mathrm{cpa}}(\mathsf{find}, pk_0, pk_1) = A_{\mathrm{cca}}(\mathsf{find}, pk_0, pk_1)] \geq 1 - (q_d - q_d^{\mathrm{find}}) \cdot (1 - \lambda)\end{aligned}$$

where q_d^{find} is a number of decryption queries of A_{cca} in the find stage. Hence, $\epsilon' \geq \epsilon - 2q_d(1 - \lambda)$.

It is easy to see that the running time of A_{cpa} is less than $t_{\mathrm{cca}} + q_d \cdot t_{\mathrm{KETK}}$.

5 Fujisaki–Okamoto Conversion

In this section, we review the conversion proposed by Fujisaki and Okamoto [15].

Let $\Pi^{\mathrm{pub}} = (\mathcal{G}^{\mathrm{pub}}, \mathcal{K}^{\mathrm{pub}}, \mathcal{E}^{\mathrm{pub}}, \mathcal{D}^{\mathrm{pub}})$ be a public-key encryption scheme and let $\Pi^{\mathrm{sym}} = (\mathcal{E}^{\mathrm{sym}}, \mathcal{D}^{\mathrm{sym}})$ be a symmetric-key encryption scheme. Let $G : \mathtt{MSPC}^{\mathrm{pub}} \to \mathtt{KSPC}^{\mathrm{sym}}$ and $H : \mathtt{MSPC}^{\mathrm{pub}} \times \mathtt{MSPC}^{\mathrm{sym}} \to \mathtt{COINS}^{\mathrm{pub}}$ be hash functions.

A public-key encryption scheme $\Pi^{\mathrm{hy}} = (\mathcal{G}^{\mathrm{hy}}, \mathcal{K}^{\mathrm{hy}}, \mathcal{E}^{\mathrm{hy}}, \mathcal{D}^{\mathrm{hy}})$ derived from the Fujisaki-Okamoto conversion is as follows:

– Common key generation and key generation: $\mathcal{G}^{\mathrm{hy}}$ and $\mathcal{K}^{\mathrm{hy}}$ are the same as $\mathcal{G}^{\mathrm{pub}}$ and $\mathcal{K}^{\mathrm{pub}}$, respectively.
– Encryption:

$$\mathcal{E}^{\mathrm{hy}}_{pk}(m; \sigma) = \mathcal{E}^{\mathrm{pub}}_{pk}(\sigma; H(\sigma, m)) \,||\, \mathcal{E}^{\mathrm{sym}}_{G(\sigma)}(m)$$

  where $\mathtt{COINS}^{\mathrm{hy}} = \mathtt{MSPC}^{\mathrm{pub}}$ and $\mathtt{MSPC}^{\mathrm{hy}} = \mathtt{MSPC}^{\mathrm{sym}}$.
– Decryption:

$$\mathcal{D}^{\mathrm{hy}}_{sk}(c_1 || c_2) = \begin{cases} \hat{m} & \mathtt{if}\ c_1 = \mathcal{E}^{\mathrm{pub}}_{pk}(\hat{\sigma}; H(\hat{\sigma}, \hat{m})) \\ \perp & \mathtt{otherwise} \end{cases}$$

  where $\hat{\sigma} \leftarrow \mathcal{D}^{\mathrm{pub}}_{sk}(c_1)$ and $\hat{m} \leftarrow \mathcal{D}^{\mathrm{sym}}_{G(\hat{\sigma})}(c_2)$.

Fujisaki and Okamoto showed that the public-key encryption scheme Π^{hy} is secure in the sense of IND-CCA in the random oracle model when

– Π^{pub} is γ-uniform ($\gamma < 1$) and secure in the sense of OW, and
– Π^{sym} is secure in the sense of FG.

6 Generic Conversion for the Anonymity

In this section, we propose the generic conversion for the anonymity, that is, we prove that the public-key encryption scheme derived from the Fujisaki-Okamoto conversion with the following assumptions is secure in the sense of IK-CCA in the random oracle model.

- Π^{pub} use the common message space $\mathtt{MSPC}^{\mathrm{pub}}(I)$ and the common randomness space $\mathtt{COINS}^{\mathrm{pub}}(I)$ as the message space $\mathtt{MSPC}^{\mathrm{pub}}(pk)$ and the randomness space $\mathtt{COINS}^{\mathrm{pub}}(pk)$, respectively, for any public key pk outputted by $K(I)$,
- Π^{pub} is secure in the sense of IK-CPA,
- Π^{pub} is γ-uniform ($\gamma < 1$) and secure in the sense of OW, and
- Π^{sym} is secure in the sense of FG.

Since these conditions are sufficient that Π^{hy} meets IND-CCA, we can get a public-key encryption scheme which is secure in the sense of IND-CCA and IK-CCA in the random oracle model when we assume the above four conditions.

IK-CPA Security. We prove the following lemma with respect to the anonymity property.

Lemma 1. *Let Π^{pub} be a public-key encryption scheme where Π^{pub} uses the common message space $\mathtt{MSPC}^{\mathrm{pub}}(I)$ and the common randomness space $\mathtt{COINS}^{\mathrm{pub}}(I)$ as the message space $\mathtt{MSPC}^{\mathrm{pub}}(pk)$ and the randomness space $\mathtt{COINS}^{\mathrm{pub}}(pk)$, respectively, for any public key pk outputted by $K(I)$.*

Suppose that Π^{pub} is (t_1, ϵ_1)-secure in the sense of IK-CPA, and (t_2, ϵ_2)-secure in the sense of OW. Let ℓ_2 be the size of $\mathtt{MSPC}^{\mathrm{sym}}$. Then, Π^{hy} is (t, q_g, q_h, ϵ)-secure in the sense of IK-CPA in the random oracle model, where $t = \min\{t_1, t_2\} - \mathit{poly}(\ell_2)$ and $\epsilon = \epsilon_1 + 2(q_g + q_h) \cdot \epsilon_2$.

Remark 1. Note that IK-CPA does not imply OW. For example, let $\Pi = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme which is secure in the sense of IK-CPA. Then, consider the public-key encryption scheme Π' whose encryption algorithm is defined as $\mathcal{E}'_{pk}(m) := \mathcal{E}_{pk}(m)||m$. We can easily see that Π' meets IK-CPA, and does not meet OW.

Proof. Suppose that A is a (t, q_g, q_h, ϵ)-adversary for Π^{hy} in the sense of IK-CPA in the random oracle model. We show that there exists a (t_1, ϵ_1)-adversary B for Π^{pub} in the sense of IK-CPA and a (t_2, ϵ_2)-adversary C for Π^{pub} in the sense of OW, where $t = \min\{t_1, t_2\} - \mathit{poly}(\ell_2)$ and $\epsilon = \epsilon_1 + 2(q_g + q_h) \cdot \epsilon_2$.

We construct the adversaries B and C by using the adversary A. B and C have to simulate the random oracles G and H for A. We describe how to simulate the random oracles in both B and C. We use the lists $\mathcal{T}_G$ and $\mathcal{T}_H$ which are initially empty lists.

- *The simulation of G.* For a query σ, if there exist an entry $(\sigma', g') \in \mathcal{T}_G$ such that $\sigma = \sigma'$, it returns g' to A. Otherwise, it picks a string $g \xleftarrow{R} \mathtt{KSPC}^{\mathrm{sym}}(k)$, returns g to A, and puts (σ, g) on the list $\mathcal{T}_G$.
- *The simulation of H.* For a query (σ, m), if there exist an entry $(\sigma', m', h') \in \mathcal{T}_H$ such that $\sigma = \sigma'$ and $m = m'$, it returns h' to A. Otherwise, it picks a string $h \xleftarrow{R} \mathtt{COINS}^{\mathrm{pub}}(I)$, returns h to A, and puts (σ, m, h) on the list $\mathcal{T}_H$.

We construct the adversary B in the sense of IK-CPA as follows.

$\mathtt{Algorithm}\ B(\mathsf{find}, pk_0, pk_1)$	$\mathtt{Algorithm}\ B(\mathsf{guess}, c, \mathsf{si}')$
$(m, \mathsf{si}) \leftarrow A(\mathsf{find}, pk_0, pk_1)$	$x \xleftarrow{R} \mathtt{KSPC}^{\mathrm{sym}}(k)$
$\sigma \xleftarrow{R} \mathtt{MSPC}^{\mathrm{pub}}(I)$	$c' \leftarrow c\|\|\mathcal{E}^{\mathrm{sym}}_x(m)$
$\mathsf{si}' \leftarrow (\mathsf{si}, m)$	$b' \leftarrow A(\mathsf{guess}, c, \mathsf{si})$
$\mathtt{return}\ (\sigma, \mathsf{si}')$	$\mathtt{return}\ b'$

We construct the adversary C in the sense of OW as follows.

$\mathtt{Algorithm}\ C(c, pk)$
$(pk', sk') \leftarrow \mathcal{K}^{\mathrm{pub}}(I)$
$d \xleftarrow{R} \{0,1\};\ pk_d \leftarrow pk;\ pk_{1-d} \leftarrow pk'$
$(m, \mathsf{si}) \leftarrow A(\mathsf{find}, pk_0, pk_1)$
$b \xleftarrow{R} \{0,1\};\ x \xleftarrow{R} \mathtt{KSPC}^{\mathrm{sym}}(k);\ c' \leftarrow c||\mathcal{E}_x^{\mathrm{sym}}(m)$
$b' \leftarrow A(\mathsf{guess}, c')$
$\hat{\sigma} \xleftarrow{R} \{\sigma' | (\sigma', g') \in \mathcal{T}_G \text{ or } (\sigma', m', h') \in \mathcal{T}_H\}$
$\mathtt{return}\ \hat{\sigma}$

It is easy to see that the running times of B and C is at most that of A plus the time for computing $\mathcal{E}_x^{\mathrm{sym}}(m)$, that is, $t_1, t_2 < t + poly(\ell_2)$.

We analyze the advantages of B and C. We define the following events.

- $\mathsf{AskA} = [A$ asks σ to the oracle G or asks (σ, m) to the oracle H where the challenge ciphertext is $c' = \mathcal{E}_{pk_b}^{\mathrm{pub}}(\sigma; H(\sigma, m))||\mathcal{E}_{G(\sigma)}^{\mathrm{sym}}(m).]$
- $\mathsf{SuccA} = [G, H \leftarrow \Omega;\ I \leftarrow \mathcal{G}^{\mathrm{hy}}(1^k);\ (pk_0, sk_0), (pk_1, sk_1) \leftarrow \mathcal{K}^{\mathrm{hy}}(I);$ $(m, \mathsf{si}) \leftarrow A^{G,H}(\mathsf{find}, pk);\ b \xleftarrow{R} \{0,1\};\ c' \leftarrow \mathcal{E}_{pk_b}^{\mathrm{hy}}(m)\ :\ A^{G,H}(\mathsf{guess}, c', \mathsf{si}) = b]$
- $\mathsf{SuccB} = [I \leftarrow \mathcal{G}^{\mathrm{pub}}(1^k);\ (pk_0, sk_0), (pk_1, sk_1) \leftarrow \mathcal{K}^{\mathrm{pub}}(I);$ $(\sigma, \mathsf{si}) \leftarrow B(\mathsf{find}, pk);\ b \xleftarrow{R} \{0,1\};\ c \leftarrow \mathcal{E}_{pk_b}^{\mathrm{pub}}(\sigma)\ :\ B(\mathsf{guess}, c, \mathsf{si}) = b]$
- $\mathsf{SuccC} = [I \leftarrow \mathcal{G}^{\mathrm{pub}}(1^k);\ (pk, sk) \leftarrow \mathcal{K}^{\mathrm{pub}}(I);\ \sigma \xleftarrow{R} \mathtt{MSPC}^{\mathrm{pub}}(pk)$ $c \leftarrow \mathcal{E}_{pk}^{\mathrm{pub}}(\sigma)\ :\ C(c, pk) = \sigma]$

In the experiment of B, if the event $\neg\mathsf{AskA}$ holds, the view of A simulated in B is identical to the real A's view. Therefore, $\Pr[\mathsf{SuccB}] \geq \Pr[\mathsf{SuccA}|\neg\mathsf{AskA}] \cdot \Pr[\neg\mathsf{AskA}]$.

In the experiment of C, if the event AskA holds, there exist a string σ such that $c = \mathcal{E}_{pk_b}^{\mathrm{pub}}(\sigma)$ in $\{\sigma' | (\sigma', g') \in \mathcal{T}_G \text{ or } (\sigma', m', h') \in \mathcal{T}_H\}$ and C can output the correct answer with probability at least $1/(q_G + q_H)$. Furthermore, if $b = d$ holds, the probability that C asks such σ is the same as the probability that the real A asks such σ. Therefore, $\Pr[\mathsf{SuccC}] \geq \Pr[b = d] \times \Pr[\mathsf{SuccC}|b = d] \geq 1/(2(q_G + q_H)) \cdot \Pr[\mathsf{AskA}]$.

Hence, we have

$$\begin{aligned}\Pr[\mathsf{SuccA}] &= \Pr[\mathsf{SuccA}|\neg\mathsf{AskA}] \cdot \Pr[\neg\mathsf{AskA}] + \Pr[\mathsf{SuccA}|\mathsf{AskA}] \cdot \Pr[\mathsf{AskA}] \\ &\leq \Pr[\mathsf{SuccA}|\neg\mathsf{AskA}] \cdot \Pr[\neg\mathsf{AskA}] + \Pr[\mathsf{AskA}] \\ &\leq \Pr[\mathsf{SuccB}] + 2(q_G + q_H) \cdot \Pr[\mathsf{SuccC}].\end{aligned}$$

Since $\epsilon = 2 \cdot \Pr[\mathsf{SuccA}] - 1$, $\epsilon_1 = 2 \cdot \Pr[\mathsf{SuccB}] - 1$, and $\epsilon_2 = \Pr[\mathsf{SuccC}]$, we have $\epsilon \leq \epsilon_1 + (q_G + q_H) \cdot \epsilon_2$.

Knowledge Extractor for PATK. We show the existence of the knowledge extractor for PATK of our scheme.

Though we mentioned that we could not use the knowledge extractor for PA directly as that for PATK, fortunately, we can use the knowledge extractor for PA as that for PATK in the case of the Fujisaki-Okamoto conversion.

We show the following lemma.

Lemma 2. *Suppose that Π^{pub} is γ-uniform and (t_2, ϵ_2)-secure in the sense of OW. Suppose that Π^{sym} is (t_3, ϵ_3)-secure in the sense of FG. Let ℓ_1 and ℓ_2 be the sizes of $\mathtt{MSPC}^{\mathrm{pub}}$ and $\mathtt{MSPC}^{\mathrm{sym}}$, respectively. Then, there exist a $(t, \lambda, q_g, q_h, q_e)$-knowledge extractor K for PATK of Π^{hy} such that $t = (q_g + q_h) \cdot poly(\ell_1 + \ell_2)$ and $\lambda = 1 - 2q_e \cdot \epsilon_2 - 2\epsilon_3 - \gamma - 2^{-\ell_2}$.*

Proof. The construction of the knowledge extractor for PATK is the same as that for PA in [15]. We first describe the knowledge extractor $K(T_G, T_H, C, c, pk)$ as follows. Here, let $T_G = \{(\sigma_i, g_i)|i = 1, \ldots, q_g\}$ and $T_H = \{(\sigma'_j, m_j, h_j)|j = 1, \ldots, q_h\}$.

1. Set two empty lists, S_1 and S_2.
2. Find all elements in T_H such that $c_1 = \mathcal{E}^{\mathrm{pub}}_{pk}(\sigma'_j, h_j)$ and put them into list S_1. If $S_1 = \emptyset$, then output $\perp$.
3. For every $(\sigma'_j, m_j, h_j) \in S_1$, find all elements in T_G such that $\sigma_i = \sigma'_j$ and put them (i.e. $(\sigma'_j, m_j, h_j)||(\sigma_i, g_i)$'s) into S_2. If $S_2 = \emptyset$, then output $\perp$.
4. Check in S_2 if there exists a $(\sigma'_j, m_j, h_j)||(\sigma_i, g_i)$ such that $c_2 = \mathcal{E}^{\mathrm{sym}}_{g_i}(m_j)$. If it exists in S_2, then output m_j otherwise output $\perp$.

This protocol runs in $(q_g + q_h) \cdot poly(\ell_1 + \ell_2)$.

Next, we examine the advantage of the knowledge extractor for PATK. We define the following events.

- $\mathsf{Inv0}$ is true if there exists $(c_1^*, c_2^*) \in C$ and $(\sigma_i, g_i) \in T_G$ or $(\sigma_j, m_j, h_j) \in T_H$ such that $\sigma_i = \mathcal{D}^{\mathrm{pub}}_{sk_0}(c_1^*)$ or $\sigma_j = \mathcal{D}^{\mathrm{pub}}_{sk_0}(c_1^*)$.
- $\mathsf{Inv1}$ is true if there exists $(c_1^*, c_2^*) \in C$ and $(\sigma_i, g_i) \in T_G$ or $(\sigma_j, m_j, h_j) \in T_H$ such that $\sigma_i = \mathcal{D}^{\mathrm{pub}}_{sk_1}(c_1^*)$ or $\sigma_j = \mathcal{D}^{\mathrm{pub}}_{sk_1}(c_1^*)$.
- $\mathsf{Inv} = \mathsf{Inv0} \vee \mathsf{Inv1}$.
- $p(S_1)$ true if $S_1 \neq \emptyset$.
- $p(S_2)$ true if $S_2 \neq \emptyset$.
- Find is true if there exists a $(\sigma'_j, m_j, h_j)||(\sigma_i, g_i)$ in S_2 such that $c_2 = \mathcal{E}^{\mathrm{sym}}_{g_i}(m_j)$.
- Fail is true if "the output of knowledge extractor K for PATK" $\neq \mathcal{D}^{\mathrm{hy}}_{sk}(c_1, c_2)$.

We further define the following events:

$$
\begin{aligned}
\text{`}\mathtt{1}' &= \mathsf{Inv}. \\
\text{`}\mathtt{00}' &= \neg\mathsf{Inv} \wedge \neg p(S_1). \\
\text{`}\mathtt{010}' &= \neg\mathsf{Inv} \wedge p(S_1) \wedge \neg p(S_2). \\
\text{`}\mathtt{0110}' &= \neg\mathsf{Inv} \wedge p(S_1) \wedge p(S_2) \wedge \neg\mathsf{Find}. \\
\text{`}\mathtt{0111}' &= \neg\mathsf{Inv} \wedge p(S_1) \wedge p(S_2) \wedge \mathsf{Find}.
\end{aligned}
$$

We have

$$
\begin{aligned}
\Pr[\mathsf{Fail}] &= \Pr[\mathsf{Fail}|\mathtt{1}] \cdot \Pr[\mathtt{1}] + \Pr[\mathsf{Fail}|\mathtt{00}] \cdot \Pr[\mathtt{00}] + \Pr[\mathsf{Fail}|\mathtt{010}] \cdot \Pr[\mathtt{010}] \\
&\quad + \Pr[\mathsf{Fail}|\mathtt{0110}] \cdot \Pr[\mathtt{0110}] + \Pr[\mathsf{Fail}|\mathtt{0111}] \cdot \Pr[\mathtt{0111}] \\
&\leq \Pr[\mathtt{1}] + \Pr[\mathsf{Fail}|\mathtt{00}] + \Pr[\mathsf{Fail}|\mathtt{010}] + \Pr[\mathsf{Fail}|\mathtt{0110}] + \Pr[\mathsf{Fail}|\mathtt{0111}] \\
&= \Pr[\mathtt{1}] + \Pr[\mathsf{Fail}|\mathtt{00}] + \Pr[\mathsf{Fail}|\mathtt{010}].
\end{aligned}
$$

We prove the following claim.

Claim. $\Pr[\mathtt{1}] \leq 2q_e \cdot \epsilon_2$.

Proof. We first consider $\Pr[\mathsf{Inv0}]$. For any $i \in \{0, 1\}$, when the adversary B makes a query m to the encryption oracle $\mathcal{E}^{hy}_{pk_i}$, the oracle picks random coins σ and returns $(\mathcal{E}^{\mathrm{pub}}_{pk_i}(\sigma, H(\sigma, m))||\mathcal{E}^{\mathrm{sym}}_{G(\sigma)}(m))$ to B. B makes at most q_e to the encryption oracles. Therefore, $\Pr[\mathtt{Inv0}] \leq q_e \cdot \epsilon_2$. Similarly, we have $\Pr[\mathtt{Inv1}] \leq q_e \cdot \epsilon_2$. Hence, $\Pr[\mathtt{1}] = \Pr[\mathtt{Inv}] \leq 2q_e \cdot \epsilon_2$

The proofs of the following claims are the same as those in [15].

Claim. $\Pr[\mathtt{Fail}|\mathtt{00} \leq \gamma$.

Claim. $\Pr[\mathtt{Fail}|\mathtt{010}] \leq 2\epsilon_3 + 2^{-\ell_2}$.

Therefore, $\Pr[\mathsf{Fail}] \leq 2q_e \cdot \epsilon_2 + \gamma + 2\epsilon_3 + 2^{-\ell_2}$. Hence,

$$\lambda = 1 - \Pr[\mathsf{Fail}] \geq 1 - (2q_e \cdot \epsilon_2 + \gamma + 2\epsilon_3 + 2^{-\ell_2}).$$

From Theorem 1 and Lemmas 1 and 2, we have the following theorem.

Theorem 2. *Let Π^{pub} be a public-key encryption scheme where Π^{pub} uses the common message space $\mathtt{MSPC}^{\mathrm{pub}}(I)$ and the common randomness space $\mathtt{COINS}^{\mathrm{pub}}(I)$ as the message space $\mathtt{MSPC}^{\mathrm{pub}}(pk)$ and the randomness space $\mathtt{COINS}^{\mathrm{pub}}(pk)$ for any public key pk outputted by $K(I)$, respectively.*

Suppose that Π^{pub} is γ-uniform, (t_1, ϵ_1)-secure in the sense of IK-CPA, and (t_2, ϵ_2)-secure in the sense of OW. Suppose that Π^{sym} is (t_3, ϵ_3)-secure in the sense of FG. Let ℓ_1 and ℓ_2 be the sizes of $\mathtt{MSPC}^{\mathrm{pub}}$ and $\mathtt{MSPC}^{\mathrm{sym}}$, respectively. Then, Π^{hy} is $(t, q_g, q_h, q_d, \epsilon)$-secure in the sense of IK-CCA in the random oracle model where $t = \min\{t_1, t_2\} - (q_g + q_h) \cdot poly(\ell_1 + \ell_2)$. and $\epsilon = \epsilon_1 + 2(q_g + q_h)\epsilon_2 + 2q_d(2\epsilon_2 + 2\epsilon_3 + \gamma + 2^{-\ell_2})$.

7 Concluding Remarks

In this paper, we have proposed the notion of plaintext awareness in the two-key setting, called PATK, and proved that if a public-key encryption scheme is secure in the sense of PATK, then it is also secure in the sense of IK-CCA. Since it looks much easier to prove that a public-key encryption scheme is secure in the sense of PATK than to prove directly that it is secure in the sense of IK-CCA, the notion of PATK is useful to prove the anonymity property of public-key encryption schemes. The previously proposed public-key encryption schemes in [2, 17, 18] which are based on RSA-OAEP and secure in the sense of IK-CCA seem to meet PAKE.

We have also proposed the first generic conversion scheme for the anonymity from IK-CPA to IK-CCA. More precisely, we have proved that the public-key encryption scheme derived from the Fujisaki-Okamoto conversion scheme, where the basic public-key encryption scheme is secure in the sense of IK-CPA, is secure in the sense of IK-CCA in the random oracle model.

It might be interesting to consider the definition of the plaintext awareness in the two-key setting without random oracles and the schemes in the standard model which meet the plaintext awareness in the two-key setting.

References

1. Abadi, M., and Rogaway, P. Reconciling Two Views of Cryptography (The Computational Soundness of Formal Encryption). In *Proceedings of the First IFIP International Conference on Theoretical Computer Science* (Sendai, Japan, August 2000), vol. 1872 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 3–22.
2. Bellare, M., Boldyreva, A., Desai, A., and Pointcheval, D. Key-Privacy in Public-Key Encryption. In *Advances in Cryptology – ASIACRYPT 2001* (Gold Coast, Australia, December 2001), C. Boyd, Ed., vol. 2248 of *LNCS*, Springer-Verlag, pp. 566–582. Full version of this paper, available via `http://www-cse.ucsd.edu/users/mihir/`.
3. Bellare, M., Desai, A., Pointcheval, D., and Rogaway, P. Relations among Notions of Security for Public-Key Encryption Schemes. In *Advances in Cryptology – CRYPTO '98* (Santa Barbara, California, USA, August 1998), H. Krawczyk, Ed., vol. 1462 of *LNCS*, Springer-Verlag, pp. 26–45.
4. Bellare, M., and Palacio, A. Towards Plaintext-Aware Public-Key Encryption without Random Oracles. In *Advances in Cryptology – ASIACRYPT 2004* (Jeju Island, Korea, December 2004), P. J. Lee, Ed., vol. 3329 of *LNCS*, Springer-Verlag, pp. 48–62.
5. 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 *LNCS*, Springer-Verlag, pp. 92–111.
6. Boneh, D. Simplified OAEP for the RSA and Rabin functions. In Kilian [20], pp. 275–291.
7. Boneh, D., and Franklin, M. K. Identity-Based Encryption from the Weil Pairing. In Kilian [20], pp. 213–229.

8. 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 *LNCS*, Springer-Verlag, pp. 93–118.
9. Coron, J.-S., Handschuh, H., Joye, M., Paillier, P., Pointcheval, D., and Tymen, C. GEM: A Generic Chosen-Ciphertext Secure Encryption Method. In *Topics in Cryptology – CT-RSA 2002* (San Jose, CA, USA, February 2002), B. Preneel, Ed., vol. 2271 of *LNCS*, Springer-Verlag, pp. 263–276.
10. Cui, Y., Kobara, K., and Imai, H. Compact Conversion Schemes for the Probabilistic OW-PCA Primitives. In *Advances in Cryptology – CRYPTO 2005* (Huhehaote, China, October 2003), S. Qing, eDieter Gollmann, and J. Zhou, Eds., vol. 2836 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 269–279.
11. Cui, Y., Kobara, K., and Imai, H. A Generic Conversion with Optimal Redundancy. In *Topics in Cryptology – CT-RSA 2005* (San Francisco, CA, USA, February 2005), A. Menezes, Ed., vol. 3376 of *LNCS*, Springer-Verlag, pp. 104–117.
12. Desai, A. The Security of All-or-Nothing Encryption: Protecting against Exhaustive Key Search. In *Advances in Cryptology – CRYPTO 2000* (Santa Barbara, California, USA, August 2000), M. Bellare, Ed., vol. 1880 of *LNCS*, Springer-Verlag, pp. 359–375.
13. Fischlin, M. Pseudorandom Function Tribe Ensembles Based on One-Way Permutations. In *Advances in Cryptology – EUROCRYPT '99* (Prague, Czech Republic, May 1999), J. Stern, Ed., vol. 1592 of *LNCS*, Springer-Verlag, pp. 432–445.
14. Fujisaki, E. Plaintext-Simulatability. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Cryptography and Information Security E89-A*, 1 (January 2006), 55–65.
15. Fujisaki, E., and Okamoto, T. Secure Integration of Asymmetric and Symmetric Encryption Schemes. In *Advances in Cryptology – CRYPTO '99* (Santa Barbara, California, USA, August 1999), M. Wiener, Ed., vol. 1666 of *LNCS*, Springer-Verlag, pp. 537–554.
16. Fujisaki, E., Okamoto, T., Pointcheval, D., and Stern, J. RSA-OAEP is Secure under the RSA Assumption. In Kilian [20], pp. 260–274.
17. 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 *LNCS*, Springer-Verlag, pp. 291–304.
18. 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 *LNCS*, Springer-Verlag, pp. 216–233.
19. Imai, H., and Zheng, Y., Eds. *Public Key Cryptography – PKC 2000, 3rd International Workshop on Theory and Practice in Public Key Cryptography* (Melbourne, Victoria, Australia, January 2000), vol. 1751 of *LNCS*, Springer-Verlag.
20. Kilian, J., Ed. *Advances in Cryptology – CRYPTO 2001* (Santa Barbara, California, USA, August 2001), vol. 2139 of *LNCS*, Springer-Verlag.
21. Okamoto, T., and Pointcheval, D. REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. In *Topics in Cryptology – CT-RSA 2003* (San Francisco, CA, USA, April 2001), D. Naccache, Ed., vol. 2020 of *LNCS*, Springer-Verlag, pp. 159–175.
22. Okamoto, T., and Pointcheval, D. The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes. In *Public Key Cryptography – PKC 2001, 4th International Workshop on Theory and Practice in Public Key Cryptography* (Cheju Island, Korea, February 2001), K. Kim, Ed., vol. 1992 of *LNCS*, Springer-Verlag, pp. 104–118.
23. Phan, D. H., and Pointcheval, D. Chosen-Ciphertext Security without Redundancy. In *Advances in Cryptology – ASIACRYPT 2003* (Taipei, Taiwan, November 2003), C. S. Laih, Ed., vol. 2894 of *LNCS*, Springer-Verlag, pp. 1–18.
24. Pointcheval, D. Chosen-Ciphertext Security for Any One-Way Cryptosystem. In Imai and Zheng [19], pp. 129–146.
25. Sako, K. An Auction Protocol Which Hides Bids of Losers. In Imai and Zheng [19], pp. 422–432.
26. Shoup, V. OAEP Reconsidered. In Kilian [20], pp. 239–259.

A Indistinguishability and Plaintext Awareness

A.1 Indistinguishability

In this section, we describe the definition of the indistinguishability of ciphertexts, following [15].

Definition 8 (IND-CPA, IND-CCA). *Let $\Pi = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme. Let A_{cpa} and A_{cca} be adversaries that run in two stages,* find *and* guess*. The adversaries A_{cpa} and*

A_{cca} have access to some oracles $\mathcal{O}_{\mathrm{cpa}}$ and O_{cca}, respectively. For atk $\in \{$cpa, cca$\}$, we define the advantages of A_{atk} via

$$\mathbf{Adv}^{\text{ind-atk}}_{\Pi,A_{\mathrm{atk}}}(k) = 2 \cdot \Pr[I \leftarrow \mathcal{G}(1^k);\ (pk, sk) \leftarrow \mathcal{K}(I);\ (m_0, m_1, \mathsf{si}) \leftarrow A^{\mathcal{O}_{\mathrm{atk}}}_{\mathrm{atk}}(\mathsf{find}, pk);\ b \xleftarrow{R} \{0,1\};\ c \leftarrow \mathcal{E}_{pk}(m_b)\ :\ A^{\mathcal{O}_{\mathrm{atk}}}_{\mathrm{atk}}(\mathsf{guess}, c, \mathsf{si}) = b] - 1$$

where $\mathcal{O}_{\mathrm{cpa}} = \epsilon$ and $\mathcal{O}_{\mathrm{cca}} = \mathcal{D}_{sk}$. Note that si *is the state information. It contains the public key pk, the messages m_0 and m_1, and so on. We require that $m_0 \neq m_1$ and $m_0, m_1 \in \mathtt{MSPC}(pk)$. We also require that A_{cca} never queries the challenge c to $\mathcal{D}_{sk}$ in the guess stage.*

We say that A_{cpa} is a (t, ϵ)-adversary for Π in the sense of IND-CPA if A_{cpa} runs in at most time t and achieves $\mathbf{Adv}^{\text{ind-cpa}}_{\Pi,A_{\mathrm{cpa}}}(k) \geq \epsilon$.

Similarly, we say that A_{cca} is a (t, q_d, ϵ)-adversary for Π in the sense of IND-CCA if A_{cca} runs in at most time t, asks at most q_d queries to decryption oracle $\mathcal{D}_{sk}$, and achieves $\mathbf{Adv}^{\text{ind-cca}}_{\Pi,A_{\mathrm{cca}}}(k) \geq \epsilon$.

We say that Π is (t, ϵ)-secure (respectively (t, q_d, ϵ)-secure) in the sense of IND-CPA (resp. IND-CCA) if there is no (t, ϵ)-adversary (resp. (t, q_d, ϵ)-adversary) for Π in the corresponding sense.

Indistinguishability in the Random Oracle Model. We can consider the definition of the indistinguishability in the random oracle model in a similar way as that in the standard model described above.

We define Ω as the map family from an appropriate range. The domain and range depend on the underlying encryption scheme. Even if we choose two random functions that have distinct domains and distinct ranges respectively, we just write the experiment, for convenience, as $G, H \leftarrow \Omega$, instead of preparing two map families.

In the random oracle model, we begin the experiment of A_{atk} described above (which defines advantage) by $H \leftarrow \Omega$. Then, we add the random oracle H to both $\mathcal{O}_{\mathrm{cpa}}$ and $\mathcal{O}_{\mathrm{cca}}$, and allow that $\mathcal{E}_{pk}$ and $\mathcal{D}_{sk}$ may depend on H (which we write $\mathcal{E}^H_{pk}$ and $\mathcal{D}^H_{sk}$, respectively).

We define the adversaries in a similar way as those in the standard model, that is, we define a (t, q_h, ϵ)-adversary in the sense of IND-CPA in the random oracle model and a (t, q_h, q_d, ϵ)-adversary in the sense of IND-CCA in the random oracle model where the adversary makes at most q_h queries to H.

We say that Π is (t, q_h, ϵ)-secure (respectively (t, q_h, q_d, ϵ)-secure) in the sense of IND-CPA (resp. IND-CCA) in the random oracle model if there is no (t, q_h, ϵ)-adversary (resp. (t, q_h, q_d, ϵ)-adversary) for Π in the corresponding sense in the random oracle model.

A.2 Knowledge Extractor and Plaintext Awareness

The notion of knowledge extractor and plaintext awareness for a public-key encryption scheme is defined in [5, 3]. We describe the definitions by Bellare, Desai, Pointcheval, and Rogaway [3].

Definition 9 (Knowledge Extractor and Plaintext Awareness). *Let $\Pi = (\mathcal{G}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme. Let B and K be algorithms, called adversary and knowledge extractor, respectively. They work in the random oracle model as follows:*

- *B is a (q_h, q_e)-adversary that takes a public-key pk and makes queries at most q_h and q_e times to the random oracle H and the encryption oracle $\mathcal{E}^H_{pk}$, respectively. B finally outputs $c \notin C$, where*
  - *T_H denotes the set of all pairs of B's queries and the corresponding answers from H,*
  - *C denotes the set of all answers from $\mathcal{E}^H_{pk}$.*

  We write the above experiment as $(T_H, C, c, pk) \leftarrow \mathtt{run}\ B^{H, \mathcal{E}^H_{pk}}(pk)$.
- *Knowledge extractor K takes (T_H, C, c, pk) and output a string m.*

For any $k \in \mathbb{N}$, we define

$$\mathbf{Succ}^{\mathrm{pa}}_{K,B,\Pi}(k) = \Pr[H \leftarrow \Omega;\ I \leftarrow \mathcal{G}(1^k);\ (pk, sk) \leftarrow \mathcal{K}(I);\\ (T_H, C, c, pk) \leftarrow \mathtt{run}\ B^{H,\mathcal{E}^H_{pk}}(pk)\ :\ K(T_H, C, c, pk) = \mathcal{D}^H_{sk}(c)].$$

We say that K is a $(t_{\mathrm{KE}}, \lambda, q_h, q_e)$-knowledge extractor for PA of Π if for any (q_h, q_e)-adversary B, K runs in at most time t_{KE} and achieves $\mathbf{Succ}^{\mathrm{pa}}_{K,B,\Pi}(k) \geq \lambda$.

We say that Π is $(t_{\mathrm{cpa}}, t_{\mathrm{KE}}, q_h, q_e, \epsilon, \lambda)$-secure in the sense of PA if Π is $(t_{\mathrm{cpa}}, q_h, \epsilon)$-secure in the sense of IND-CPA, and there exists a $(t_{\mathrm{KE}}, \lambda, q_h, q_e)$-knowledge extractor K for PA of Π.

Bellare, Desai, Pointcheval, and Rogaway [3] showed that if the public-key encryption scheme is secure in the sense of PA, then it is also secure in the sense of IND-CCA.