ISSN 1342-2812

Research Reports on Mathematical and Computing Sciences

Token-Controlled Public-Key Encryption in the Multi-User Setting

Ryotaro Hayashi and Keisuke Tanaka

February 2007, C–242

Department of
Mathematical and
Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

Token-Controlled Public-Key Encryption in the Multi-User Setting

Ryotaro Hayashi and Keisuke Tanaka *

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

February 22, 2007

Abstract

In this paper, we formalize the security notions for token-controlled public-key encryption in the multi-user setting, by not simply modifying the previous security notions in the single-user setting proposed by Baek, Safavi-Naini, and Susilo [1], and Galindo and Herranz [4], but employing the idea to formalize the attacks in the multi-user setting proposed by Bellare, Boldyreva, and Micali [2]. We formalize four security notions, called M-T1-CCA, M-T2-CCA, M-IS-CPA, and M-SETUF. Our security notions capture the possibility that the adversary sees the encryptions of the related messages under the *same* token and *different* keys when the choice of the relation is made by the adversary. We then show the relationships between the previous and our proposed security notions. We also prove that the Galindo–Herranz scheme, which was proved to be secure in the single-user setting, also meets our proposed four security notions in the multi-user setting. that is, we show that the Galindo–Herranz scheme meets M-T1-CCA, M-T2-CCA, M-IS-CPA, and M-SETUF.

Keywords: token-controlled public-key encryption, multi-user setting, timed-release encryption.

1 Introduction

Consider the following situation. There is a millionaire who would like to write a will for his three sons. This will is written, sealed, and sent to his sons. However, he will not allow his sons to read the will before he passes away. Baek, Safavi-Naini, and Susilo [1] gave a solution to this situation by introducing a cryptographic primitive called token-controlled public-key encryption. In the token-controlled public-key encryption schemes, the sender encrypts messages by using the public key of the receiver together with an extra piece of information called "token." Then, no one can decrypt the ciphertext even if the underlying token is not released, and only the receiver who has the secret key can decrypt the ciphertext when the token is released. In the above scenario, by using the token-controlled public-key encryption scheme, the millionaire encrypts his will with his sons' public keys and sends the ciphertext to his sons. Then, he sends the token used to create the sealed will to a lawyer whom he trusts. In this case, his sons cannot read his will until the token is revealed by the lawyer. Furthermore, the lawyer cannot read his will since the lawyer does not have a secret key.

Token-controlled public-key encryption is related to other previously proposed primitives in the context of timed-release encryption [5, 6]. Most of these schemes require the trusted third party which

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

must perform some costly cryptographic operations. In token-controlled public-key encryption, the only cost for the external entity is to store and deliver a token when some condition (not necessarily related to time) is satisfied. It is required for the token-controlled public-key encryption schemes that the space to store the token is much less than that to store the ciphertext.

In [1], Baek, Safavi-Naini, and Susilo formalized the definition and the security properties for token-controlled public-key encryption as the indistinguishability against the outsider attacks (T1-CCA, T2-CCA), and that against the insider attacks (IS-CPA). The notions T1-CCA and T2-CCA capture the property that, given a ciphertext (and a token), the person who does not have a secret key cannot get any information about the plaintext underlying the ciphertext. The adversary in the T1-CCA game holds neither a secret-key nor a token, while the adversary in the T2-CCA game does not have a secret-key but has a token. (Note that T2-CCA does not imply T1-CCA since there are some restrictions with respect to the oracle queries for the adversary in the T2-CCA game, while there is no such a restriction for that in the T1-CCA game.) On the other hand, the notion IS-CPA captures the property that, if the token is not revealed, given a ciphertext, not only the person who does not have a secret key but also the secret-key holder cannot get any information about the plaintext underlying the ciphertext. They also proposed a token-controlled public-key encryption scheme and proved its security.

In [4], Galindo and Herranz proposed a new security notion for token-controlled public-key encryption, called the strong existential token unforgeability (SETUF). This security notion captures the property that anyone cannot produce one ciphertext c and two tokens tk_0, tk_1 such that two pairs, (c, tk_0) and (c, tk_1), are valid, and the two corresponding plaintexts are different. In the will scenario, if the scheme does not satisfy this security property, the lawyer may be able to change the will that the millionaire wants to send to his sons by replacing the token. Galindo and Herranz also showed that the scheme proposed in [1] does not satisfy SETUF. They also proposed a very simple and efficient generic construction of token-controlled public-key encryption schemes from any trap-door partial one-way function, and proved its security.

In the practical situation, we can consider the situation that the sender sends many ciphertexts to many receivers by using the token-controlled public-key encryption schemes. In this case, it is convenient that one token can control the decryption operation of multiple messages and multiple receivers. In fact, in [1], Baek, Safavi-Naini, and Susilo noted that the token can be reusable in the multiple receiver setting, that is, one token can control the decryption operation of multiple receivers without compromising the security. They also noted that the security notions in the single-user setting can be extended to those in the multi-user setting. In [4], Galindo and Herranz described the notion of T2-CCA in the multi-user setting by simply modifying that in the single-user setting.

Incidentally, Bellare, Boldyreva, and Micali [2] formalized the security notion (of the indistinguishability) on public-key encryption in the multi-user setting. This security notion is not the simple extension of that in the single-user setting. In their formalization, they captured the possibility that the adversary sees the encryptions of the related messages under the different keys when the choice of the relation is made by the adversary. They also showed that any public-key encryption scheme which is secure in the sense of IND-CCA satisfies the security in the multi-user setting formalized by Bellare, Boldyreva, and Micali.

In this paper, we formalize the security notions for token-controlled public-key encryption in the multi-user setting, by not simply modifying the previous security notions in [1], such as [4], but employing the idea to formalize the attacks in the multi-user setting proposed by Bellare, Boldyreva, and Micali [2]. We formalize three security notions in the multi-user setting, M-T1-CCA, M-T2-CCA, and M-IS-CPA, which corresponds to T1-CCA, T2-CCA, and IS-CPA in the single-user setting, respectively. Our security notions capture the possibility of an adversary seeing encryptions of related messages under the *same* token and *different* keys when the choice of the relation can be made by the adversary, while the definition in [4] does not. We also propose the strong existential token unforgeability in the multi-user setting, M-SETUF. Our proposed security notions are considered to be stronger than the previous security notions. In fact, it is easy to see that M-T1-CCA, M-T2-CCA,

M-IS-CPA, and M-SETUF imply T1-CCA, T2-CCA, IS-CPA, and SETUF, respectively.

We then show the relationships between the previous and our proposed security notions. We show that M-T2-CCA does not imply M-T1-CCA and M-IS-CPA implies M-T1-CCA. We also show the equivalence between T2-CCA and M-T2-CCA, and that between SETUF and M-SETUF. However, it is not clear whether T1-CCA implies M-T1-CCA or not, and whether IS-CPA implies M-IS-CPA or not.

We also show that the Galindo–Herranz scheme [4], which was proved to be secure in the single-user setting, is also secure in the multi-user setting. More precisely, we prove that the Galindo–Herranz scheme meets M-IS-CPA. Furthermore, combining the previous result by Galindo and Herranz and our results with respect to the relationships between the security notions, we show that their scheme meets M-T1-CCA, M-T2-CCA, and M-SETUF.

The organization of this paper is as follows. In Section 2, we review the definitions of families of trap-door functions and the partial one-wayness. We also review the definition of token-controlled public-key encryption. In Section 3, we propose security notions for token-controlled public-key encryption in the multi-user setting. In Section 4, we show the relationships between the previous and our proposed security notions. In Section 5, we show that the scheme proposed by Galindo and Herranz [4] is secure in the multi-user setting. We conclude in Section 6.

2 Preliminaries

2.1 Families of Trap-Door Functions

In this section, we review the definitions of families of trap-door functions and the θ-partial one-wayness.

Definition 1 (Families of Trap-Door Functions)**.** *A family of trap-door functions $\mathcal{TF} = (K, f)$ has a following properties.*

- *The key generation algorithm K is a polynomial-time algorithm which takes a security parameter 1^k and outputs a public key pk and a matching secret key (trap-door) sk.*
- *The function f_{pk} is an injective function from the domain $\mathtt{Dom}_{\mathcal{TF}}(\mathsf{pk})$ to the range $\mathtt{Rng}_{\mathcal{TF}}(\mathsf{pk})$, where $\mathtt{Dom}_{\mathcal{TF}}(\mathsf{pk})$ and $\mathtt{Rng}_{\mathcal{TF}}(\mathsf{pk})$ are uniquely determined by pk. We define the inverse function f_{sk}^{-1} from $\mathtt{Rng}_{\mathcal{TF}}(\mathsf{pk})$ to $\mathtt{Dom}_{\mathcal{TF}}(\mathsf{pk})$ as follows. For any $y \in \mathtt{Rng}_{\mathcal{TF}}(\mathsf{pk})$, we define $f_{\mathsf{sk}}^{-1}(y) := x$ if there exists $x \in \mathtt{Dom}_{\mathcal{TF}}(\mathsf{pk})$ such that $y = f_{\mathsf{pk}}(x)$. Otherwise, we define $f_{\mathsf{sk}}^{-1}(y) := \perp$.*
- *There exists a polynomial-time evaluation algorithm which takes pk, $x \in \mathtt{Dom}_{\mathcal{TF}}(\mathsf{pk})$, and outputs $y = f_{\mathsf{pk}}(x)$.*
- *There exists a polynomial-time inversion algorithm which takes sk, $y \in \mathtt{Rng}_{\mathcal{TF}}(\mathsf{pk})$, and outputs $x = f_{\mathsf{sk}}^{-1}(y)$.*

Definition 2 (θ-Partial One-Wayness)**.** *Let $k \in \mathbb{N}$ be a security parameter, and $0 < \theta \leq 1$ a constant. Let $\mathcal{TF} = (K, f)$ be a family of trap-door functions, and A an adversary. We consider the following experiment:*

$$
\begin{array}{l}
\mathtt{Experiment}\ \mathbf{Exp}^{\theta\text{-pow}}_{\mathcal{TF},A}(k) \\
\quad (\mathsf{pk}, \mathsf{sk}) \leftarrow K(1^k);\ x \xleftarrow{R} \mathtt{Dom}_{\mathcal{TF}}(\mathsf{pk});\ y \leftarrow f_{\mathsf{pk}}(x) \\
\quad x_1 \leftarrow A(\mathsf{pk}, y)\ \mathtt{where}\ |x_1| = \lceil \theta \cdot |x| \rceil \\
\quad \mathtt{if}\ (f_{\mathsf{pk}}(x_1 || x_2) = y\ \mathtt{for\ some}\ x_2)\ \mathtt{return}\ 1 \\
\quad \mathtt{else\ return}\ 0
\end{array}
$$

Here, "$||$" denotes concatenation. We define the advantage of the adversary via

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

where the probability is taken over K, $x \xleftarrow{R} \mathsf{Dom}_{\mathcal{TF}}(\mathsf{pk})$, *and* A. *We say that* $\mathcal{TF}$ *is* θ*-partial one-way if the function* $\mathbf{Adv}^{\theta\text{-pow}}_{\mathcal{TF},A}(k)$ *is negligible for any polynomial-time adversary* A.

Note that when $\theta = 1$ the notion of θ-partial one-wayness implies the standard notion of one-wayness.

2.2 The Definition of Token-Controlled Public-Key Encryption

In this section, we review the definition of token-controlled public-key encryption proposed by Baek, Safavi-Naini, and Susilo [1].

Definition 3 (Token-Controlled Public-Key Encryption)**.** *A token-controlled public-key encryption scheme* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *is as follows.*

- *The key-generation algorithm* GK *is a randomized algorithm that takes a security parameter* k, *and returns a pair of public and secret keys* (pk, sk). *The public key* pk *includes the security parameter* k, *descriptions of a token space* $\mathcal{T}_k$, *a plaintext space* $\mathcal{P}_{pk}$, *and a ciphertext space* $\mathcal{C}_{pk}$. *Note that the token space is uniquely determined by the security parameter, while the plaintext and the ciphertext spaces are uniquely determined by the public key.*
- *The token generation algorithm* GT *is a randomized algorithm that takes a security parameter* k, *and returns a token* $tk \in \mathcal{T}_k$ *at random.*
- *The encryption algorithm* E *is a randomized algorithm that takes a public key* pk, *a token* tk, *and a message* $m \in \mathcal{P}_{pk}$, *and returns a ciphertext* $c \in \mathcal{C}_{pk}$.
- *The decryption algorithm* D *is a deterministic algorithm that takes a secret key* sk, *a token* tk, *and a ciphertext* c, *and returns the corresponding plaintext* $m \in \mathcal{P}_{pk}$ *or a special symbol* $\perp$ *to indicate that the ciphertext* c *is invalid.*

3 Token-Controlled Public-Key Encryption in the Multi-User Setting

In this section, we propose the security notions for token-controlled public-key encryption in the multi-user setting.

For comparison, we describe the security notions for token-controlled public-key encryption in the single-user setting proposed by [1, 4], T1-CCA, T2-CCA, IS-CPA, and SETUF, and that in the multi-user setting proposed by [4], which we call M-T2-CCA-GH, in Appendix A. We stress that we formalize the security notions in the multi-user setting by not simply modifying the previous security notions in [1], such as [4], but employing the idea to formalize the attacks in the multi-user setting proposed by Bellare, Boldyreva, and Micali [2].

In order to define the security notions for token-controlled public-key encryption in the multi-user setting, we employ the left or right selector and the left-or-right (LR) encryption oracle in [2].

- The left or right selector is a map LR defined by $\mathrm{LR}(m_0, m_1, b) := m_b$ for $b \in \{0, 1\}$.
- By using the map LR, the left-or-right (LR) encryption oracle $\mathsf{E}_{pk}(tk^*, \mathrm{LR}(\cdot, \cdot, b))$ is defined. For $b \in \{0, 1\}$, the LR encryption oracle, given a query (m_0, m_1) such that $m_0, m_1 \in \mathcal{P}_{pk}$, returns a ciphertext of m_b under the token tk^* and the public key pk.

3.1 Outsider Attacks

First, we consider the security notions against the outside attackers. These security notions capture the property that, given a ciphertext (and a token), the person who does not have a secret key cannot get any information about the plaintext underlying the ciphertext.

We can consider two kinds of outside attackers, "type-1" attackers who hold neither a secret-key nor a token, and "type-2" attackers who does not have a secret-key but has a token. Note that since there are some restrictions with respect to the oracle queries for the type-1 attackers, while there is no such a restriction for the type-2 attackers. (See also Section 4.)

We first propose the indistinguishability against type-1 outside chosen ciphertext attacks in the multi-user setting (M-T1-CCA). The corresponding definition in the single-user setting, T1-CCA, is available in Appendix A.1.

Definition 4 (M-T1-CCA). *Let* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *be a token-controlled public-key encryption scheme. Let* $b \in \{0,1\}$ *and* $k \in \mathbb{N}$. *Let* $A = (A_1, A_2)$ *be an adversary that runs in two stages. We consider the following experiment:*

$$
\begin{array}{l}
\texttt{Experiment } \mathbf{Exp}^{\text{m-t1-cca-}b}_{\mathsf{TCPKE},A}(k) \\
\quad (pk_i, sk_i) \leftarrow \mathsf{GK}(1^k) \ \ \texttt{for } i = 1, \ldots, n \\
\quad tk^* \leftarrow \mathsf{GT}(1^k) \\
\quad d \leftarrow A^{\mathcal{O}_{\text{m-t1-cca}}}(pk_1, \ldots, pk_n) \\
\quad \texttt{return } d
\end{array}
$$

where $\mathcal{O}_{\text{m-t1-cca}} = \{\mathsf{E}_{pk_i}(tk^*, \mathrm{LR}(\cdot,\cdot,b)),\ \mathsf{E}_{pk_i}(tk^*,\cdot),\ \mathsf{D}_{sk_i}(\cdot,\cdot)\}_{1\le i\le n}$. *That is, for* $i = 1, \cdots, n$, *the adversary can make access to the left-or-right encryption oracle* $\mathsf{E}_{pk_i}(tk^*, \mathrm{LR}(\cdot,\cdot,b))$, *the token-embedded encryption oracle* $\mathsf{E}_{pk_i}(tk^*,\cdot)$, *and the decryption oracle* $\mathsf{D}_{sk_i}(\cdot,\cdot)$.

We define the advantage via

$$
\mathbf{Adv}^{\text{m-t1-cca}}_{\mathsf{TCPKE},A}(k) = \Big|\Pr[\mathbf{Exp}^{\text{m-t1-cca-0}}_{\mathsf{TCPKE},A}(k) = 1] - \Pr[\mathbf{Exp}^{\text{m-t1-cca-1}}_{\mathsf{TCPKE},A}(k) = 1]\Big|.
$$

We say that a token-controlled public-key encryption scheme TCPKE *meets M-T1-CCA if* $\mathbf{Adv}^{\text{m-t1-cca}}_{\mathsf{TCPKE},A}(k)$ *is negligible for any polynomial-time adversary A.*

Note that it is easy to see that M-T1-CCA implies T1-CCA (See [1] or Appendix A.1 for T1-CCA.).

We next propose the indistinguishability against type-2 outside chosen ciphertext attacks in the multi-user setting (M-T2-CCA). The corresponding definition in the single-user setting, T2-CCA, is available in Appendix A.2. Note that, in the following definition, the adversary gets not only the public keys but also the token.

Definition 5 (M-T2-CCA). *Let* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *be a token-controlled public-key encryption scheme. Let* $b \in \{0,1\}$ *and* $k \in \mathbb{N}$. *Let* $A = (A_1, A_2)$ *be an adversary that runs in two stages. We consider the following experiment:*

$$
\begin{array}{l}
\texttt{Experiment } \mathbf{Exp}^{\text{m-t2-cca-}b}_{\mathsf{TCPKE},A}(k) \\
\quad (pk_i, sk_i) \leftarrow \mathsf{GK}(1^k) \ \ \texttt{for } i = 1, \ldots, n \\
\quad tk^* \leftarrow \mathsf{GT}(1^k) \\
\quad d \leftarrow A^{\mathcal{O}_{\text{m-t2-cca}}}(tk^*, pk_1, \ldots, pk_n) \\
\quad \texttt{return } d
\end{array}
$$

where $\mathcal{O}_{\text{m-t2-cca}} = \{\mathsf{E}_{pk_i}(tk^*, \mathrm{LR}(\cdot,\cdot,b)),\ \mathsf{D}_{sk_i}(\cdot,\cdot)\}_{1\le i\le n}$. *That is, for* $i = 1, \cdots, n$, *the adversary makes access to the left-or-right encryption oracle* $\mathsf{E}_{pk_i}(tk^*, \mathrm{LR}(\cdot,\cdot,b))$, *and the decryption oracle* $\mathsf{D}_{sk_i}(\cdot,\cdot)$. *However, the adversary cannot ask the pair* (c_i, tk^*) *to the decryption oracle* D_{sk_i} *where* c_i *is an output of the left-or-right encryption oracle* $\mathsf{E}_{pk_i}(tk^*, \mathrm{LR}(\cdot,\cdot,b))$, *for* $i = 1, \cdots, n$.

We define the advantage via

$$\mathbf{Adv}^{\text{m-t2-cca}}_{\mathsf{TCPKE},A}(k) = \left|\Pr[\mathbf{Exp}^{\text{m-t2-cca-0}}_{\mathsf{TCPKE},A}(k) = 1] - \Pr[\mathbf{Exp}^{\text{m-t2-cca-1}}_{\mathsf{TCPKE},A}(k) = 1]\right|.$$

We say that a token-controlled public-key encryption scheme TCPKE *meets M-T2-CCA if* $\mathbf{Adv}^{\text{m-t2-cca}}_{\mathsf{TCPKE},A}(k)$ *is negligible for any polynomial-time adversary A.*

Note that it is easy to see that M-T2-CCA implies T2-CCA (See [1] or Appendix A.2 for T2-CCA.).

Remark 1. In [4], Galindo and Herranz proposed a security notion of the indistinguishability against type-2 outside chosen ciphertext attacks which is different from T2-CCA (in the single-user setting) by Baek, Safavi-Naini, and Susilo. Their formalization seems to consider the multi-user setting. We call their formalization M-T2-CCA-GH, which is available in Appendix A.3. Similar to our formalization, the adversary takes n public keys and token in the M-T2-CCA-GH game.

There are some differences between their formalization and ours. First, in the Galindo–Herranz formalization, the adversary is allowed to get only one challenge ciphertext, while in our formalization, the adversary can make polynomial-time queries to the left-or-right encryption oracle adaptively. Second, in the Galindo–Herranz formalization, the adversary has to choose messages m_0 and m_1 to generate a challenge ciphertext from $\cap_{i=1}^{n}\mathcal{P}_{pk_i}$. Because of this restriction, even if the scheme achieves M-T2-CCA-GH, it is not clear that the scheme satisfies T2-CCA. It seems to be a little unnatural since the security in the multi-user setting may not imply that in the single-user setting. Note that if the message space is common to each public key pk_i, then M-T2-CCA-GH implies T2-CCA. In fact, Galindo and Herranz showed their proposed scheme satisfies M-T2-CCA-GH, and we can see that it also satisfies M-T2-CCA since the plaintext space of their scheme is common to each public key.

In our formalization, the adversary chooses messages m_0 and m_1 from $\mathcal{P}_{pk_i}$ if the adversary makes a query to the left-or-right encryption oracle with the public key pk_i. We can easily see that the scheme which meets M-T2-CCA also meets T2-CCA. We will prove that T2-CCA implies M-T2-CCA later on.

3.2 Insider Attacks

Next, we consider the security notion against the inside attackers. This security notion captures the property that, if the token is not revealed, given a ciphertext, not only the person who does not have a secret key but also the secret-key holder cannot get any information about the plaintext underlying the ciphertext.

We propose the indistinguishability against inside chosen plaintext attacks in the multi-user setting (M-IS-CPA). The corresponding definition in the single-user setting, IS-CPA, is available in Appendix A.4. Note that, in the following definition, the adversary gets the public key and the corresponding secret key, while the adversary does not get the token.

Definition 6 (M-IS-CPA)**.** *Let* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *be a token-controlled public-key encryption scheme. Let* $b \in \{0,1\}$ *and* $k \in \mathbb{N}$*. Let A be an adversary. We consider the following experiment:*

$$\begin{array}{l}\texttt{Experiment } \mathbf{Exp}^{\text{m-is-cpa-}b}_{\mathsf{TCPKE},A}(k)\\ \quad (pk_i, sk_i) \leftarrow \mathsf{GK}(1^k) \ \texttt{ for } i = 1, \ldots, n\\ \quad tk^* \leftarrow \mathsf{GT}(1^k)\\ \quad d \leftarrow A^{\mathcal{O}_{\text{m-is-cpa}}}(pk_1, \ldots, pk_n, sk_1, \ldots, sk_n)\\ \quad \texttt{return } d\end{array}$$

where $\mathcal{O}_{\text{m-is-cpa}} = \{\mathsf{E}_{pk_i}(tk^*, \mathrm{LR}(\cdot,\cdot,b)),\ \mathsf{E}_{pk_i}(tk^*,\cdot)\}_{1\le i\le n}$*. That is, for* $i = 1, \cdots, n$*, the adversary makes access to the left-or-right encryption oracle* $\mathsf{E}_{pk_i}(tk^*, \mathrm{LR}(\cdot,\cdot,b))$*, which takes a pair of two*

	input	oracles	restriction
M-T1-CCA	$\{pk_i\}$	LR encryption, decryption, token-embedded encryption	none
M-T2-CCA	$\{pk_i\}$, tk^*	LR encryption, decryption	cannot ask (c_i, tk^*) to D_{sk_i} (c_i : challenge ciphertext from LR encryption oracle with pk_i)
M-T2-CCA-GH	$\{pk_i\}$, tk^*	encryption (can access only once and $m_0, m_1 \in \cap_{i=1}^{n} \mathcal{P}_{pk_i}$) decryption	cannot ask (c_i, tk^*) to D_{sk_i} (c_i : challenge ciphertext from LR encryption oracle with pk_i)
M-IS-CPA	$\{pk_i\}$, $\{sk_i\}$	LR encryption, token-embedded encryption	none

Table 1: The differences of the adversaries in M-T1-CCA, M-T2-CCA, M-T2-CCA-GH, and M-IS-CPA.

messages (m_0, m_1) *such that* $m_0, m_1 \in \mathcal{P}_{pk_i}$*, and returns* $\mathsf{E}_{pk_i}(tk^*, m_b)$*. The adversary can also make access to the token-embedded encryption oracle* $\mathsf{E}_{pk_i}(tk^*, \cdot)$ *for* $i = 1, \cdots, n$*.*

We define the advantage via

$$\mathbf{Adv}^{\text{m-is-cpa}}_{\mathsf{TCPKE},A}(k) = \left|\Pr[\mathbf{Exp}^{\text{m-is-cpa-0}}_{\mathsf{TCPKE},A}(k) = 1] - \Pr[\mathbf{Exp}^{\text{m-is-cpa-1}}_{\mathsf{TCPKE},A}(k) = 1]\right|.$$

We say that a token-controlled public-key encryption scheme TCPKE *meets M-IS-CPA if* $\mathbf{Adv}^{\text{m-is-cpa}}_{\mathsf{TCPKE},A}(k)$ *is negligible for any polynomial-time adversary A.*

Note that it is easy to see that M-IS-CPA implies IS-CPA (See [1] or Appendix A.4 for IS-CPA.).

The differences of the adversaries in M-T1-CCA, M-T2-CCA, M-T2-CCA-GH, and M-IS-CPA are described in Table 1.

3.3 Strong Existential Token Unforgeability

We describe the definition of the strong existential token unforgeability (SETUF) in the single-user setting by Galindo and Herranz in Appendix A.5. In the experiment of SETUF, the adversary does not receive any challenge ciphertext. Thus, we do not need to apply the idea by Bellare, Boldyreva, and Micali in order to define the security notion in the multi-user setting. Therefore, we simply modify SETUF in the single user setting to that in the multi-user setting as follows.

Definition 7 (M-SETUF)**.** *Let* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *be a token-controlled public-key encryption scheme. Let* $k \in \mathbb{N}$ *be a security parameter, and A an adversary. We consider the following experiment:*

$\mathtt{Experiment}\ \mathbf{Exp}^{\text{m-setuf}}_{\mathsf{TCPKE},A}(k)$
$(pk_i, sk_i) \leftarrow \mathsf{GK}(1^k)\ \ \mathtt{for}\ i = 1, \ldots, n$
$(c, pk, tk, tk') \leftarrow A^{\mathcal{O}_{\text{m-setuf}}}(pk_1, \ldots, pk_n)$
$\mathtt{if}\ ((pk \notin \{pk_i\}_{1 \le 1 \le n}) \vee (tk \notin \mathcal{T}_k) \vee (tk' \notin \mathcal{T}_k))\ \mathtt{then\ return}\ 0$
$m \leftarrow \mathsf{D}_{sk}(tk, c);\ m' \leftarrow \mathsf{D}_{sk}(tk', c)$
$\mathtt{if}\ ((m \neq \perp) \wedge (m' \neq \perp) \wedge (m \neq m'))\ \mathtt{then\ return}\ 1\ \mathtt{else\ return}\ 0$

where $\mathcal{O}_{\text{m-setuf}} = \{\mathsf{D}_{sk_i}(\cdot, \cdot)\}_{1 \le i \le n}$*. That is, for* $i = 1, \cdots, n$*, the adversary makes access to the decryption oracle* $\mathsf{D}_{sk_i}(\cdot, \cdot)$*.*

We define the advantage via

$$\mathbf{Adv}^{\text{m-setuf}}_{\mathsf{TCPKE},A}(k) = \Pr[\mathbf{Exp}^{\text{m-setuf}}_{\mathsf{TCPKE},A}(k) = 1].$$

We say that a token-controlled public-key encryption scheme TCPKE *meets M-SETUF if the function* $\mathbf{Adv}^{\text{m-setuf}}_{\mathsf{TCPKE},A}(k)$ *is negligible for any polynomial-time adversary A.*

We also note that it is easy to see that M-SETUF implies SETUF (See [4] or Appendix A for SETUF.).

4 Relationships between Security Notions

In this section, we show the relationships between the previous and our proposed security notions.

4.1 M-T2-CCA $\not\Rightarrow$ M-T1-CCA

In [4], Galindo and Herranz proposed the token-controlled public-key encryption scheme (which we describe in Section 5). Although we have two security notions against the outside attackers in the single-user setting, T1-CCA and T2-CCA, they only proved that thier scheme satisfies T2-CCA (See [1] or Appendix A for the definitions of T1-CCA and T2-CCA.).

We can see that M-T2-CCA does not imply M-T1-CCA, and that T2-CCA does not imply T1-CCA. Consider the token-controlled public-key encryption scheme $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ which is secure in the sense of M-T2-CCA. We modify this scheme by attaching the token to the ciphertext. That is, we modify the encryption and decryption algorithms as $\mathsf{E}'_{pk}(tk, m) := \mathsf{E}_{pk}(tk, m)||tk$, and $\mathsf{D}'_{sk}(tk, c_1||c_2) := \mathsf{D}_{sk}(tk, c_1)$ if $tk = c_2$ and $\mathsf{D}'_{sk}(tk, c_1||c_2) := \perp$ if $tk \neq c_2$. Then, the scheme $(\mathsf{GK}, \mathsf{GT}, \mathsf{E}', \mathsf{D}')$ is secure in the sense of M-T2-CCA, since the adversary in the M-T2-CCA game has the token and the adversary does not gain any information even if the token is attached to the ciphertext. On the other hand, in the M-T1-CCA game, since the adversary can ask the pair of the token and the challenge ciphertext to the decryption oracle, the adversary always wins the M-T1-CCA game.

From a similar argument, we can see that T2-CCA does not imply T1-CCA. Therefore, it is not clear that the Galindo–Herranz scheme meets T1-CCA. However, since we will prove that IS-CPA implies T1-CCA in the next section, we can see that the Galindo–Herranz scheme meets T1-CCA.

4.2 M-IS-CPA $\Rightarrow$ M-T1-CCA

We can see that if the scheme is secure in the sense of M-IS-CPA, then the scheme also meets M-T1-CCA. If there exists an adversary A which attaks the token-controlled public-key encryption scheme TCPKE in the sense of M-T1-CCA, we can construct the adversary B which attacks TCPKE in the sense of M-IS-CPA as follows. The algorithm B, given $\{(pk_i, sk_i)\}_{1 \leq i \leq n}$, runs $A(pk_1, \cdots, pk_n)$. During the execution of A, if A makes queries to the left-or-right oracle or the token-embedded encryption oracle, B responds to them by using B's oracles. If A makes queries to the decryption oracle D_{sk_i}, B responds to them by using the secret key sk_i which is the input of B. Finally, B returns A's output. It is easy to see that the advantage of B is the same as that of A. Note that, in the single-user setting, we can prove that IS-CPA implies T1-CCA in a similar way.

4.3 T2-CCA $\Leftrightarrow$ M-T2-CCA

We can see that M-T2-CCA implies T2-CCA. In the following, we show that T2-CCA implies M-T2-CCA (See [1] or Appendix A.2 for the definition of T2-CCA).

Theorem 1. *If there exists a polynomial-time adversary A attacking the token-controlled public-key encryptoin scheme TCPKE in the multi-user setting, which makes at most q_e queries to each left-or-right encryption oracle with pk_i ($1 \leq i \leq n$), then we can construct a polynomial-time algorithm B attacking TCPKE in the single-user setting such that*

$$\mathbf{Adv}^{\text{t2-cca}}_{\mathsf{TCPKE},B}(k) \geq \frac{1}{n \cdot q_e} \cdot \mathbf{Adv}^{\text{m-t2-cca}}_{\mathsf{TCPKE},A}(k).$$

Proof. We construct the adversary B attacking TCPKE in the sense of T2-CCA in the single-user setting. It is easy to see that B is a polynomial-time algorithm if A is a polynomial-time algorithm. Note that B can respond to the decryption queries, since B has the secret keys for $i \in \{1, \ldots, n\} \backslash \{i\}$, and B can use B's decryption oracle for $i = c$.

Algorithm $B^{\mathsf{D}_{sk}(\cdot,\cdot)}(pk)$

$\ell \xleftarrow{R} \{1, \cdots, nq_e\}$

Set c, r such that $\ell = (c-1)q_e + r$, $1 \le r \le q_e$, and $1 \le c \le n$.

$pk_c \leftarrow pk$

$(pk_i, sk_i) \leftarrow \mathsf{GK}(1^k)$ for $i \in \{1, \ldots, n\} \backslash \{c\}$

$tk^* \leftarrow \mathsf{GT}(1^k)$

Run A and get an output d of A, where if A makes a t-th query (m_0, m_1) to the left-or-right encryption oracle with pk_i ($1 \le i \le n$, $1 \le t \le q_e$), B respond it by C as follows:

- if $(i < c)$ then $C \leftarrow \mathsf{E}_{pk_i}(tk^*, m_0)$
- if $(i > c)$ then $C \leftarrow \mathsf{E}_{pk_i}(tk^*, m_1)$
- if $(i = c)$
  - if $(t < r)$ then $C \leftarrow \mathsf{E}_{pk_i}(tk^*, m_0)$
  - if $(t > r)$ then $C \leftarrow \mathsf{E}_{pk_i}(tk^*, m_1)$
  - if $(t = r)$ then B makes a query (m_0, m_1) to B's encryption oracle and sets $C \leftarrow \mathsf{E}_{pk}(tk^*, m_b)$.

return d

For $1 \le i \le nq_e - 1$, we have

$$\Pr[\mathbf{Exp}^{\text{t2-cca-0}}_{\mathsf{TCPKE},B}(k) = 1 | \ell = i] = \Pr[\mathbf{Exp}^{\text{t2-cca-1}}_{\mathsf{TCPKE},B}(k) = 1 | \ell = i+1].$$

Furthermore, we can see that

$$\Pr[\mathbf{Exp}^{\text{t2-cca-0}}_{\mathsf{TCPKE},B}(k) = 1 | \ell = nq_e] = \Pr[\mathbf{Exp}^{\text{m-t2-cca-0}}_{\mathsf{TCPKE},B}(k) = 1]$$

and

$$\Pr[\mathbf{Exp}^{\text{t2-cca-1}}_{\mathsf{TCPKE},B}(k) = 1 | \ell = 1] = \Pr[\mathbf{Exp}^{\text{m-t2-cca-1}}_{\mathsf{TCPKE},B}(k) = 1].$$

Therefore, we have

$$\begin{aligned}
\mathbf{Adv}^{\text{t2-cca}}_{\mathsf{TCPKE},B}(k) &= \frac{1}{nq_e} \cdot \left| \sum_{i=1}^{nq_e} (\Pr[\mathbf{Exp}^{\text{t2-cca-0}}_{\mathsf{TCPKE},B}(k) = 1 | \ell = i] - \Pr[\mathbf{Exp}^{\text{t2-cca-1}}_{\mathsf{TCPKE},B}(k) = 1 | \ell = i]) \right| \\
&= \frac{1}{nq_e} \cdot |\Pr[\mathbf{Exp}^{\text{t2-cca-0}}_{\mathsf{TCPKE},B}(k) = 1 | \ell = nq_e] - \Pr[\mathbf{Exp}^{\text{t2-cca-1}}_{\mathsf{TCPKE},B}(k) = 1 | \ell = 1]| \\
&= \frac{1}{nq_e} \cdot \mathbf{Adv}^{\text{m-t2-cca}}_{\mathsf{TCPKE},A}(k).
\end{aligned}$$

□

Remark 2. We have proved that T2-CCA in the single-user setting is equivalent to that in the multi-user setting, by using a simple hybrid argument.

We note that it is not clear that T1-CCA and IS-CPA in the single-user setting are equivalent to those in the multi-user setting, respectively. Assume that A is an algorithm attacking the scheme in the sense of M-T1-CCA. A takes n public keys as input. If we construct an algorithm B attacking the same scheme in the sense of T1-CCA by using A, we have to simulate the token-embedded oracles for all public keys for A, while B has only one token-embedded oracle for one public key and B does not have the token. Thus, it seems to be hard to simulate such oracles and to prove that T1-CCA implies M-T1-CCA in a similar way as in the case of T2-CCA and M-T2-CCA. We can say a similar thing on the case of IS-CPA and M-IS-CPA.

4.4 SETUF ⇔ M-SETUF

It is easy to see that M-SETUF implies SETUF (See [4] or Appendix A.5 for the definition of SETUF.). Furthermore, we can easily see that if the scheme meets SETUF the scheme also meets M-SETUF. More precisely, if there exists an algorithm A which breaks SETUF with the advantage ϵ, then there also exists an algorithm B which breaks M-SETUF with the advantage at least ϵ/n.

5 The Galindo–Herranz Scheme and its Security in the Multi-User Setting

In this section, we review the token-controlled public-key encryption scheme proposed by Galindo and Herranz [4] and prove its security in the multi-user setting.

5.1 The Galindo–Herranz Scheme

In [4], Galindo and Herranz proposed a very simple and efficient generic construction of token-controlled public-key encryption schemes from any trap-door partial one-way function. Their construction is based on the Fujisaki–Okamoto conversion [3].

Definition 8. *The Galindo–Herranz token-controlled public-key encryption scheme* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *with a family of trap-door functions* $\mathcal{TF} = (K, f)$ *is as follows. The key-generation algorithm* GK *takes a security parameter* k_0, k_1, t, n*, runs the key generation algorithm* $K(1^{k_0}, 1^{k_1})$ *of* $\mathcal{TF}$*, and gets a pair of public and secret keys* $(\mathsf{pk}, \mathsf{sk})$*, where* $\mathtt{Dom}_{\mathcal{TF}}(\mathsf{pk}) = \{0,1\}^{k_0+k_1}$ *and* $\mathtt{Rng}_{\mathcal{TF}}(\mathsf{pk}) = \{0,1\}^k$ *for some* $k \geq k_0 + k_1$*. Let* $\mathcal{T}_t = \{0,1\}^t$ *be a token space,* $\mathcal{P}_{pk} = \{0,1\}^n$ *a plaintext space, and* $\mathcal{C}_{pk} = \{0,1\}^k \times \{0,1\}^n$ *a ciphertext space. Then, it outputs a public key* $pk = (\mathsf{pk}, \mathcal{T}_t, \mathcal{P}_{pk}, \mathcal{C}_{pk})$ *and a secret key* $sk = \mathsf{sk}$*. The token-generation algorithm* GT *takes a security parameter* k_0, k_1, t, n *and outputs* $tk \xleftarrow{R} \mathcal{T}_t$*. The encryption and decryption algorithms are as follows. Note that* $G : \{0,1\}^{k_0} \times \{0,1\}^t \to \{0,1\}^n$ *and* $H : \{0,1\}^{k_0} \times \{0,1\}^n \to \{0,1\}^{k_1}$ *are hash functions.*

$\mathtt{Algorithm}\ \mathsf{E}_{pk}(tk, m)$	$\mathtt{Algorithm}\ \mathsf{D}_{sk}(tk, (c_1, c_2))$
$x \xleftarrow{R} \{0,1\}^{k_0}$	$\mathtt{if}\ (f_{\mathsf{sk}}^{-1}(c_1) = \perp)\ \mathtt{then\ return}\ \perp$
$c_1 \leftarrow f_{\mathsf{pk}}(x, H(x, m))$	$(x, y) \leftarrow f_{\mathsf{sk}}^{-1}(c_1)$
$c_2 \leftarrow G(x, tk) \oplus m$	$m \leftarrow c_2 \oplus G(x, tk)$
$\mathtt{return}\ (c_1, c_2)$	$\mathtt{if}\ (c_1 = f_{\mathsf{pk}}(x, H(x, m)))\ \mathtt{then\ return}\ m\ \mathtt{else\ return}\ \perp$

Galindo and Herranz proved that the above scheme is secure in the sense of M-T2-CCA-GH, IS-CPA, and SETUF in the random oracle model if the family of trap-door functions $\mathcal{TF}$ is $k_0/(k_0+k_1)$-partial one-way. Since the plaintext space is common to each public key in this scheme, this scheme also meets T2-CCA (See Remark 1.) and T1-CCA under the same assumption, since we have shown (M-)IS-CPA implies (M-)T1-CCA.

5.2 Security in the Multi-User Setting

We have shown in Section 4.3 that T2-CCA implies M-T2-CCA, and also shown in Section 4.4 that SETUF implies M-SETUF. Therefore, the Galindo–Herranz scheme is secure in the sense of M-T2-CCA and M-SETUF in the random oracle model under the assumption that $\mathcal{TF}$ is $k_0/(k_0+k_1)$-partial one-way.

We now show that the Galindo–Herranz scheme is secure in the sense of M-IS-CPA.

Theorem 2. *For any polynomial-time adversary* A*, making at most* q_g *queries to* G *and* q_{te} *queries to the token-embedded encryption oracle,*

$$\mathbf{Adv}^{\text{m-is-cpa}}_{\mathsf{TCPKE},A}(k) \leq \frac{nq_e(q_g + q_{te})}{2^t}.$$

Proof. Let A be an adversary. Consider the challenge ciphertexts $(\hat{c}_1^{(1,j)}, \hat{c}_2^{(1,j)}), \ldots, (\hat{c}_1^{(q_e,j)}, \hat{c}_2^{(q_e,j)})$ which the adversary gets from the left-or-right encryption oracle with the public key pk_j. Let tk^* be a token which is selected at the beginning of the M-IS-CPA game. The challenge ciphertext $(\hat{c}_1^{(i,j)}, \hat{c}_2^{(i,j)})$ is computed as

$$\begin{aligned}\hat{c}_1^{(i,j)} &= f_{\mathsf{pk}}(\hat{x}^{(i,j)}, H(\hat{x}^{(i,j)}, m_b^{(i,j)}))\\ \hat{c}_2^{(i,j)} &= G(\hat{x}^{(i,j)}, tk^*) \oplus m_b^{(i,j)}\end{aligned}$$

where $\hat{x}^{(i,j)} \xleftarrow{R} \{0,1\}^{k_0}$, $(m_0^{(i,j)}, m_1^{(i,j)})$ is an i-th query of the adversary A to the left-or-right encryption oracle with the public key pk_j, and b is a bit which the adversary A tries to guess.

We denote by $\mathsf{AskG}_{(i,j)}$ the event that the adversary A makes a query $(\hat{x}^{(i,j)}, tk^*)$ to G, and let $\mathsf{AskG} = \bigvee_{1\le i\le q_e, 1\le j\le n} \mathsf{AskG}_{(i,j)}$.

Since G is a random oracle, the value b is independent of A's view if the event AskG does not occur. Thus, $\Pr[\mathbf{Exp}^{\text{m-is-cpa-0}}_{\mathsf{TCPKE},A}(k) = 1 | \neg\mathsf{AskG}] = \Pr[\mathbf{Exp}^{\text{m-is-cpa-1}}_{\mathsf{TCPKE},A}(k) = 1 | \neg\mathsf{AskG}]$. We have

$$\begin{aligned}\mathbf{Adv}^{\text{m-is-cpa}}_{\mathsf{TCPKE},A}(k) &= |\Pr[\neg\mathsf{AskG}] \cdot (\Pr[\mathbf{Exp}^{\text{m-is-cpa-0}}_{\mathsf{TCPKE},A}(k) = 1 | \neg\mathsf{AskG}] - \Pr[\mathbf{Exp}^{\text{m-is-cpa-1}}_{\mathsf{TCPKE},A}(k) = 1 | \neg\mathsf{AskG}])\\ &\quad + \Pr[\mathsf{AskG}] \cdot (\Pr[\mathbf{Exp}^{\text{m-is-cpa-0}}_{\mathsf{TCPKE},A}(k) = 1 | \mathsf{AskG}] - \Pr[\mathbf{Exp}^{\text{m-is-cpa-1}}_{\mathsf{TCPKE},A}(k) = 1 | \mathsf{AskG}])|\\ &\le \Pr[\mathsf{AskG}] \cdot |\Pr[\mathbf{Exp}^{\text{m-is-cpa-0}}_{\mathsf{TCPKE},A}(k) = 1 | \mathsf{AskG}] - \Pr[\mathbf{Exp}^{\text{m-is-cpa-1}}_{\mathsf{TCPKE},A}(k) = 1 | \mathsf{AskG}]|\\ &\le \Pr[\mathsf{AskG}].\end{aligned}$$

Finally, we estimate $\Pr[\mathsf{AskG}_{(i,j)}]$. The adversary A has two ways of evaluating G at $(\hat{x}^{(i,j)}, tk^*)$,

- by directly making a query $(\hat{x}^{(i,j)}, tk^*)$ to G, or,
- by making a query m to the token-embedded encryption oracle. If the answer is (c_1, c_2), and the random value used to compute (c_1, c_2) is $\hat{x}^{(i,j)}$, A can recover the random value $\hat{x}^{(i,j)}$ by using the secret key sk. Then the adversary gets the value $G(\hat{x}^{(i,j)}, tk^*) = c_2 \oplus H(\hat{x}^{(i,j)}, m)$ without making a query $(\hat{x}^{(i,j)}, tk^*)$ to G directly.

Thus, we have $\Pr[\mathsf{AskG}_{(i,j)}] \le (q_g + q_{te})/2^t$ for each $1 \le i \le q_e$ and $1 \le j \le n$. Therefore,

$$\mathbf{Adv}^{\text{m-is-cpa}}_{\mathsf{TCPKE},A}(k) \le \Pr[\mathsf{AskG}] \le \sum_{i=1}^{q_e}\sum_{j=1}^{n} \Pr[\mathsf{AskG}_{(i,j)}] \le \frac{nq_e(q_g + q_{te})}{2^t}.$$

□

From Theorems 1 and 2, the Galindo–Herranz scheme meets M-T1-CCA. Therefore, the Galindo–Herranz scheme meets our proposed four security notions in the multi-user setting.

6 Concluding Remarks

In this paper, we have formalized the security notions for token-controlled public-key encryption in the multi-user setting, by not simply modifying the previous security notions in [1] and [4], but employing the idea to formalize the attacks in the multi-user setting proposed by Bellare, Boldyreva, and Micali [2]. We have formalized three security notions in the multi-user setting, M-T1-CCA, M-T2-CCA, and M-IS-CPA, which corresponds to T1-CCA, T2-CCA, and IS-CPA in the single-user setting, respectively. Our security notions capture the possibility of an adversary seeing encryptions of related messages under the *same* token and *different* keys when the choice of the relation can be made by the adversary. We have also proposed the strong existential token unforgeability in the multi-user setting, M-SETUF.

We have shown the relationships between the previous and our proposed security notions. We have shown that M-T2-CCA does not imply M-T1-CCA and M-IS-CPA implies M-T1-CCA. We

have also shown the equivalence between T2-CCA and M-T2-CCA, and that between SETUF and M-SETUF. However, it is not clear whether T1-CCA implies M-T1-CCA or not, and whether IS-CPA implies M-IS-CPA or not.

We have also shown that the Galindo–Herranz scheme is secure in the multi-user setting, that is, the Galindo–Herranz scheme meets M-T1-CCA, M-T2-CCA, M-IS-CPA, and M-SETUF.

It might be interesting to consider whether T1-CCA implies M-T1-CCA or not, and whether IS-CPA implies M-IS-CPA or not.

References

[1] Baek, J., Safavi-Naini, R., and Susilo, W. Token-Controlled Public Key Encryption. In *Information Security Practice and Experience, First International Conference, ISPEC 2005* (Singapore, April 2005), R. H. Deng, F. Bao, H. Pang, and J. Zhou, Eds., vol. 3439 of *LNCS*, Springer-Verlag, pp. 386–397.

[2] Bellare, M., Boldyreva, A., and Micali, S. Public Key Encryption in a Multi-User Setting: Security Proofs and Improvements. In *Advances in Cryptology – EUROCRYPT 2000* (Bruges, Belgium, May 2000), B. Preneel, Ed., vol. 1807 of *LNCS*, Springer-Verlag, pp. 259–274.

[3] 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.

[4] Galindo, D., and Herranz, J. A Generic Construction for Token-Controlled Public Key Encryption. In *Financial Cryptography – FC 2006* (Anguilla, British West Indies, February 2006), G. Di Crescenzo and A. Rubin, Eds., vol. 4107 of *LNCS*, Springer-Verlag, pp. 177–190.

[5] May, T. Timed-Release Crypto. manuscript, 1993.

[6] Rivest, R. L., Shamir, A., and Wagner, D. A. Time-lock puzzles and timed-release crypto. Technical Report MIT/LCS/TR-684, Massachusetts Institute of Technology, 1996. Online available at `http://theory.lcs.mit.edu/ rivest/RivestShamirWagner-timelock.ps`.

A The Previously Proposed Security Notions of Token-Controlled Public-Key Encryption

In this section, we review the security notions, T1-CCA, T2-CCA, IS-CPA, and SETUF, of token-controlled public-key encryption in the single-user setting proposed in [1] and [4]. We also review the the security notion M-T2-CCA-GH proposed in [4]. This seems to be considered as the multi-user version of T2-CCA.

A.1 T1-CCA

First, we consider the security notions against the outside attackers. These security notions capture the property that, given a ciphertext (and a token), the person who does not have a secret key cannot get any information about the plaintext underlying the ciphertext.

We can consider two kinds of outside attackers, "type-1" attackers who hold neither a secret-key nor a token, and "type-2" attackers who does not have a secret-key but has a token. Note that since there are some restrictions with respect to the oracle queries for the type-1 attackers, while there is no such a restriction for the type-2 attackers.

We review a security notion against the type-1 outside attackers in [1], which we call the indistinguishability against type1 outside chosen-ciphertext attacks (T1-CCA).

Definition 9 (T1-CCA). *Let* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *be a token-controlled public-key encryption scheme. Let* $b \in \{0,1\}$ *and* $k \in \mathbb{N}$. *Let* $A = (A_1, A_2)$ *be an adversary that runs in two stages. Note that* si *is the state information. It contains* pk, m_0, m_1, *and so on. We consider the following experiment:*

$$
\begin{array}{l}
\texttt{Experiment } \mathbf{Exp}^{\text{t1-cca-}b}_{\mathsf{TCPKE},A}(k) \\
\quad (pk, sk) \leftarrow \mathsf{GK}(1^k);\ tk^* \leftarrow \mathsf{GT}(1^k) \\
\quad (m_0, m_1, \mathsf{si}) \leftarrow A_1^{\mathcal{O}_{\text{t1-cca}}}(pk) \\
\quad c \leftarrow \mathsf{E}_{pk}(tk^*, m_b) \\
\quad d \leftarrow A_2^{\mathcal{O}_{\text{t1-cca}}}(c, \mathsf{si}) \\
\quad \texttt{return } d
\end{array}
$$

where $m_0, m_1 \in \mathcal{P}_{pk}$ *and* $\mathcal{O}_{\text{t1-cca}} = \{\mathsf{E}_{pk}(tk^*, \cdot), \mathsf{D}_{sk}(\cdot,\cdot)\}$. *That is, the adversary can make access to the token-embedded encryption oracle* $\mathsf{E}_{pk}(tk^*, \cdot)$. *The adversary can also make access to the decryption oracle* $\mathsf{D}_{sk}(\cdot,\cdot)$, *which takes a token* tk *and a ciphertext* c, *and returns the corresponding plaintext* m *or* $\perp$.

We define the advantage via

$$\mathbf{Adv}^{\text{t1-cca}}_{\mathsf{TCPKE},A}(k) = \left|\Pr[\mathbf{Exp}^{\text{t1-cca-0}}_{\mathsf{TCPKE},A}(k) = 1] - \Pr[\mathbf{Exp}^{\text{t1-cca-1}}_{\mathsf{TCPKE},A}(k) = 1]\right|.$$

We say that a token-controlled public-key encryption scheme TCPKE *meets T1-CCA if* $\mathbf{Adv}^{\text{t1-cca}}_{\mathsf{TCPKE},A}(k)$ *is negligible for any polynomial-time adversary* A.

A.2 T2-CCA

Next, we review a security notion against the type-2 outside attackers in [1], which we call the indistinguishability against type2 outside chosen-ciphertext attacks (T2-CCA). Note that, in the following definition, the adversary gets not only the public key but also the token.

Definition 10 (T2-CCA). *Let* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *be a token-controlled public-key encryption scheme. Let* $b \in \{0,1\}$ *and* $k \in \mathbb{N}$. *Let* $A = (A_1, A_2)$ *be an adversary that runs in two stages. We consider the following experiment:*

$$
\begin{array}{l}
\texttt{Experiment } \mathbf{Exp}^{\text{t2-cca-}b}_{\mathsf{TCPKE},A}(k) \\
\quad (pk, sk) \leftarrow \mathsf{GK}(1^k);\ tk^* \leftarrow \mathsf{GT}(1^k) \\
\quad (m_0, m_1, \mathsf{si}) \leftarrow A_1^{\mathcal{O}_{\text{t2-cca}}}(pk, tk^*) \\
\quad c \leftarrow \mathsf{E}_{pk}(tk^*, m_b) \\
\quad d \leftarrow A_2^{\mathcal{O}_{\text{t2-cca}}}(c, \mathsf{si}) \\
\quad \texttt{return } d
\end{array}
$$

where $m_0, m_1 \in \mathcal{P}_{pk}$ *and* $\mathcal{O}_{\text{t2-cca}} = \{\mathsf{D}_{sk}(\cdot,\cdot)\}$. *That is, the adversary can make access to the decryption oracle* $\mathsf{D}_{sk}(\cdot,\cdot)$. *However, the adversary cannot ask the pair* (tk^*, c) *to the decryption oracle.*

We define the advantage via

$$\mathbf{Adv}^{\text{t2-cca}}_{\mathsf{TCPKE},A}(k) = \left|\Pr[\mathbf{Exp}^{\text{t2-cca-0}}_{\mathsf{TCPKE},A}(k) = 1] - \Pr[\mathbf{Exp}^{\text{t2-cca-1}}_{\mathsf{TCPKE},A}(k) = 1]\right|.$$

We say that a token-controlled public-key encryption scheme TCPKE *meets T2-CCA if* $\mathbf{Adv}^{\text{t2-cca}}_{\mathsf{TCPKE},A}(k)$ *is negligible for any polynomial-time adversary* A.

A.3 M-T2-CCA-GH

In [4], Galindo and Herranz proposed a security notion of the indistinguishability against type-2 outside chosen ciphertext attacks which is different from T2-CCA (in the single-user setting) by Baek, Safavi-Naini, and Susilo. Their formalization, which we call M-T2-CCA-GH, seems to consider a multi-user setting. We review the the security notion M-T2-CCA-GH proposed in [4].

Definition 11 (M-T2-CCA-GH). *Let* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *be a token-controlled public-key encryption scheme. Let* $b \in \{0,1\}$ *and* $k \in \mathbb{N}$. *Let* $A = (A_1, A_2)$ *be an adversary that runs in two stages. We consider the following experiment:*

$$
\begin{array}{l}
\texttt{Experiment } \mathbf{Exp}^{\text{m-t2-cca-gh-}b}_{\mathsf{TCPKE},A}(k) \\
\quad (pk_i, sk_i) \leftarrow \mathsf{GK}(1^k) \ \ \texttt{for } i = 1, \ldots, n \\
\quad tk^* \leftarrow \mathsf{GT}(1^k) \\
\quad (m_0, m_1, \mathsf{si}) \leftarrow A_1^{\mathcal{O}_{\text{m-t2-cca-gh}}}(pk, tk^*) \\
\quad c_i \leftarrow \mathsf{E}_{pk}(tk^*, m_b) \ \ \texttt{for } i = 1, \ldots, n \\
\quad d \leftarrow A_2^{\mathcal{O}_{\text{m-t2-cca-gh}}}(c_1, \ldots, c_n, \mathsf{si}) \\
\quad \texttt{return } d
\end{array}
$$

where $m_0, m_1 \in \bigcap_{1 \le i \le n} \mathcal{P}_{pk_i}$ *and* $\mathcal{O}_{\text{m-t2-cca-gh}} = \{\mathsf{D}_{sk_i}(\cdot,\cdot)\}_{1 \le i \le n}$. *That is, the adversary can make access to the decryption oracle* $\mathsf{D}_{sk_i}(\cdot,\cdot)$ *for* $i = 1, \ldots, n$. *However, for* $i = 1, \ldots, n$, *the adversary cannot ask the pair* (c_i, tk^*) *to the decryption oracle* D_{sk_i}.

We define the advantage via

$$\mathbf{Adv}^{\text{m-t2-cca-gh}}_{\mathsf{TCPKE},A}(k) = \Big|\Pr[\mathbf{Exp}^{\text{m-t2-cca-gh-0}}_{\mathsf{TCPKE},A}(k) = 1] - \Pr[\mathbf{Exp}^{\text{m-t2-cca-gh-1}}_{\mathsf{TCPKE},A}(k) = 1]\Big|.$$

We say that a token-controlled public-key encryption scheme TCPKE *meets M-T2-CCA-GH if the function* $\mathbf{Adv}^{\text{m-t2-cca-gh}}_{\mathsf{TCPKE},A}(k)$ *is negligible for any polynomial-time adversary A.*

A.4 IS-CPA

Next, we consider the security notion against the inside attackers. This security notion captures the property that, if the token is not revealed, given a ciphertext, not only the person who does not have a secret key but also the secret-key holder cannot get any information about the plaintext underlying the ciphertext.

We review a security notion against the inside attackers in [1], which we call the indistinguishability against inside chosen-plaintext attacks (IS-CPA). Note that, in the following definition, the adversary gets the public key and the corresponding secret key, while the adversary does not get the token.

Definition 12 (IS-CPA). *Let* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *be a token-controlled public-key encryption scheme. Let* $b \in \{0,1\}$ *and* $k \in \mathbb{N}$. *Let* $A = (A_1, A_2)$ *be an adversary that runs in two stages. We consider the following experiment:*

$$
\begin{array}{l}
\texttt{Experiment } \mathbf{Exp}^{\text{is-cpa-}b}_{\mathsf{TCPKE},A}(k) \\
\quad (pk, sk) \leftarrow \mathsf{GK}(1^k);\ tk^* \leftarrow \mathsf{GT}(1^k) \\
\quad (m_0, m_1, \mathsf{si}) \leftarrow A_1^{\mathcal{O}_{\text{is-cpa}}}(pk, sk) \\
\quad c \leftarrow \mathsf{E}_{pk}(tk^*, m_b) \\
\quad d \leftarrow A_2^{\mathcal{O}_{\text{is-cpa}}}(c, \mathsf{si}) \\
\quad \texttt{return } d
\end{array}
$$

where $m_0, m_1 \in \mathcal{P}_{pk}$ *and* $\mathcal{O}_{\text{is-cpa}} = \{\mathsf{E}_{pk}(tk^*,\cdot)\}$. *That is, the adversary can make access to the token-embedded encryption oracle* $\mathsf{E}_{pk}(tk^*,\cdot)$, *which takes a plaintext* $m \in \mathcal{P}_{pk}$ *and returns a ciphertext* c *of* m *under the public-key* pk *and the token* tk^* *(i.e.* $c = \mathsf{E}_{pk}(tk^*, m)$*).*

We define the advantage via

$$\mathbf{Adv}^{\text{is-cpa}}_{\mathsf{TCPKE},A}(k) = \Big|\Pr[\mathbf{Exp}^{\text{is-cpa-0}}_{\mathsf{TCPKE},A}(k) = 1] - \Pr[\mathbf{Exp}^{\text{is-cpa-1}}_{\mathsf{TCPKE},A}(k) = 1]\Big|.$$

We say that a token-controlled public-key encryption scheme TCPKE *meets IS-CPA if* $\mathbf{Adv}^{\text{is-cpa}}_{\mathsf{TCPKE},A}(k)$ *is negligible for any polynomial-time adversary A.*

A.5 SETUF

In [4], Galindo and Herranz proposed a new security notion for token-controlled public-key encryption, called the strong existential token unforgeability. This security notion captures the property that anyone cannot produce one ciphertext c and two tokens tk_0, tk_1 such that two pairs, (c, tk_0) and (c, tk_1), are valid, and the two corresponding plaintexts are different. Galindo and Herranz also showed that the scheme proposed in [1] does not satisfy this security notion.

We review the strong existential token unforgeability (SETUF) in [4].

Definition 13 (SETUF)**.** *Let* $\mathsf{TCPKE} = (\mathsf{GK}, \mathsf{GT}, \mathsf{E}, \mathsf{D})$ *be a token-controlled public-key encryption scheme. Let* $k \in \mathbb{N}$ *be a security parameter, and* A *an adversary. We consider the following experiment:*

$$
\begin{array}{l}
\texttt{Experiment } \mathbf{Exp}^{\mathrm{setuf}}_{\mathsf{TCPKE},A}(k) \\
\quad (pk, sk) \leftarrow \mathsf{GT}(1^k) \\
\quad (c, tk, tk') \leftarrow A^{\mathcal{O}_{\mathrm{setuf}}}(pk) \\
\quad \texttt{if } ((tk \notin \mathcal{T}_k) \vee (tk' \notin \mathcal{T}_k)) \texttt{ then return } 0 \\
\quad m \leftarrow \mathsf{D}_{sk}(tk, c);\ m' \leftarrow \mathsf{D}_{sk}(tk', c) \\
\quad \texttt{if } ((m \neq \perp) \wedge (m' \neq \perp) \wedge (m \neq m')) \\
\quad \texttt{then return } 1 \texttt{ else return } 0
\end{array}
$$

where $\mathcal{O}_{\mathrm{setuf}} = \{\mathsf{D}_{sk}(\cdot, \cdot)\}$*. That is, the adversary can make access to the decryption oracle* $\mathsf{D}_{sk}(\cdot, \cdot)$*.*

We define the advantage via

$$\mathbf{Adv}^{\mathrm{setuf}}_{\mathsf{TCPKE},A}(k) = \Pr[\mathbf{Exp}^{\mathrm{setuf}}_{\mathsf{TCPKE},A}(k) = 1].$$

We say that a token-controlled public-key encryption scheme TCPKE *meets SETUF if* $\mathbf{Adv}^{\mathrm{setuf}}_{\mathsf{TCPKE},A}(k)$ *is negligible for any polynomial-time adversary* A*.*