Relationship between Standard Model Plaintext Awareness and Message Hiding

Isamu Teranishi[†,‡] and Wakaha Ogata[‡]

† NEC Corporation.
1753, Shimonumabe, Nakahara-Ku, Kawasaki, Kanagawa, 211-8666, Japan.
‡ Tokyo Institute of Technology.
2-12-1 Ookayama, Meguro-ku Tokyo, 152-8550, Japan.
`teranisi@ah.jp.nec.com, wakaha@mot.titech.ac.jp`

Abstract. Recently, Bellare and Palacio succeeded in defining the plaintext awareness, which is also called PA2, in the standard model. They propose three valiants of the standard model PA2 named perfect, statistical, and computational PA2. In this paper, we study the relationship between the standard model PA2 and the property about message hiding, that is, IND-CPA. Although it seems that these two are independent notions at first glance, we show that all of the perfect, statistical, and computational PA2 in the standard model imply the IND-CPA security if the encryption function is oneway. By using this result, we also showed that "PA2 + Oneway ⇒ IND-CCA2". This result shows the "all-or-nothing" aspect of the PA2. That is, a standard model PA2 secure public-key encryption scheme either satisfies the strongest message hiding property, IND-CCA2, or does not satisfy even the weakest message hiding property, onewayness. We also showed that the computational PA2 notion is strictly stronger than the statistical one.

Keywords: Plaintext Awareness, Standard Model.

1 Introduction

The *Plaintext Awareness* [BR94,BDPR98,HLM03,BP04], which is also known as *PA2*, is a notion about the security of a public-key encryption scheme. Intuitively, we say that a public-key encryption scheme satisfies the PA2, if no adversary can generate a ciphertext "without knowing" the corresponding plaintext.

The PA2 notion is important, because it implies the chosen ciphertext security [BR94,BDPR98,BP04], if a public-key encryption scheme is the IND-CPA secure. Moreover, it is useful when one instantiates the ideal functions in the Dolev-Yao model [DY83], since the relation between the PA2 and the Dolev-Yao model is known [HLM03].

The original definition of the PA2 security was formalized in the random oracle model [BR94,BDPR98] and was highly dependent on this model, although the intuitive definition, mentioned above, does not depend on this model. Therefore, in the earlier study of the PA2, one of the main concerns was how to define the PA2 in the standard model.

In Asiacrypt 2004, Bellare and Palacio [BP04] succeeded in defining the standard model PA2. Their result is important, because we can analize encryption schemes from the new view point whether these are PA2 secure. Here we briefly review their definition. They define PA2 notion based on the indistinguishabilty of two worlds, "Dec world", and "Ext world". An adversary in the Dec world can access the decryption oracle and so on. In contrast, the adversary in the Ext world can access an extractor, which simulates the decryption oracle, and so on. The extractor has to simulate the decryption oracle by using only data "which the adversary knows". They define the three types of the PA2, named *perfect/statistical/computational* PA2, depending on that the Dec world and the Ext world are perfectly/statistically/computationally indistinguishable for the adversary.

They also succeeded in proving the fundamental theorem, which state that all of these plaintext awareness notions, together with IND-CPA security, imply the chosen ciphertext security.

1.1 Our Contributions

In this paper, we study the relationship between the standard model PA2 and the property about message hiding, that is, IND-CPA. At first glance, it seems that these two are independent notions. Indeed, it is well known that the random oracle model PA2 property does not imply the IND-CPA property and vise versa.

We however show that all of the perfect, statistical, and computational PA2 security in the standard model imply the IND-CPA security if the encryption function is oneway. Recall that the fundamental theorem that "(perfect, statistical, or computational) PA2 + IND-CPA ⇒ IND-CCA2" holds. Therefore, our result combining with the fundamental theorem shows the stronger variant of the fundamental theorem, "(perfect, statistical, or computational) PA2 + Oneway ⇒ IND-CCA2". This result shows the "all-or-nothing" aspect of the PA2. That is, the standard model PA2 secure public-key encryption scheme either satisfies the strongest message hiding property, IND-CCA2, or does not satisfy even weakest message hiding property, onewayness.

Our result has not only theoretical interest but also can be useful when one prove the IND-CCA2 securities of public-key encryption schemes. Recall that it is non trivial to show the IND-CPA securities of some schemes satisfying the random oracle PA2, such as schemes with OAEP+ [OP01], 3-round OAEP [PP04], or Kobara-Imai [KI01] padding. However, in the case for schemes satisfying the standard model PA2, we are not required to prove the IND-CPA securities, since our result assures it.

We also study the gap between the computational and statistical PA2 securities. That is, we show that the computational PA2 security is strictly stronger than the statistical one. It is interesting to compare our result with Fujisaki's result [F06] about the random oracle PA2. In his paper, he defined a *plaintext simulatability* (PS) notion, which was a "computational variant" of the random oracle PA2, and showed that plaintext simulatability notion was strictly stronger than the random oracle PA2. Therefore, our result can be recognized as the standard model variant of Fujisaki's result [F06]. By comparing his result with our result, we can say that statistical and computational standard model PA2 notions are related to the random oracle PA2 and the PS, respectively.

We stress that, although our result and Fujisaki's result themselves are similar, these are of different model with different proof. Indeed we cannot use his proof because it highly depends on the random oracle model. Our proof is simpler and more intuitive than his.

1.2 Previous Works

Before the random oracle PA2 was defined, a weaker variant of it, named the random oracle *PA1* [BR94], had been defined. The first schemes satisfying the random oracle PA1 and PA2 were proposed in the paper of Bellare-Rogaway [BR94] and Fujisaki-Okamoto [FO99] respectively. In these papers, the authors proposed conversions which transform a trapdoor oneway permutation and an IND-CPA secure public-key encryption scheme to PA1 and PA2 secure public-key encryption scheme respectively. These conversions are called the OAEP and the Fujisaki-Okamoto conversions respectively.

Shoup [S01] showed that the random oracle PA1 + IND-CPA does not imply the IND-CCA2 security, although previously it had been thought that it did. In his paper, he also gave a revised version of the OAEP conversion, named the OAEP+, which transforms a trapdoor oneway permutation to a PA2 secure public-key encryption scheme on the random oracle model. The OAEP and other conversions satisfying a similar property are also studied in [CHJPPT98,B01,FOPS01,M01,OP01,CJNP02,KI01,KO03].

As far as we know, the first attempt to define the plaintext awareness not in the random oracle model was made by Herzog, Liskov, and Micali [HLM03]. They defined the PA2 notion on the key registration model [HLM03] and constructed a public-key encryption scheme which satisfies their PA2.

Bellare and Palacio [BP04] define not only the standard model PA2 but also the standard model PA1. They also showed that the Damgård [D91] and the lite Cramer-Shoup [CS01] public-key encryption schemes satisfy the standard model PA1 under the Diffie-Hellman Knowledge assumption [D91,BP04] and the DDH assumption. Later, Dent [D06] showed that the Cramer-Shoup public-key encryption scheme [CS98,CS01] satisfies the standard model PA2 security under the same assumption.

1.3 Organization

The paper is organized as follows: In Section 2, we review the definition of the standard model PA2. In Section 3, we show that the statistical PA2 is strictly stronger than the computational one. In Section 4, we show the main theorem, which states that "(perfect, statistical, or computational) PA2 + Oneway $\Rightarrow$ IND-CPA". Finally, in Section 5, we give the conclusion of our paper.

2 Definition of Standard Model PA2

In this section, we review the definition of the standard model PA2 [BP04]. Before giving the formal definition of the standard model PA2, we give intuitive explanation about it. The definition of the standard model PA2 is based on the indistinguishability of two worlds, named *Dec world* and *Ext world*, and uses entities named *adversary* and *extractor*. In the Dec world, the adversary can access to the decryption oracle and the encryption oracle. In contrast, the adversary in the Ext world can access to the extractor and the encryption oracle. The extractor has to simulate the decryption oracle by using only data "which the adversary can see", that is, the adversary's description, its random tape, and the answers from the encryption oracle.

It is a characteristic feature for the definition that it has a mechanism to hide the encryption query of the adversary from the extractor. In order to hide the encryption query, the entity, named *plaintext creator*, is also introduced. It is an entity which makes encryption queries as the adversary's proxy. The adversary, in both Dec and Ext worlds, does not make encryption queries directly but sends an order to the plaintext creator, in order to make it send a query to the encryption oracle.

The extractor is not allowed to watch the plaintext creator's random tape, although it is allowed to watch the adversary's one. Hence it cannot know what queries are made to the encryption oracle. We say that an encryption scheme satisfies the standard model PA2, if the Dec and Ext worlds are indistinguishable for the adversary from each other.

We now define the standard model PA2 formally:

Definition 1 (Standard Model PA2 [BP04]) Let $\mathit{\Pi} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme. Let $\mathcal{A}$, $\mathcal{P}$, $\mathcal{K}$ be polytime machines, which are respectively called *adversary*, *plaintext creator*, and *extractor*. Let $\mathcal{A}(\mathsf{pk}; R_{\mathcal{A}})$ denotes the execution of an algorithm $\mathcal{A}$ on inputting pk with the random coin $R_{\mathcal{A}}$. For a security parameter $\kappa \in \mathbb{N}$, we define two experiments $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\mathit{\Pi},\mathcal{A},\mathcal{P}}(\kappa)$ and $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\mathit{\Pi},\mathcal{A},\mathcal{K},\mathcal{P}}(\kappa)$, shown in Fig. 1. In these experiments, it is required that $\mathcal{A}$ makes no query (dec, C) for which $C \in \mathsf{CList}$.

We say that the public-key encryption scheme $\mathit{\Pi}$ is *perfectly/statistically/computationally standard model PA2* secure if

$$^{\forall}\mathcal{A}^{\exists}\mathcal{K}^{\forall}\mathcal{P} : \mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\mathit{\Pi},\mathcal{A},\mathcal{P}}(\kappa) \text{ and } \mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\mathit{\Pi},\mathcal{A},\mathcal{K},\mathcal{P}}(\kappa) \text{ are}$$
$$\text{perfectly/statistically/computationally indistinguishable for } \kappa.$$

Since we only discuss about the standard model PA2, we simply say that $\mathit{\Pi}$ is *perfectly/statistically/computationally PA2* secure if it is perfectly/statistically/computationally standard model PA2 secure.

Theorem 2 (Fundamental Theorem for Standard Model PA2 [BP04]). *Let $\mathit{\Pi}$ be an IND-CPA secure public-key encryption scheme. If $\mathit{\Pi}$ is (perfect, statistical, or computational) PA2 secure, then $\mathit{\Pi}$ is IND-CCA2 secure.*

```
—$\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A},\mathcal{P}}(\kappa)$—
Take coins $R_{\mathcal{A}}$ and $R_{\mathcal{P}}$ for $\mathcal{A}$ and $\mathcal{P}$ randomly.
$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$, $\mathsf{CList} \leftarrow \varepsilon$, $\mathsf{St}_{\mathcal{P}} \leftarrow \varepsilon$. (Here $\mathsf{St}_{\mathcal{P}}$ is the state of $\mathcal{P}$).
Run $\mathcal{A}(\mathsf{pk};R_{\mathcal{A}})$ until it halts, replying to its oracle queries as follows:
  If $\mathcal{A}$ makes query $(\mathsf{enc},Q)$
    $(M,\mathsf{St}_{\mathcal{P}}) \leftarrow \mathcal{P}(Q,\mathsf{St}_{\mathcal{P}};R_{\mathcal{P}})$, $C \leftarrow \mathsf{Enc}_{\mathsf{pk}}(M)$, $\mathsf{CList} \leftarrow \mathsf{CList}||C$.
    Send $C$ to $\mathcal{A}$ as the reply.
  If $\mathcal{A}$ makes query $(\mathsf{dec},Q)$
    $M \leftarrow \mathsf{Dec}_{\mathsf{sk}}(Q)$. Send $M$ to $\mathcal{A}$ as the reply.
Return an output $S$ of $\mathcal{A}$.
```

```
—$\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A},\mathcal{K},\mathcal{P}}(\kappa)$—
Take coins $R_{\mathcal{A}}$, $R_{\mathcal{P}}$, and $R_{\mathcal{K}}$ for $\mathcal{A}$, $\mathcal{P}$, and $\mathcal{K}$ randomly.
$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$, $\mathsf{CList} \leftarrow \varepsilon$, $\mathsf{St}_{\mathcal{P}} \leftarrow \varepsilon$, $\mathsf{St}_{\mathcal{K}} \leftarrow (\mathsf{pk},R_{\mathcal{A}})$.
    (Here $\mathsf{St}_{\mathcal{P}}$ and $\mathsf{St}_{\mathcal{K}}$ are the states of $\mathcal{P}$ and $\mathcal{K}$).
Run $\mathcal{A}(\mathsf{pk};R_{\mathcal{A}})$ until it halts, replying to its oracle queries as follows:
  If $\mathcal{A}$ makes query $(\mathsf{enc},Q)$
    $(M,\mathsf{St}_{\mathcal{P}}) \leftarrow \mathcal{P}(Q,\mathsf{St}_{\mathcal{P}};R_{\mathcal{P}})$, $C \leftarrow \mathsf{Enc}_{\mathsf{pk}}(M)$, $\mathsf{CList} \leftarrow \mathsf{CList}||C$.
    Send $C$ to $\mathcal{A}$ as the reply.
  If $\mathcal{A}$ makes query $(\mathsf{dec},Q)$
    $(M,\mathsf{St}_{\mathcal{K}}) \leftarrow \mathcal{K}(Q,\mathsf{CList},\mathsf{St}_{\mathcal{K}};R_{\mathcal{K}})$. Send $M$ to $\mathcal{A}$ as the reply.
Return an output $S$ of $\mathcal{A}$.
```

Fig. 1. Experiments used to define PA2 of [BP04]

3 Statistical PA2 is Stronger than Computational PA2

In this section, we show that the computational PA2 security is strictly stronger than the statistical one. That is, we give an example of a computational PA2 secure public-key encryption scheme $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ which is not statistical PA2 secure.

Let κ be a security parameter. Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme which is statistical PA2 secure and IND-CPA secure (and therefore IND-CCA2 secure). For instance, we can set Π to the Cramer-Shoup scheme [CS01], if the Diffie-Hellman Knowledge assumption [D91,BP04] and the DDH assumption holds. We construct the desired public-key encryption scheme $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ by modifying Π. The key generation algorithm $\mathsf{Gen}'(1^\kappa)$ first executes $\mathsf{Gen}(1^\kappa)$ and obtains a public key/secret key pair $(\mathsf{pk}, \mathsf{sk})$ as the output. After that, it selects a message M_0 randomly and computes a ciphertext $C_0 = \mathsf{Enc}_{\mathsf{pk}}(M_0)$. Then it sets $\mathsf{pk}' = (\mathsf{pk}, C_0)$ and $\mathsf{sk}' = \mathsf{sk}$. Finally, it outputs the public key/secret key pair $(\mathsf{pk}', \mathsf{sk}')$. We also set $\mathsf{Enc}'_{\mathsf{pk}'}(M) = \mathsf{Enc}_{\mathsf{pk}}(M)$ and $\mathsf{Dec}'_{\mathsf{sk}'}(C) = \mathsf{Dec}_{\mathsf{sk}}(C)$. See Fig. 2 also for the description of Π'.

We first see that Π' is not statistical PA2 secure. In order to see it, we construct an adversary $\mathcal{A}'_0$ such that no extractor can extract a message from the ciphertext output by $\mathcal{A}'_0$. Our adversary $\mathcal{A}'_0$ is the one who obtains C_0 from its input $\mathsf{pk}' = (\mathsf{pk}, C_0)$ and outputs C_0. Recall that not $\mathcal{A}'_0$ but the key generation algorithm Gen' generates M_0 and C_0. Therefore, $\mathcal{A}'_0$ "does not know" the message

```
$\mathsf{Gen}'(1^\kappa)$:
    $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$
    Select a message $M_0$ randomly.
    $C_0 \leftarrow \mathsf{Enc}_{\mathsf{pk}}(M_0)$.
    $\mathsf{pk}' \leftarrow (\mathsf{pk}, C_0)$, $\mathsf{sk}' \leftarrow \mathsf{sk}$.
    Output $(\mathsf{pk}', \mathsf{sk}')$.

$\mathsf{Enc}'_{\mathsf{pk}'}(M) = \mathsf{Enc}_{\mathsf{pk}}(M)$, $\mathsf{Dec}'_{\mathsf{sk}'}(C) = \mathsf{Dec}_{\mathsf{sk}}(C)$.
$\mathcal{A}'_0(\mathsf{pk}')$:
    Parse $\mathsf{pk}'$ as $(\mathsf{pk}, C_0)$ and output $C_0$.
```

Fig. 2. Descriptions of $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ and $\mathcal{A}'_0$.

M_0 corresponding to C_0. Since an extractor $\mathcal{K}'$ is input only data which the adversary can see, $\mathcal{K}'$ "cannot know" $M_0 = \mathsf{Dec}'_{\mathsf{sk}'}(C_0) = \mathsf{Dec}_{\mathsf{sk}}(C_0)$ either. This means that Π' is not statistical PA2 secure.

However, we can show that Π' is the computational PA2 secure. At first glance, it seems that Π' cannot be computational PA2 secure either, because even an extractor $\mathcal{K}'$ for the computational PA2 "cannot know" $M_0 = \mathsf{Dec}'_{\mathsf{sk}'}(C_0)$ either. However, we actually do not require the extractor who "can know" such M_0. Recall that the extractor $\mathcal{K}'$ is only required to simulate the decryption oracle in such a way that an adversary $\mathcal{A}'_0$ cannot *computationally* distinguish the output of $\mathcal{K}'$ from that of decryption oracle. Therefore, $\mathcal{K}'$ does not need to output the plaintext M_0 itself, but can output the plaintext M_1 such that $\mathcal{A}'_0$ cannot computationally distinguish the distribution of M_1 from that of M_0.

Recall that $\mathcal{A}'_0$ "knows" neither the plaintext M_0 nor the random number r which was used in the computation of $C_0 = \mathsf{Enc}_{\mathsf{pk}}(M_0; r)$. Recall also that Π satisfies the IND-CCA2 security. Hence, $\mathcal{A}'_0$ cannot distinguish a randomly selected message M_1 from M_0. Therefore, $\mathcal{K}'$ can output a randomly selected message M_1 as the answer to the decryption query C_0.

Based on the above discussion, we can prove the following theorem.

Theorem 3. *Suppose that there exists at least one computational PA2 secure public-key encryption scheme. (For instance, if the Cramer-Shoup scheme [CS01] satisfies it under the DDH assumption and the Diffie-Hellman Knowledge assumption [D91,BP04]). Then there exists a computational PA2 secure public-key encryption which is not statistical PA2 secure.*

It is interesting to compare our result with Fujisaki's result [F06] about the random oracle PA2. In his paper, he defined a *plaintext simulatability* (PS) notion, which was an "computational variant" of the random oracle PA2, and showed that plaintext simulatability notion was strictly stronger than the random oracle PA2. Therefore, our result can be recognized as the standard model variant of Fujisaki's result [F06]. By comparing his result with our result, we can say that statistical and computational standard model PA2 notions is related to the random oracle PA2 and the PS, respectively.

4 PA2-04 together with Onewayness Implies IND-CPA

Our main result is the following:

Theorem 4. *Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme, which satisfies the onewayness property. If Π is perfectly, statistically, or computationally PA2 secure, then Π is IND-CPA secure, (and therefore IND-CCA2 secure).*

This result shows the "all-or-nothing" aspect of the PA2. That is, the (perfect, statistical, or computational) PA2 secure encryption scheme either satisfies the strongest message hiding property, IND-CCA2, or does not satisfy even the weakest message hiding property, onewayness.

Before proving Theorem 4, we see that one cannot remove the onewayness assumption from Theorem 4:

Theorem 5. *There is a public-key encryption which is perfect PA2 secure but is neither oneway nor IND-CPA secure.*

Proof (Theorem 5, sketch). Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme, such that an encryption $\mathsf{Enc}_{\mathsf{pk}}(M)$ of a message M is M itself. Then Π is clearly not IND-CPA secure. Recall the definition of the statistical PA2. We say that Π satisfies the statistical PA2 security if, for any adversary $\mathcal{A}$, there exists an extractor $\mathcal{K}$ such that $\mathcal{K}$ succeeds in extracting the plaintext M which corresponds to a ciphertext C output by $\mathcal{A}$. Since $\mathcal{K}$ can know the message M directly from the ciphertext itself, Π satisfies the perfect PA2.

We first prove Theorem 4 for the special case where Π is statistically PA2 secure. Theorem 4 for the perfect PA2 security is clearly followed from it.

Proof (Theorem 4 for the statistical PA2, sketch). Let us make a contradictory supposition. That is, we suppose that there exists a statistically PA2 secure public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ which is not IND-CPA secure. Then we show that Π is not oneway.

In order to show it, we construct an adversary $\mathcal{A}_0$ which satisfies the following tricky property: $\mathcal{A}_0$ can obtain a ciphertext C_0 such that (1) $\mathcal{A}_0$ "does not know" the plaintext $M_0 = \mathsf{Dec}_{\mathsf{sk}}(C_0)$ and (2) C_0 is not generated by the encryption oracle. For a moment, suppose that we succeed in constructing such $\mathcal{A}_0$. Since C_0 is not generated by the encryption oracle, $\mathcal{A}_0$ can make the query C_0 to the decryption oracle. Then, from the definition of the plaintext awareness, there exists an extractor $\mathcal{K}$ which can extract the plaintext M_0 from the query C_0 of $\mathcal{A}_0$. (Here we exploit the supposition that Π is statistically PA2 secure). This means that $\mathcal{K}$ succeeds in outputting the unknown plaintext M_0 of a ciphertext C_0. That is, $\mathcal{K}$ can invert the encryption function Enc. This contradicts to the assumption that Π is oneway.

We next describe how to construct $\mathcal{A}_0$. At first glance, it seems impossible to construct such $\mathcal{A}_0$, since the definition of the plaintext awareness disable $\mathcal{A}_0$ generating a ciphertext C_0 "without knowing" the corresponding plaintext M_0.

The basic idea how $\mathcal{A}_0$ obtains such ciphertext C_0 is similar to that used in Section 3. In Section 3, the adversary obtains such C_0 from the key generation algorithm. In this proof, $\mathcal{A}_0$ obtains such C_0 from another entity, that is, a plaintext creator $\mathcal{P}_0$. Then $\mathcal{A}_0$ "does not know" the message M_0 corresponding to C_0, since not $\mathcal{A}_0$ itself but $\mathcal{P}_0$ generates C_0. (We stress that not the encryption oracle but $\mathcal{P}_0$ itself generates C_0. If the encryption oracle generates C_0, $\mathcal{A}_0$ cannot send C_0 to the decryption oracle).

In order to employ the technique mentioned above, $\mathcal{P}_0$ has to send C_0 to $\mathcal{A}_0$. However, there is no inherent communication channel which enables $\mathcal{P}_0$ to send C_0 directly to $\mathcal{A}_0$. So, we construct a "virtual" communication channel from $\mathcal{P}_0$ to $\mathcal{A}_0$.

Here we exploit the assumption that the public-key encryption scheme Π is not IND-CPA secure. Recall that the definition of the statistical PA2 security allows $\mathcal{P}_0$ to send plaintexts to the encryption oracle. Therefore, $\mathcal{P}_0$ can send to $\mathcal{A}_0$ a ciphertext c such that $\mathcal{P}_0$ generates the corresponding plaintext. Since Π is not IND-CPA secure, the ciphertext c leaks information of the corresponding plaintext. This means that $\mathcal{P}_0$ can send to $\mathcal{A}_0$ some sort of information via the ciphertext c. That is, $\mathcal{P}_0$ can use the ciphertext as the virtual channel.

We now describe more precisely how $\mathcal{P}_0$ "sends" C_0 to $\mathcal{A}_0$. Let pk_0 be a public key and sk_0 be the unknown secret key corresponding to pk_0. Since Π is not IND-CPA secure, there exist an algorithm $\mathcal{B}$, a state $\mathsf{St}_\mathcal{B}$ of $\mathcal{B}$, a pair of messages (m_0, m_1), and a non negligible and non negative valued function $\mu = \mu(\kappa)$ satisfying

$$\Pr(\mathcal{B}(\mathsf{pk}_0, m_0, m_1, \mathsf{Enc}_{\mathsf{pk}_0}(m_1), \mathsf{St}_\mathcal{B}) = 1) - \Pr(\mathcal{B}(\mathsf{pk}_0, m_0, m_1, \mathsf{Enc}_{\mathsf{pk}_0}(m_0), \mathsf{St}_\mathcal{B}) = 1) \geq \mu.$$

We set N to $\lceil 1/\mu \rceil$. Let b_i be the i-th bit of the ciphertext $C_0 = \mathsf{Enc}_{\mathsf{pk}_0}(M_0)$ such that M_0 is unknown. In advance, $\mathcal{A}_0$ sends $\mathsf{pk}_0||m_0||m_1||N$ to $\mathcal{P}_0$, via the communication channel which enables $\mathcal{A}_0$ to query. For each i, $\mathcal{P}_0$ sends a message m_{b_i} as a query to the encryption oracle N times. Then the encryption oracle sends $c_1^{(i)} = \mathsf{Enc}_{\mathsf{pk}_0}(m_{b_i}), \ldots, c_N^{(i)} = \mathsf{Enc}_{\mathsf{pk}_0}(m_{b_i})$ to $\mathcal{A}_0$ as the answers. After receiving $\{c_j^{(i)}\}$, $\mathcal{A}_0$ executes $\mathcal{B}(\mathsf{pk}_0, m_0, m_1, c_j^{(i)}, \mathsf{St}_\mathcal{B})$ and obtains an output $u_j^{(i)}$ of $\mathcal{B}$ for each i and j. Then $\mathcal{A}_0$ sets $b'_i = 1$ if the number of j satisfying $u_j^{(i)} = 1$ is more than the number of j satisfying $u_j^{(i)} = 0$. Otherwise $\mathcal{A}_0$ sets $b'_i = 0$. Since $\mathcal{B}$ has a non negligible advantage, the equality $u_j^{(i)} = b_i$ is satisfied with probability $1/2 +$ (non negligible). Hence the equation $b'_i = b_i$ is satisfied with overwhelming probability. That is, $\mathcal{A}_0$ succeeds in reconstructing the bit b_i of the ciphertext C_0 for each i. Therefore, $\mathcal{A}_0$ can reconstruct the ciphertext $C_0 = b_1|| \cdots ||b_n$. In this way, $\mathcal{A}_0$ succeeds in "receiving" C_0 from $\mathcal{P}_0$.□

We now give the proof for the general case where Π satisfies only the computational PA2 security.

Proof (Theorem 4 for the computational PA2, sketch). As in the case of the proof of for statistical PA2, we suppose that there exists a computationally PA2 secure public-key encryption scheme Π which is not IND-CPA secure. Then we show that Π is not oneway.

We use similar algorithms to $\mathcal{A}_0$ and $\mathcal{P}_0$ of the proof for the statistical PA2. However, in the case of Π is computational PA2, the extractor $\mathcal{K}$ may output a plaintext M' which is not equal to the plaintext $M_0 = \mathsf{Dec}_{\mathsf{sk}_0}(C_0)$, although the distribution of M' has to be computationally indistinguishable from that of M_0. Therefore, in order to obtain M_0, we modify the description of $\mathcal{A}_0$ and $\mathcal{P}_0$.

We will first construct an adversary $\mathcal{A}_1$ by modifying $\mathcal{A}_0$. Then, for some extractor $\mathcal{K}$, $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}'}(\kappa)$ is computationally indistinguishable from $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}'}(\kappa)$ for any $\mathcal{P}'$. Then, by modifying $\mathcal{P}_0$, we will construct a plaintext creator $\mathcal{P}_1$ such that $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ is, in fact, *statistically* indistinguishable from $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$, although we cannot exploit $\mathcal{P}_1$ itself to obtain the secret plaintext M_0. We will finally construct a plaintext creator $\mathcal{P}_2$, by modifying $\mathcal{P}_1$, such that $\mathcal{P}_2$ can be exploited to obtain M_0.

We will now give a brief description of $\mathcal{A}_1$ and $\mathcal{P}_1$ by describing the experiment $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$. (We stress that we first choose $\mathcal{A}_1$, next obtain $\mathcal{K}$, and finally choose $\mathcal{P}_1$, although we first describe about $\mathcal{A}_1$ and $\mathcal{P}_1$, and next describe $\mathcal{K}$. One can easily check that we can take $\mathcal{K}$ which does not depend on $\mathcal{P}_1$). In the experiment $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$, the experimenter first executes the key generation algorithm $\mathsf{Gen}(1^\kappa)$ and obtains a public key/secret key pair $(\mathsf{pk}, \mathsf{sk})$ as an output. Then he inputs pk to the adversary $\mathcal{A}_1$, the encryption oracle, and the decryption oracle. He also inputs sk to the decryption oracle. Then $\mathcal{A}_1$ executes $\mathcal{B}(\mathsf{pk})$ and obtains $(m_0, m_1, \mathsf{St}_\mathcal{B})$ as an output. After that, $\mathcal{A}_1$ sends $\mathsf{pk}||m_0||m_1||N$ to $\mathcal{P}_1$, via the communication channel which enables $\mathcal{A}_1$ to query. Here $N = \lceil 1/\mu \rceil$.

Then $\mathcal{P}_1$ generates a message M_1 randomly, and computes a ciphertext $C_1 = \mathsf{Enc}_{\mathsf{pk}}(M_1)$. After that, $\mathcal{A}_1$ and $\mathcal{P}_1$ execute the same procedures as those of $\mathcal{A}_0$ and $\mathcal{P}_0$ except that they execute these procedures using not C_0 but C_1. That is, $\mathcal{P}_1$ "sends" C_1 to $\mathcal{A}_1$ via the "virtual" channel. After "receiving" C_1 from $\mathcal{P}_1$, $\mathcal{A}_1$ makes query C_1 to the decryption oracle. Then the decryption oracle sends back a message M' to $\mathcal{A}_1$ as the answer to the query C_1. (Note that the decryption oracle sends back a message $M' = M_1 = \mathsf{Dec}_{\mathsf{sk}}(C_1)$, although an extractor $\mathcal{K}$ may send back a message M' other than M_1).

After that, $\mathcal{A}_1$ sends M' to $\mathcal{P}_1$ via the communication channel which enables $\mathcal{A}_1$ to query. $\mathcal{P}_1$ checks whether $M_1 = M'$ or not. Then $\mathcal{P}_1$ sets $S = 1$ if $M_1 = M'$, otherwise sets $S = 0$. After that, $\mathcal{P}_1$ "sends" S to $\mathcal{A}_1$ via the "virtual" channel. Finally, $\mathcal{A}_1$ outputs S.

Then, for some extractor $\mathcal{K}$, $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}'}(\kappa)$ is computationally indistinguishable from $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}'}(\kappa)$ for any $\mathcal{P}'$. In particular, $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ is computationally indistinguishable from $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$.

We show that $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ is, in fact, *statistically* indistinguishable from $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$. In the case where $\mathcal{A}_1$ and $\mathcal{P}_1$ are in the real experiment $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$, the output S of $\mathcal{A}_1$ is always 1. Recall that $\mathcal{A}_1$ cannot computationally distinguish $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ from $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$. Therefore, even in the experiment $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$, $S = 1$ is satisfied with overwhelming probability. Recall that $S = 1$ holds if and only if $M' = M$. Hence, $\mathcal{K}$ succeeds in outputting the correct message M corresponding to $C'_1 = C_1 = \mathsf{Enc}_{\mathsf{pk}}(M)$ with overwhelming probability. This means that $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ is statistically indistinguishable from $\mathbf{Exp}^{\mathsf{PA2\text{-}Dec}}_{\Pi,\mathcal{A}_1,\mathcal{P}_1}(\kappa)$.

We next construct a plaintext creator $\mathcal{P}_2$, by modifying $\mathcal{P}_1$. Let (pk_0, C_0) be an instance of the onewayness game, and sk_0 be the unknown secret key corresponding to pk_0. Our goal is to compute $M_0 = \mathsf{Dec}_{\mathsf{sk}_0}(C_0)$. The description of $\mathcal{P}_2$ is equal to that of $\mathcal{P}_1$, except that (1) $\mathcal{P}_2$ takes C_0 as an input, (2) $\mathcal{P}_2$ does not use a ciphertext C_1 generated by $\mathcal{P}_2$ itself but instead uses a part C_0 of the instance (pk_0, C_0) of the onewayness game, and (3) $\mathcal{P}_2$ always sets $S = 1$.

We consider a modified version of the experiment $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa)$, named $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa,\ \mathsf{pk}_0,\ C_0)$, in which the experimenter uses not the public key pk generated by $\mathsf{Gen}(1^\kappa)$ but instead uses a part pk_0 of the instance (pk_0, C_0) of the onewayness game. Recall that both $\mathcal{P}_1$ in $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ and $\mathcal{P}_2$ in $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa, \mathsf{pk}_0, C_0)$ set $S = 1$ with overwhelming probability. Moreover, the distribution of (pk_0, C_0) is equal to that of (pk, C) selected randomly. Hence, the behavior of $\mathcal{P}_1$ in $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$ is statistically indistinguishable from that of $\mathcal{P}_2$ in $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa, \mathsf{pk}_0, C_0)$. (Recall that $\mathcal{K}$ is not input the random coin of a plaintext creator. Therefore, $\mathcal{K}$ cannot distinguish the behavior of $\mathcal{P}_1$ from that of $\mathcal{P}_2$).

Therefore, the distribution of the output of $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa, \mathsf{pk}_0, C_0)$ is statistically indistinguishable from that of the output of $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$. Recall that, in the experiment $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_1}(\kappa)$, the output M' of $\mathcal{K}$ is equal to $M_1 = \mathsf{Dec}_{\mathsf{sk}_0}(C_1)$ with overwhelming probability. Therefore, even in the experiment $\mathbf{Exp}^{\mathsf{PA2\text{-}Ext*}}_{\Pi,\mathcal{A}_1,\mathcal{K},\mathcal{P}_2}(\kappa, \mathsf{pk}_0, C_0)$, the output M' of $\mathcal{K}$ is equal to $M_0 = \mathsf{Dec}_{\mathsf{sk}_0}(C_0)$ with overwhelming probability. This means that $\mathcal{K}$ succeeds in obtaining the unknown plaintext $M_0 = \mathsf{Dec}_{\mathsf{sk}_0}(C_0)$ with overwhelming probability. □

We see that Theorem 4 does not hold in the case of the random oracle PA2. See Appendix A for the definition of the random oracle PA2.[1]

Proposition 6 *Suppose that there exists a group $\mathcal{G}$ on which the DDH problem is easy although the CDH problem is hard. (For instance, we can set $\mathcal{G}$ to an elliptic curve group on which a bilinear pairing [BF01,MOV93,JN03,SOK01] is defined). Then there exists a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ which satisfies the random oracle PA2 security and the onewayness but does not satisfy the IND-CPA security.*

Proof (sketch). The desired encryption scheme is the Fujisaki-Okamoto [FO99] padded ElGamal encryption scheme such that a message and elements g and h of a public key (g, h) are taken from the above $\mathcal{G}$. Similar to the case of the original

[1] The definition of the random oracle PA2 differ subtly depending on papers. Our definitions are those of [BR94,FOPS01]. In some papers, such as [BDPR98,F06], the authors say that a public-key encryption scheme satisfies the random oracle PA2, if it satisfies both our definition and the IND-CPA security.

Fujisaki-Okamoto padded ElGamal encryption scheme, we can prove that the encryption scheme satisfies the random oracle model PA2 security. Moreover, it satisfies onewayness since the CDH problem is hard on $\mathcal{G}$. However, it does not satisfy the IND-CPA security since the DDH problem on $\mathcal{G}$ is easy. $\Box$

By applying the similar idea to the Damgård scheme [D91], one can also show that there exists a public-key encryption scheme which satisfies the standard model PA1 security [BP04] and the onewayness but does not satisfy the IND-CPA security. See Appendix A for the definition of the standard model PA1.

5 Conclusion

In this paper, we studied the relationship between the standard model PA2 and the property about message hiding, that is, IND-CPA. Although it seems that these two are independent notions at first glance, we showed that all of the perfect, statistical, and computational PA2 in the standard model imply the IND-CPA security if the encryption function is oneway. This result combining with the fundamental theorem implies the stronger variant of the fundamental theorem, "(perfect, statistical or computational) PA2 + Oneway $\Rightarrow$ IND-CCA2". It shows the "all-or-nothing" aspect of the PA2. That is, a (perfect, statistical, or computational) PA2 secure public-key encryption scheme either satisfies the strongest message hiding property, IND-CCA2, or does not satisfy even the weakest message hiding property, onewayness.

We also showed that the computational PA2 notion is strictly stronger than the statistical one. By comparing Fujisaki's result [F06] with our result, we can say that statistical and computational standard model PA2 notions is related to the random oracle PA2 and the plaintext simulatability [F06], respectively.

Acknowledgements

We thank anonymous reviewers for helpful comments.

References

[BDPR98] Mihir Bellare, Anand Desai, David Pointcheval, Phillip Rogaway. Relations Among Notions of Security for Public-Key Encryption Schemes. CRYPTO 1998, pp.26-45.

[BP04] Mihir Bellare, Adriana Palacio. Towards plaintext-aware public-key encryption without random oracles. ASIACRYPT 2004, pp. 48-62.

[BR94] Mihir Bellare, Phillip Rogaway. Optimal Asymmetric Encryption. EUROCRYPT 1994, pp.92-111.

[BR96] Mihir Bellare, Phillip Rogaway. The Exact Security of Digital Signatures: How to Sign with RSA and Rabin. EUROCRYPT 1996, pp.399-416.

[B01] Dan Boneh. Simplified OAEP for the RSA and Rabin Functions. CRYPTO 2001, pp.275-291.

[BF01] Dan Boneh, Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. CRYPTO 2001, pp.213-229.

[CHJPPT98] Jean-Se'bastien Coron, Helena Handschuh, Marc Joye, Pascal Paillier, David Pointcheval, Christophe Tymen. Optimal Chosen-Ciphertext Secure Encryption of Arbitrary-Length Messages. PKC 2002, pp. 17-33.

[CJNP02] Jean-Se'bastien Coron, Marc Joye, David Naccache, Pascal Paillier. Universal Padding Schemes for RSA. CRYPTO 2002, pp. 226-241.

[CS98] Ronald Cramer, Victor Shoup. A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack. CRYPTO 1998, pp.13-25.

[CS01] Ronald Cramer, Victor Shoup. Design and Analysis of Practical Public-Key Encryption Schemes. manuscript, 2001. Full version: SIAM J. Comp. 2004, 33(1), pp.167-226.

[D91] Ivan Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In CRYPTO'91, pp.445-456.

[D06] Alexander W. Dent. Cramer-Shoup is Plaintext-Aware in the Standard Model. EUROCRYPT 2006.

[DDN00] Danny Dolev, Cynthia Dwork, Moni Naor. Nonmalleable Cryptography. SIAM J. Comp. 2000, 30(2), pp. 391-437.

[DY83] Danny Dolev, Andrew Chi-Chih Yao. On the security of public key protocols. IEEE Transactions on Information Theory, 1983, 29(2) pp.198-207.

[F06] Eiichiro Fujisaki. Plaintext Simulatability. IEICE Trans. Fundamentals 2006, E89-A, pp.55-65, doi:10.1093/ietfec/e89-a.1.55. Preliminary version is available at http://eprint.iacr.org/2004/ 218.pdf

[FO99] Eiichiro Fujisaki, Tatsuaki Okamoto. How to Enhance the Security of Public-Key Encryption at Minimum Cost. PKC'99, pp. 53-68.

[FOPS01] Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, Jacques Stern. RSA-OAEP Is Secure under the RSA Assumption. CRYPTO 2001, pp.260-274. J. Cryptology 2004, 17(2), pp.81-104.

[HLM03] Jonathan Herzog, Moses Liskov, Silvio Micali. Plaintext Awareness via Key Registration. CRYPTO 2003, pp.548-564

[JN03] Antoine Joux, Kim Nguyen. Separating Decision Diffie-Hellman from Computational Diffie-Hellman in Cryptographic Groups. J. Cryptology, 2003,16(4), pp.239-247. http://eprint.iacr.org/2001/003

[KI01] Kazukuni Kobara, Hideki Imai. Semantically Secure McEliece Public-Key Cryptosystems-Conversions for McEliece PKC. In PKC 2001, pp. 19-35.

[KO03] Yuichi Komano, Kazuo Ohta. Efficient Universal Padding Techniques for Multiplicative Trapdoor One-Way Permutation. CRYPTO 2003, pp. 366-382.

[M01] James Manger. A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1 v2.0. CRYPTO 2001, pp.230-238.

[MOV93] Alfred Menezes, Tatsuaki Okamoto, Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. on Information Theory 1993, 39(5), pp.1639-1646.

[OP01] Tatsuaki Okamoto, David Pointcheval. REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. CT-RSA 2001, pp.159-175.

[PP04] Duong Hieu Phan, David Pointcheval. OAEP 3-Round: A Generic and Secure Asymmetric Encryption Padding. In Asiacrypt 2004. pp. 63-77.

[SOK01] Ryuichi Sakai, Kiyoshi Ohgishi, Masao Kasahara. Cryptosystems Based on Pairings. SCIS 2001.

[S00] Victor Shoup. Using Hash Functions as a Hedge against Chosen Ciphertext Attack. EUROCRYPT 2000, pp.275-288.

[S01] Victor Shoup. OAEP Reconsidered. CRYPTO 2001, pp.239-259. J. Cryptology, 2002, 15(4), pp. 223-249.

A Definitions

A.1 Security Definitions of an Encryption Scheme

Definition 7 (IND-CPA/CCA1/CCA2) Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme and κ be a security parameter. For a public key/secret key pair $(\mathsf{pk}, \mathsf{sk})$ for Π, we let $\mathcal{O}_{\mathsf{dec}}(\mathsf{sk}, \cdot)$ be the oracle (named *decryption oracle*) such that it returns $\mathsf{Dec}_{\mathsf{sk}}(C)$ to an adversary when the adversary sends a ciphertext C to it. Let b be a bit. We also let $\mathcal{O}_{\mathsf{enc}}(b, \mathsf{pk}, \cdot)$ be the oracle (named *encryption oracle*) such that it returns $\mathsf{Enc}_{\mathsf{pk}}(M_b)$ to an adversary when the adversary sends a pair (M_0, M_1) of messages with the same length to it. We call $\mathsf{Enc}_{\mathsf{pk}}(M_b)$ the *challenge ciphertext*.

For a bit b and a polytime adversary $\mathcal{A}$, we set

$$\mathbf{P}^{(b)}_{\Pi,\mathcal{A}}(\kappa) = \Pr((\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa), b' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{enc}}(b,\mathsf{pk},\cdot),\mathcal{O}_{\mathsf{dec}}(\mathsf{sk},\cdot)}(\mathsf{pk}) : b' = 1),$$

and $\mathbf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{A}}(\kappa) = |\mathbf{P}^{(1)}_{\Pi,\mathcal{A}}(\kappa) - \mathbf{P}^{(0)}_{\Pi,\mathcal{A}}(\kappa)|$.

Above, $\mathcal{A}$ can make a query to $\mathcal{O}_{\mathsf{enc}}(b, \mathsf{pk}, \cdot)$ only once. Moreover, $\mathcal{A}$ is not allowed to send the challenge ciphertext to $\mathcal{O}_{\mathsf{dec}}(\mathsf{sk}, \cdot)$.

We say that Π is *IND-CPA secure* if $\mathbf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{A}}(\kappa)$ is negligible for any polytime adversary $\mathcal{A}$ such that $\mathcal{A}$ has made no query to $\mathcal{O}_{\mathsf{dec}}(\mathsf{sk}, \cdot)$. We say that Π is *IND-CCA1 secure* if $\mathbf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{A}}(\kappa)$ is negligible for any polytime adversary $\mathcal{A}$ such that $\mathcal{A}$ has made no query to $\mathcal{O}_{\mathsf{dec}}(\mathsf{sk}, \cdot)$ after receiving the challenge ciphertext from $\mathcal{O}_{\mathsf{enc}}(b, \mathsf{pk}, \cdot)$. We also say that Π is *IND-CCA2 secure* if $\mathbf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{A}}(\kappa)$ is negligible for any polytime adversary $\mathcal{A}$.

Definition 8 (Onewayness) Let κ be a security parameter, $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme, and $\mathcal{M}_{\mathsf{pk}}$ be a message space of Π in the case where the public key is pk. We say that Π is *oneway* (against CPA attack) if for any polytime adversary $\mathcal{I}$ (named *inverter*), the probability

$$\Pr((\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa), M \leftarrow \mathcal{M}_{\mathsf{pk}}, C \leftarrow \mathsf{Enc}_{\mathsf{pk}}(M), M' \leftarrow \mathcal{I}(\mathsf{pk}, C) : M = M')$$

is negligible for κ.

Plaintext Awareness defined in [BR94,BDPR98] We review the definitions of the PA1 and the PA2 in the random oracle model, defined in [BR94,BDPR98].

Definition 9 (Random Oracle PA2) Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme which uses a hash function. For a hash function Hash, we let $\mathsf{Gen}^{\mathsf{Hash}}$, $\mathsf{Enc}^{\mathsf{Hash}}$, and $\mathsf{Dec}^{\mathsf{Hash}}$ denote the key generation, encryption, and decryption algorithms instantiated by the hash function Hash. Let $\mathcal{A}$ and $\mathcal{K}$ be polytime machines, which are respectively called *adversary* and *extractor*. For a security parameter $\kappa \in \mathbb{N}$, let $\mathbf{Exp}^{\mathsf{PA2\text{-}RO}}_{\Pi,\mathcal{A},\mathcal{K}}(\kappa)$ denote the experiment described in Fig. 3.

```
$\mathsf{Hash} \leftarrow$ (Set of all hash functions), $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}^{\mathsf{Hash}}(1^\kappa)$.
$C \leftarrow \mathcal{A}^{\mathsf{Hash},\mathsf{Enc}_{\mathsf{pk}}^{\mathsf{Hash}}}(\mathsf{pk})$.
$\mathsf{HList} \leftarrow$(The list of all pairs of hash queries of $\mathcal{A}$ and the corresponding answers),
$\mathsf{CList} \leftarrow$(The list of all answers of the oracle $\mathsf{Enc}_{\mathsf{pk}}^{\mathsf{Hash}}$).
$M \leftarrow \mathcal{K}(\mathsf{pk}, C, \mathsf{HList}, \mathsf{CList})$.
If $M = \mathsf{Dec}_{\mathsf{sk}}^{\mathsf{Hash}}(C)$, return 1. Otherwise return 0.
```

Fig. 3. Experiment used to define the random oracle PA2

In this experiment, C must not be an element of CList. We say the public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *random oracle PA2 secure*, if there exists $\mathcal{K}$ such that, for any $\mathcal{A}$, the success probability

$$\mathsf{Succ}_{\Pi,\mathcal{A},\mathcal{K}}^{\mathsf{PA2\text{-}RO}}(\kappa) = \Pr(\mathbf{Exp}_{\Pi,\mathcal{A},\mathcal{K}}^{\mathsf{PA2\text{-}RO}}(\kappa) = 1)$$

is overwhelming for κ.

Definition 10 (Random Oracle PA1) We say that a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ satisfies the *random oracle PA1*, if there exists an extractor $\mathcal{K}$ such that, for any adversary $\mathcal{A}$ which makes no query to the encryption oracle, the success probability $\mathsf{Succ}_{\Pi,\mathcal{A},\mathcal{K}}^{\mathsf{PA2\text{-}RO}}(\kappa)$ is negligible for κ.

Theorem 11. ***(Fundamental Theorem for the random oracle PA [BR94, BDPR98])*** *Let Π be an IND-CPA secure public-key encryption scheme in the random oracle model. If Π satisfies the random oracle PA1 or PA2 security, then Π is IND-CCA1 or IND-CCA2 secure respectively.*

Standard Model PA1 We next review the definition of the PA1 in the sense of [BP04]. We use two experiments for defining PA1. These experiments are almost the same as those for PA2, except that an adversary makes no query to the plaintext creator $\mathcal{P}$. Since the experiments do not depend on $\mathcal{P}$, we denote them by $\mathbf{Exp}_{\Pi,\mathcal{A}}^{\mathsf{PA1\text{-}Dec}}(\kappa)$ and $\mathbf{Exp}_{\Pi,\mathcal{A},\mathcal{K}}^{\mathsf{PA1\text{-}Ext}}(\kappa)$.

Definition 12 (standard model PA1) We say that a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *perfect/statistical/computational PA1 secure* in the sense of [BP04], or easily *perfect/statistical/computational PA1 secure*, if for each adversary $\mathcal{A}$ such that it makes no query to the plaintext creator, there exists $\mathcal{K}$ such that the two experiments $\mathbf{Exp}_{\Pi,\mathcal{A}}^{\mathsf{PA1\text{-}Dec}}(\kappa)$ and $\mathbf{Exp}_{\Pi,\mathcal{A},\mathcal{K}}^{\mathsf{PA1\text{-}Ext}}(\kappa)$ are perfectly/statistically/computationally indistinguishable. We simply say that Π is *PA1 secure* in the sense of [BP04], (or *PA1 secure*) if Π is computationally PA1 secure.

Theorem 13 (Fundamental Theorem for Standard Model PA1 [BP04]). *Let Π be an IND-CPA secure public-key encryption scheme. If Π is (perfect, statistical, or computational) PA1 secure, then Π is IND-CCA1 secure.*