On Multi-Key FuncCPA Secure Encryption Schemes

Eri Nakajima
Department of Information and Computer Sciences
Osaka University
Osaka, Japan
e-nakajima@ist.osaka-u.ac.jp

Keisuke Hara
Cyber Physical Security Research Center
National Institute of Advanced Industrial Science and Technology
Tokyo, Japan
Yokohama National University
Kanagawa, Japan
0000-0003-3598-0988

Kyosuke Yamashita
Department of Information and Computer Sciences
Osaka University
Osaka, Japan
0000-0001-7998-8039

***Abstract*—The notion of funcCPA security for homomorphic encryption schemes was introduced by Akavia *et al.* (TCC 2022). Whereas it aims to capture the bootstrapping technique in homomorphic encryption schemes, Dodis *et al.* (TCC 2023) pointed out that funcCPA security can also be applied to non-homomorphic public-key encryption schemes (PKE). As an example, they presented a use case for privacy-preserving outsourced computation without homomorphic computation. It should be noted that prior work on funcCPA security, including the use case presented by Dodis *et al.*, considered only the single-key setting. However, in recent years, multi-party collaboration in outsourced computation has garnered significant attention, making it desirable for funcCPA security to support the multi-key setting. Therefore, in this work, we introduce a new notion of security called Multi-Key funcCPA (MKfunc) to address this need, and show that if a PKE scheme is KDM-secure, then it is also MKfuncCPA secure. Furthermore, we show that similar discussions can be applied to symmetric-key encryption.**

***Index Terms*—public-key encryption, symmetric-key encryption, functional re-encryption security (funcCPA security), key-dependent message (KDM) security**

I. Introduction

The fundamental security notions for public-key encryption (PKE) scheme include chosen plaintext attack (CPA) security and chosen ciphertext attack (CCA) security. These are widely accepted as they cover many scenarios for PKE. However, they do not encompass all scenarios. For example, Key-Dependent Message (KDM) security [1], [2] ensures confidentiality even if an adversary can observe ciphertexts of messages that depend on the secret keys. CPA security and CCA security do not assume that an adversary can obtain ciphertexts related to the secret keys, but there are real-world scenarios where ciphertexts of the secret keys are embedded in hardware [3]. Therefore, considering the importance of PKE, it is crucial to also address security notions that capture situations beyond what CPA security and CCA security cover.

One such security notion, funcCPA security, was recently introduced by Akavia *et al.* [4]. It was proposed in the context of bootstrapping techniques [5] for homomorphic encryption schemes, specifically addressing scenarios where an adversary can access an entity that responds to a queried ciphertext with a fresh re-encrypted ciphertext. The fundamental security notions for PKE do not consider such entities. While funcCPA security was proposed to capture the bootstrapping technique in homomorphic encryption schemes, Dodis *et al.* [6] pointed out that it can be applied to non-homomorphic PKE schemes as well. They further demonstrated the relationships between funcCPA security and existing security notions.

To consider funcCPA security for standard PKE schemes, Dodis *et al.* presented the following use case of privacy-preserving outsourced computation using a "secure enclave." An analyst seeks to analyse clients' personal data and solicits their data. The analysis is performed on a server that has access to a secure enclave as follows. The analyst generates a public-secret key pair and sends the secret key to the secure enclave. Multiple clients encrypt their own data under the analyst's public key and send them to the server. The server collects the data and, at the request of the analyst, asks the enclave to perform computations on the encrypted data. The enclave decrypts the data, performs the required computation, encrypts the result, and returns it to the server. When the computations are complete, the server forwards the encrypted result to the analyst. In this use case, what the analyst obtains is fresh ciphertexts of the computed results, and this is precisely the kind of scenario that funcCPA security considers.

Existing works addressing funcCPA security [4], [6] have only considered it in a single-key setting. However, in the above-mentioned use case, it is natural to consider the presence of multiple analysts, as recently there has been a significant demand for data collaboration between companies. Figure 1 illustrates the use case in such a scenario. There are mul-

tiple analysts (i.e. the organization A and B in Figure 1), each of whom generates a public-secret key pair (denoted as $(\mathsf{pk}_\mathsf{A}, \mathsf{sk}_\mathsf{A})$ and $(\mathsf{pk}_\mathsf{B}, \mathsf{sk}_\mathsf{B})$ for organizations A and B, respectively). Each analyst sends its secret key to the secure enclave. Clients use the public key of the analyst that they believe (i.e. either pk_A or pk_B) to encrypt their data and send it to the server. When one of the analysts (the organization A in Figure 1) requests some computation on data that is stored on the server, the analyst first sends the desired function (the function f in Figure 1) to the server. Then, the server forwards this request along with the index of the requesting analyst to the secure enclave. Although the encrypted data from the clients may not necessarily be encrypted under the public key of the requesting analyst, the secure enclave retains each analyst's secret key and can decrypt the data using the corresponding secret key. Then, similarly to the previous example, the computation is performed, the result is encrypted with the public key of the requesting analyst, and sent back to the server.

Considering the above multi-clients use case, it is desirable for funcCPA security to support multi-key settings. However, to the best of our knowledge, funcCPA security in the multi-key setting has not been discussed previously. Furthermore, although prior work only considered funcCPA security in the context of standard PKE schemes, the above-mentioned use case is also applicable to symmetric-key encryption.

In this work, we introduce a new notion of Multi-Key funcCPA (MKfunc) security, extending funcCPA security to support multi-key settings for both public-key and symmetric-key encryption schemes. We emphasize that our definition captures the aforementioned multi-analysts scenario. We also demonstrate that if a PKE scheme is KDM secure, then it is also MKfuncCPA secure. By defining MKfuncCPA security, we can discuss the security of encryption schemes in the context of multi-party collaboration for outsourced computation, a topic that has recently garnered significant attention.

We remark that this article aims to extend the funcCPA security to the multi-user settings. Although reducing MK-funcCPA security to KDM-CPA security may seem somewhat straightforward, there is no denying the possibility of achieving MKfuncCPA from weaker security notions such as IND-CCA security.

A. Related Work

FuncCPA security was introduced by Akavia *et al.* [4] in the context of homomorphic encryption, and afterwards, Dodis *et al.* [6] pointed out that it can also be applied to non-homomorphic public-key encryption. Dodis *et al.* specifically proposed funcCPA$^+$ security and proved that it implies func-CPA security, whereas the opposite was not proved. Later, Shinozaki *et al.* [7] demonstrated that PKE schemes that are funcCPA secure for functions with two or more inputs also meet funcCPA$^+$ security. Nuida [8] considered the problem of querying invalid ciphertexts in the funcCPA game.

KDM security encompasses various types depending on the supported function class, including circular security [2], projection-KDM security [3], bounded-KDM security [9], and full-KDM security, among others. Waters *et al.* [10] showed how to upgrade single-key KDM-secure PKE to multi-key KDM-secure PKE using garbled circuits [11].

II. Preliminaries

In this section, we present the notations and definitions used throughout this paper, including public-key encryption (PKE) schemes, symmetric-key encryption (SKE) schemes, and key-dependent message (KDM) security for both PKE and SKE.

We denote the security parameter by $\lambda \in \mathbb{N}$, polynomial functions by $\mathsf{poly}()$, and negligible functions by $\mathsf{negl}()$. For any $n \in \mathbb{N}$, define $[n] = \{1, 2, \ldots, n\}$. Any algorithm is given the security parameter 1^λ but we omit it when clear from context. We denote the message space of each encryption scheme by $\mathcal{M}$. Probabilistic polynomial time is abbreviated as PPT.

A public-key encryption (PKE) scheme is defined by the following syntax and correctness requirement.

Definition 1 (Public-key encryption (PKE) scheme)**.** *A public-key encryption (PKE) scheme* Π *consists of the three algorithms* $(\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *that operate as follows:*

- $\mathsf{KG}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$ *:* KG *is a PPT algorithm that takes the security parameter* 1^λ *as input and outputs a public-secret key pair* $(\mathsf{pk}, \mathsf{sk})$.
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}) \to c$ *:* Enc *is a PPT encryption algorithm that takes a public key* pk *and a message* $\mathsf{m} \in \mathcal{M}$ *as input and outputs a ciphertext* c.
- $\mathsf{Dec}(\mathsf{sk}, c) = \mathsf{m}$ *:* Dec *is a deterministic decryption algorithm that takes a secret key* sk *and a ciphertext* c *as input and outputs a message* $\mathsf{m} \in \{\perp\} \cup \mathcal{M}$.

Definition 2 (Correctness of a PKE scheme)**.** *A PKE scheme* Π *is correct if for every security parameter* $\lambda \in \mathbb{N}$*, every message* $\mathsf{m} \in \mathcal{M}$ *and every* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}(1^\lambda)$*,* $\Pr[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, \mathsf{m})) = \mathsf{m}] = 1$.

We introduce the Key-dependent message (KDM) security for PKE schemes by Kitagawa and Matsuda [12] as follows.

Definition 3 (Key-dependent message (KDM) security for a PKE scheme)**.** *Let* $\Pi = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a PKE scheme,* $\mathcal{F}$ *be a function family. The PKE scheme* Π *is KDM-CPA secure if for every sufficiently large security parameter* λ*, all PPT adversaries* $\mathcal{A}$*, and a function class* $\mathcal{F}$*, it holds that* $|\Pr[\mathsf{ExpPKEKDM}_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda) = 1] - 1/2| \leq \mathsf{negl}(\lambda)$ *where* $\mathsf{ExpPKEKDM}_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda)$ *is the experiment defined as follows.*

$\mathsf{ExpPKEKDM}_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda)$

$b \leftarrow \{0,1\}$; $(\mathsf{pk}^j, \mathsf{sk}^j) \leftarrow \mathsf{KG}(1^\lambda)$ $(j = 1, ..., l)$;

$b' \leftarrow \mathcal{A}^{\mathsf{O}^b_{\mathsf{KDM}}}(\mathsf{pk}^1, \ldots, \mathsf{pk}^l)$:

output 1 if $b' = b$ otherwise 0

The oracle $\mathsf{O}^b_{\mathsf{KDM}}$ *takes an index* $j^* \in [l]$ *and a function* $f \in \mathcal{F}$ *as input and operates as follows.*

- $\mathsf{O}^1_{\mathsf{KDM}}$ *returns* $c^* \leftarrow \mathsf{Enc}(\mathsf{pk}^{j^*}, f(\mathsf{sk}^1, \ldots, \mathsf{sk}^l))$.
- $\mathsf{O}^0_{\mathsf{KDM}}$ *returns* $c^* \leftarrow \mathsf{Enc}(\mathsf{pk}^{j^*}, 0^{|f(\mathsf{sk}^1, \ldots, \mathsf{sk}^l)|})$.

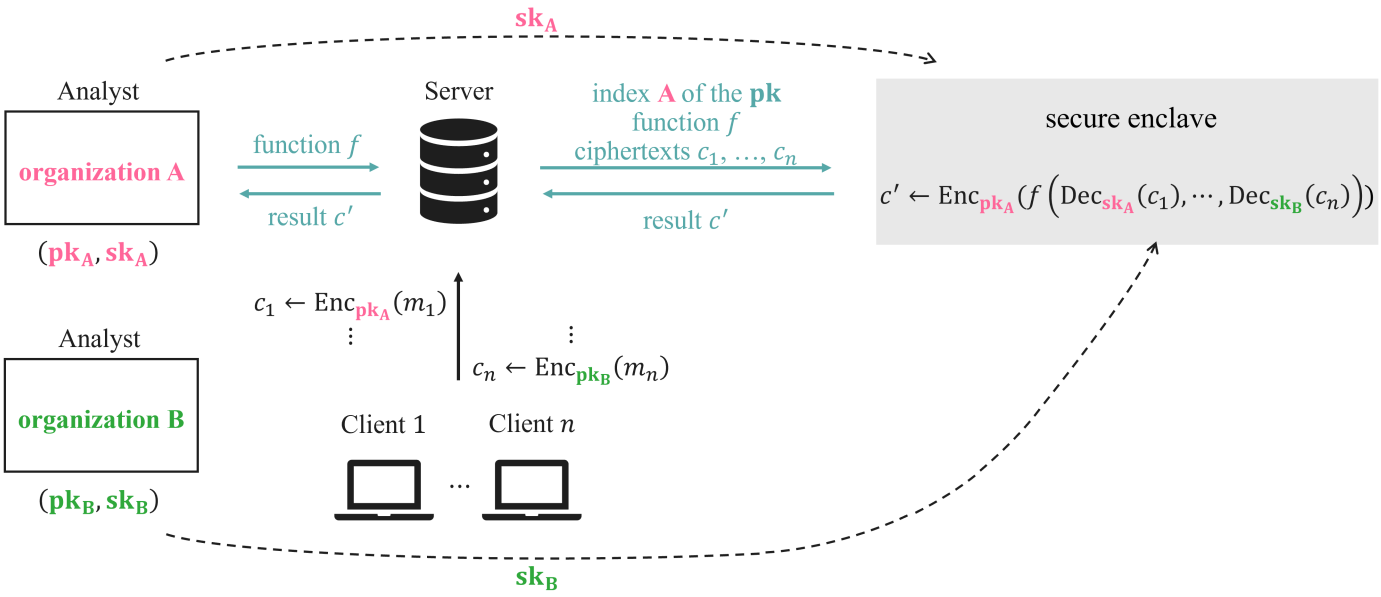

Fig. 1. Our proposed use case of multi-party collaboration in outsourced computation using a "secure enclave."

We denote the advantage of the adversary in $\mathsf{ExpPKEKDM}_{\Pi,\mathcal{A},\mathcal{F}}$ by $Adv^{\mathsf{KDMPKE}}_{\Pi,\mathcal{A},\mathcal{F}}$.

A symmetric-key encryption (SKE) scheme is defined by the following syntax and correctness requirement.

Definition 4 (Symmetric-key encryption (SKE) scheme)**.** *An SKE scheme E consists of the three algorithms* $(\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *that operate as follows:*

- $\mathsf{KG}(1^\lambda) \to \mathsf{sk}$ *: KG is a PPT algorithm that takes the security parameter 1^λ as input and outputs a key* sk.
- $\mathsf{Enc}(\mathsf{sk}, \mathsf{m}) \to c$ *: Enc is a PPT encryption algorithm that takes a key* sk *and a message* $\mathsf{m} \in \mathcal{M}$ *as input and outputs a ciphertext c.*
- $\mathsf{Dec}(\mathsf{sk}, c) = \mathsf{m}$ *: Dec is a deterministic decryption algorithm that takes a key* sk *and a ciphertext c as input and outputs a message* $\mathsf{m} \in \{\perp\} \cup \mathcal{M}$.

Definition 5 (Correctness of an SKE scheme)**.** *An SKE scheme E is correct if for every security parameter $\lambda \in \mathbb{N}$, every message $\mathsf{m} \in \mathcal{M}$ and every $\mathsf{sk} \leftarrow \mathsf{KG}(1^\lambda)$,* $\Pr[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{sk}, \mathsf{m})) = \mathsf{m}] = 1$.

We define the Key-dependent message (KDM) security for an SKE scheme as follows.

Definition 6 (Key-dependent message (KDM) security for an SKE scheme)**.** *Let $E = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ be an SKE scheme and $\mathcal{F}$ be a function family. The SKE scheme E is KDM-CPA secure if for every sufficiently large security parameter λ, all PPT adversaries $\mathcal{A}$, and a function class $\mathcal{F}$, it holds that* $|\Pr[\mathsf{ExpSKEKDM}_{E,\mathcal{A},\mathcal{F}}(1^\lambda) = 1] - 1/2| \leq \mathsf{negl}(\lambda)$ *where $\mathsf{ExpSKEKDM}_{E,\mathcal{A},\mathcal{F}}(1^\lambda)$ is the experiment that is defined as follows.*

$\mathsf{ExpSKEKDM}_{E,\mathcal{A},\mathcal{F}}(1^\lambda)$

$b \leftarrow \{0,1\}; \mathsf{sk}^j \leftarrow \mathsf{KG}(1^\lambda)\ (j = 1, ..., l);$

$b' \leftarrow \mathcal{A}^{\mathsf{O}^b_{\mathsf{KDM}}}(1^\lambda)$:

output 1 if $b' = b$ otherwise 0

The oracle $\mathsf{O}^b_{\mathsf{KDM}}$ takes an index $j^* \in [l]$ and a function $f \in \mathcal{F}$ as input and operates as follows.

- $\mathsf{O}^1_{\mathsf{KDM}}$ *returns* $c^* \leftarrow \mathsf{Enc}(\mathsf{sk}^{j^*}, f(\mathsf{sk}^1, \ldots, \mathsf{sk}^l))$.
- $\mathsf{O}^0_{\mathsf{KDM}}$ *returns* $c^* \leftarrow \mathsf{Enc}(\mathsf{sk}^{j^*}, 0^{|f(\mathsf{sk}^1, \ldots, \mathsf{sk}^l)|})$.

We denote the advantage of the adversary in $\mathsf{ExpSKEKDM}_{E,\mathcal{A},\mathcal{F}}$ by $Adv^{\mathsf{KDMSKE}}_{E,\mathcal{A},\mathcal{F}}$.

In this paper, we do not treat the (single-key) funcCPA security. However, we introduce funcCPA security (and funcCPA$^+$ security) in appendix for reference.

III. Multi-Key FuncCPA Security for PKE

In this section, we define the notion of Multi-Key funcCPA (MKfunc) security and show that if a PKE scheme is KDM secure, then it is also MKfuncCPA secure. We remark that the definition of MKfuncCPA is similar to that of funcCPA$^+$ rather than funcCPA. We argue that such a formalization would be justified because it is known that funcCPA$^+$ security implies funcCPA security [7].

A. Definition of Multi-Key funcCPA (MKfunc) Security

We define the concept of MKfuncCPA security. MKfuncCPA security is defined by providing the adversaries with the following oracle. The adversaries have access to an oracle that, given a query consisting of an index $j^* \in [l]$ of the public key for re-encryption, pairs of ciphertexts and the indices of the corresponding public keys $\{c_i, j_i\}_{i\in[n], j_i\in[l]}$, and a function f,

returns $\mathsf{Enc}(\mathsf{pk}^{j^*}, f(\mathsf{Dec}(\mathsf{sk}^{j_1}, c_1), \ldots, \mathsf{Dec}(\mathsf{sk}^{j_n}, c_n)))$. The formal definition is as below.

Definition 7 (Multi-Key FuncCPA Security for PKE)**.** *Let* $\Pi = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a PKE scheme, and let* $\mathcal{F} = \{f : (\mathcal{M} \cup \{\perp\})^n \to \mathcal{M} | n \in \mathbb{N}\}$ *be a function family. The scheme* Π *is said to be Multi-Key funcCPA (MKfuncCPA) secure for the function family* $\mathcal{F}$ *if, for every sufficiently large security parameter* λ*, every PPT adversary* $\mathcal{A}$*, and the function family* $\mathcal{F}$*, it holds that* $|\Pr[\mathsf{ExpMKfuncPKE}_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda) = 1] - 1/2| \leq \mathsf{negl}(\lambda)$ *where* $\mathsf{ExpMKfuncPKE}_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda)$ *is the experiment defined as follows.*

$\mathsf{ExpMKfuncPKE}_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda)$
$b \leftarrow \{0,1\}; (\mathsf{pk}^j, \mathsf{sk}^j) \leftarrow \mathsf{KG}(1^\lambda)\ (j = 1, ..., l);$
$b' \leftarrow \mathcal{A}^{\mathsf{O}^b_{\mathsf{ReEnc}}}(\mathsf{pk}^1, \ldots, \mathsf{pk}^l)$:
output 1 if $b' = b$ otherwise 0

The oracle $\mathsf{O}^b_{\mathsf{ReEnc}}$ *takes an index* $j^* \in [l]$*, pairs of ciphertexts along with the indices of the corresponding public keys* $\{c_i, j_i\}_{i\in[n], j_i\in[l]}$*, and a function* $f \in \mathcal{F}$ *as input and operates as follows.*

- $\mathsf{O}^1_{\mathsf{ReEnc}}$ *returns* $c^* \leftarrow \mathsf{Enc}(\mathsf{pk}^{j^*}, f(\mathsf{Dec}(\mathsf{sk}^{j_1}, c_1), \ldots, \mathsf{Dec}(\mathsf{sk}^{j_n}, c_n)))$.
- $\mathsf{O}^0_{\mathsf{ReEnc}}$ *returns* $c^* \leftarrow \mathsf{Enc}(\mathsf{pk}^{j^*}, 0^{|f(\mathsf{Dec}(\mathsf{sk}^{j_1}, c_1), \ldots, \mathsf{Dec}(\mathsf{sk}^{j_n}, c_n))|})$.

We denote the advantage of the adversary in $\mathsf{ExpMKfuncPKE}_{\Pi,\mathcal{A},\mathcal{F}}$ by $Adv^{\mathsf{MKfuncPKE}}_{\Pi,\mathcal{A},\mathcal{F}}$. Note that if we restrict $l = 1$, then the above game corresponds to that of funcCPA$^+$ security (for the formal definition of funcCPA$^+$ security, see appendix).

B. KDM Security Implies MKfuncCPA Security

We demonstrate that if a PKE scheme Π_{KDM} is KDM secure, then it is also MKfuncCPA secure. Note that, in this paper, we focus on KDM security with respect to bounded circuits as the function family. This type of KDM security is referred to as bounded-KDM security. Applebaum [13] and Kitagawa and Matsuda [12] have each shown that bounded-KDM security can be achieved by transforming schemes that satisfy (more basic) projection-KDM security or circular security. Therefore, we assume that Π_{KDM} is bounded-KDM secure, but this is not a tight restriction on our result.

To achieve our goal, we assume the existence of a PPT adversary $\mathcal{A}$ that can break MKfuncCPA security of Π_{KDM} with non-negligible probability. We then show that such an adversary $\mathcal{A}$ can be used to construct a PPT reduction algorithm (i.e., another adversary) $\mathcal{B}$ that can break KDM security of Π_{KDM} with non-negligible probability.

To construct this reduction algorithm, it is necessary to properly simulate the oracle for the adversary $\mathcal{A}$ against MKfuncCPA security. In this simulation, the KDM security oracle can be used. However, the KDM security oracle cannot be queried with pairs of ciphertexts and the indices of the corresponding public keys $\{c_i, j_i\}_{i\in[n], j_i\in[l]}$ that are part of the MKfuncCPA security oracle query. Therefore, we introduce a new function f' and embed the pairs $\{c_i, j_i\}_{i\in[n], j_i\in[l]}$ into this function f'. Concretely, given an oracle query $(j^*, \{c_i, j_i\}_{i\in[n], j_i\in[l]}, f)$ from the adversary $\mathcal{A}$, the adversary $\mathcal{B}$ defines the function f' as follows: $f'(\mathsf{sk}^1, \ldots, \mathsf{sk}^l) := f(\mathsf{Dec}(\mathsf{sk}^{j_1}, c_1), \ldots, \mathsf{Dec}(\mathsf{sk}^{j_n}, c_n))$. Then, the adversary $\mathcal{B}$ queries the challenger with (j^*, f') and returns the result as the response to the adversary $\mathcal{A}$. This approach enables the simulation of the oracle for an adversary $\mathcal{A}$ against MKfuncCPA security.

Lemma 1. *If a PKE scheme* Π_{KDM} *satisfies bounded-KDM security against CPA attacks, then* Π_{KDM} *is also MKfuncCPA secure.*

Proof. We assume for contradiction the existence of a PPT adversary $\mathcal{A}$ that can break MKfuncCPA security of Π_{KDM} with non-negligible probability. We then show that there exists a PPT reduction algorithm $\mathcal{B}$ that breaks the KDM-CPA security of Π_{KDM} with non-negligible probability with accessing to $\mathcal{A}$. In the experiment $\mathsf{ExpPKEKDM}_{\Pi_{\mathrm{KDM}},\mathcal{B}^{\mathcal{A}},\mathcal{F}}$, the reduction algorithm $\mathcal{B}^{\mathcal{A}}$ operates as follows, simulating the experiment $\mathsf{ExpMKfuncPKE}_{\Pi_{\mathrm{KDM}},\mathcal{A},\mathcal{F}^*}$.

Setup phase: The reduction algorithm $\mathcal{B}$ receives the set of public keys $(\mathsf{pk}^1, \ldots, \mathsf{pk}^l)$ from the challenger and provides these public keys as input to the adversary $\mathcal{A}$.

Oracle simulation: When the adversary $\mathcal{A}$ makes oracle queries during its execution, $\mathcal{B}$ simulates the oracle $\mathsf{O}_{\mathsf{ReEnc}}$ as follows. Given an index $j^* \in [l]$ for the public key to be used in re-encryption, pairs of ciphertexts and the indices of the corresponding public keys $\{c_i, j_i\}_{i\in[n], j_i\in[l]}$, and a function $f \in \mathcal{F}^*$ from $\mathcal{A}$, $\mathcal{B}$ defines $f'(\mathsf{sk}^1, \ldots, \mathsf{sk}^l) := f(\mathsf{Dec}(\mathsf{sk}^{j_1}, c_1), \ldots, \mathsf{Dec}(\mathsf{sk}^{j_n}, c_n))$. Next, $\mathcal{B}$ queries (j^*, f') to $\mathsf{O}_{\mathsf{KDM}}$ in the experiment $\mathsf{ExpPKEKDM}_{\Pi_{\mathrm{KDM}},\mathcal{B}^{\mathcal{A}},\mathcal{F}}$ and outputs the result c^*.

Challenge phase: The adversary $\mathcal{A}$ outputs b', and the reduction algorithm $\mathcal{B}$ outputs b' as well. If the reduction algorithm $\mathcal{B}$ does not receive an output from the adversary $\mathcal{A}$, it outputs a random bit b.

Analysis: Under the assumption that $\mathcal{A}$ breaks the func-CPA security of Π_{KDM} with non-negligible probability, we demonstrate that $\mathcal{B}^{\mathcal{A}}$ can break KDM-CPA security of Π_{KDM} with non-negligible probability. In other words, we show $Adv^{\mathsf{MKfuncPKE}}_{\Pi_{\mathrm{KDM}},\mathcal{A},\mathcal{F}} = Adv^{\mathsf{KDMPKE}}_{\Pi_{\mathrm{KDM}},\mathcal{B}^{\mathcal{A}},\mathcal{F}}$.

First, we confirm that the oracle $\mathsf{O}_{\mathsf{ReEnc}}$ in the experiment $\mathsf{ExpMKfuncPKE}_{\Pi_{\mathrm{KDM}},\mathcal{A},\mathcal{F}^*}$ is correctly simulated. In the oracle simulation, the function f' is defined based on a function f. This is because the oracle $\mathsf{O}_{\mathsf{KDM}}$ in the experiment $\mathsf{ExpPKEKDM}_{\Pi_{\mathrm{KDM}},\mathcal{B}^{\mathcal{A}},\mathcal{F}}$ cannot be queried with pairs of ciphertexts and the indices of the corresponding public keys $\{c_i, j_i\}_{i\in[n], j_i\in[l]}$. By replacing f with f' in $\mathsf{O}_{\mathsf{KDM}}$ from Definition 3, it becomes clear that $\mathsf{O}_{\mathsf{KDM}}$ is equivalent to $\mathsf{O}_{\mathsf{ReEnc}}$ from Definition 7. Therefore, the oracle $\mathsf{O}_{\mathsf{ReEnc}}$ in $\mathsf{ExpMKfuncPKE}_{\Pi_{\mathrm{KDM}},\mathcal{A},\mathcal{F}^*}$ is correctly simulated.

Second, we show that if $\mathcal{A}$ wins the game, then $\mathcal{B}^{\mathcal{A}}$ will also win. Since the simulation of $\mathsf{O}_{\mathsf{ReEnc}}$ in $\mathsf{ExpMKfuncPKE}_{\Pi_{\mathrm{KDM}},\mathcal{A},\mathcal{F}^*}$ utilizes $\mathsf{O}_{\mathsf{KDM}}$ from $\mathsf{ExpPKEKDM}_{\Pi_{\mathrm{KDM}},\mathcal{B}^{\mathcal{A}},\mathcal{F}}$, the bit b in $\mathsf{ExpMKfuncPKE}_{\Pi_{\mathrm{KDM}},\mathcal{A},\mathcal{F}^*}$ is equivalent to the bit b in

$\mathsf{ExpPKEKDM}_{\Pi_{\mathrm{KDM}},\mathcal{B}^{\mathcal{A}},\mathcal{F}}$. In the challenge phase, if the adversary $\mathcal{A}$ outputs b', then the reduction algorithm $\mathcal{B}$ also outputs b'. Therefore, if $\mathsf{ExpMKfuncPKE}_{\Pi_{\mathrm{KDM}},\mathcal{A},\mathcal{F}^*} = 1$, then $\mathsf{ExpPKEKDM}_{\Pi_{\mathrm{KDM}},\mathcal{B}^{\mathcal{A}},\mathcal{F}} = 1$. Thus, we can conclude that if $\mathcal{A}$ wins, then $\mathcal{B}^{\mathcal{A}}$ also wins.

Additionally, by the initial assumption, $\mathcal{A}$ can break MKfuncCPA security of Π_{KDM} with non-negligible probability. From the above considerations, the lemma is proven. □

IV. Multi-Key FuncCPA Security for SKE

In this section, we define the notion of Multi-Key funcCPA (MKfunc) security for SKE and show that if an SKE scheme is KDM secure, it is also MKfuncCPA secure. The formulation and the approach to reduction to KDM security are similar to those in Section III.

A. Definition of Multi-Key funcCPA (MKfunc) Security

In this section, we define the concept of MKfuncCPA security for SKE schemes.

Definition 8 (Multi-Key FuncCPA Security for SKE Schemes)**.** *Let* $E = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be an SKE scheme, and let* $\mathcal{F} = \{f : (\mathcal{M} \cup \{\perp\})^n \to \mathcal{M} | n \in \mathbb{N}\}$ *be a function family. The SKE scheme E is said to be Multi-Key funcCPA (MKfuncCPA) secure for the function family* $\mathcal{F}$ *if, for every sufficiently large security parameter* λ*, every PPT adversary* $\mathcal{A}$*, and the function family* $\mathcal{F}$*, it holds that* $|\Pr[\mathsf{ExpMKfuncSKE}_{E,\mathcal{A},\mathcal{F}}(1^\lambda) = 1] - 1/2| \leq \mathsf{negl}(\lambda)$ *where* $\mathsf{ExpMKfuncSKE}_{E,\mathcal{A},\mathcal{F}}(1^\lambda)$ *is the experiment defined as follows.*

$\mathsf{ExpMKfuncSKE}_{E,\mathcal{A},\mathcal{F}}(1^\lambda)$
$b \leftarrow \{0,1\}; \mathsf{sk}^j \leftarrow \mathsf{KG}(1^\lambda)\ (j = 1, ..., l);$
$b' \leftarrow \mathcal{A}^{\mathsf{O}^b_{\mathsf{ReEnc}}}(1^\lambda)$:
output 1 if $b' = b$ otherwise 0

The oracle $\mathsf{O}^b_{\mathsf{ReEnc}}$ *takes an index* $j^* \in [l]$*, pairs of ciphertexts along with the indices of the corresponding keys* $\{c_i, j_i\}_{i\in[n],j_i\in[l]}$*, and a function* $f \in \mathcal{F}$ *as input and operates as follows.*

- $\mathsf{O}^1_{\mathsf{ReEnc}}$ *returns* $c^* \leftarrow \mathsf{Enc}(\mathsf{sk}^{j^*}, f(\mathsf{Dec}(\mathsf{sk}^{j_1}, c_1), \ldots, \mathsf{Dec}(\mathsf{sk}^{j_n}, c_n)))$
- $\mathsf{O}^0_{\mathsf{ReEnc}}$ *returns* $c^* \leftarrow \mathsf{Enc}(\mathsf{sk}^{j^*}, 0^{|f(\mathsf{Dec}(\mathsf{sk}^{j_1},c_1),\ldots,\mathsf{Dec}(\mathsf{sk}^{j_n},c_n))|})$

We denote the advantage of the adversary in $\mathsf{ExpMKfuncSKE}_{E,\mathcal{A},\mathcal{F}}$ by $Adv^{\mathsf{MKfuncSKE}}_{E,\mathcal{A},\mathcal{F}}$.

B. KDM Security Implies MKfuncCPA Security

We demonstrate that if an SKE schemes is KDM secure, then it is also MKfuncCPA secure. Note that, as in Section III, we focus on KDM security with respect to bounded circuits as the function family. The approach to the reduction proof is similar to that in Section III.

Lemma 2. *If an SKE scheme* E_{KDM} *satisfies bounded-KDM security against CPA attacks, then* E_{KDM} *is also MKfuncCPA secure.*

Proof. We assume for contradiction the existence of a PPT adversary $\mathcal{A}$ that can break MKfuncCPA security of E_{KDM} with non-negligible probability. We then show that there exists a PPT reduction algorithm $\mathcal{B}$ that breaks the KDM-CPA security of E_{KDM} with non-negligible probability with accessing to $\mathcal{A}$. In the experiment $\mathsf{ExpSKEKDM}_{E_{\mathrm{KDM}},\mathcal{B}^{\mathcal{A}},\mathcal{F}}$, the reduction algorithm $\mathcal{B}^{\mathcal{A}}$ operates as follows, simulating the experiment $\mathsf{ExpMKfuncSKE}_{E_{\mathrm{KDM}},\mathcal{A},\mathcal{F}^*}$.

Setup phase: The reduction algorithm $\mathcal{B}$ initiates the adversary $\mathcal{A}$.

Oracle simulation: When the adversary $\mathcal{A}$ makes oracle queries during its execution, $\mathcal{B}$ simulates the oracle $\mathsf{O}_{\mathsf{ReEnc}}$ and responds as follows. Given an index $j^* \in [l]$ for the public key to be used in re-encryption, pairs of ciphertexts and the indices of the corresponding keys $\{c_i, j_i\}_{i\in[n],j_i\in[l]}$, and a function $f \in \mathcal{F}^*$ from $\mathcal{A}$, the adversary $\mathcal{B}$ defines $f'(\mathsf{sk}^1, \ldots, \mathsf{sk}^l) := f(\mathsf{Dec}(\mathsf{sk}^{j_1}, c_1), \ldots, \mathsf{Dec}(\mathsf{sk}^{j_n}, c_n))$. Next, $\mathcal{B}$ queries (j^*, f') to $\mathsf{O}_{\mathsf{KDM}}$ in the experiment $\mathsf{ExpSKEKDM}_{E_{\mathrm{KDM}},\mathcal{B}^{\mathcal{A}},\mathcal{F}}$ and outputs the result c^*.

Challenge phase: When the adversary $\mathcal{A}$ outputs b', the reduction algorithm $\mathcal{B}$ outputs b' as well. If the reduction algorithm $\mathcal{B}$ does not receive an output from the adversary $\mathcal{A}$, it outputs a random bit b.

Analysis: Under the initial assumption that $\mathcal{A}$ can break MKfuncCPA security of E_{KDM} with non-negligible probability, we demonstrate that $\mathcal{B}^{\mathcal{A}}$ can break KDM-CPA security of E_{KDM} with non-negligible probability. In other words, we show $Adv^{\mathsf{MKfuncSKE}}_{E_{\mathrm{KDM}},\mathcal{A},\mathcal{F}} = Adv^{\mathsf{KDMSKE}}_{E_{\mathrm{KDM}},\mathcal{B}^{\mathcal{A}},\mathcal{F}}$.

As in Section III, we confirm that the oracle $\mathsf{O}_{\mathsf{ReEnc}}$ in the experiment $\mathsf{ExpMKfuncSKE}_{E_{\mathrm{KDM}},\mathcal{A},\mathcal{F}^*}$ is correctly simulated. In the oracle simulation, the function f' is defined based on a function f. By replacing f with f' in $\mathsf{O}_{\mathsf{KDM}}$ from Definition 6, it becomes clear that $\mathsf{O}_{\mathsf{KDM}}$ is equivalent to $\mathsf{O}_{\mathsf{ReEnc}}$ from Definition 8. Therefore, the oracle $\mathsf{O}_{\mathsf{ReEnc}}$ in $\mathsf{ExpMKfuncSKE}_{E_{\mathrm{KDM}},\mathcal{A},\mathcal{F}^*}$ is correctly simulated.

In addition, it follows that if $\mathcal{A}$ wins, then $\mathcal{B}^{\mathcal{A}}$ will also win. Given the initial assumption that $\mathcal{A}$ can break MKfuncCPA security of E_{KDM} with non-negligible probability, the lemma is thereby proven. □

V. Conclusions

In this paper, we proposed a new security notion called Multi-Key funcCPA (MKfunc) security for both PKE and SKE, which extends the concept of funcCPA security to handle multiple keys. We also demonstrated that if an encryption scheme satisfies KDM security, it also satisfies MKfuncCPA security. The proposed MKfuncCPA security notion enables discussions on the security of cryptographic schemes in scenarios such as multi-party collaboration in outsourced computation, which have recently garnered attention.

Future challenges include proposing a general construction to transform SKE schemes that satisfy MKfuncCPA security into PKE schemes that also meet MKfuncCPA security by using additional cryptographic primitives, and clarifying the relationship between funcCPA security and MKfuncCPA security.

References

[1] J. Black, P. Rogaway, and T. Shrimpton, "Encryption-scheme security in the presence of key-dependent messages," in *Selected Areas in Cryptography*, K. Nyberg and H. Heys, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 62–75.

[2] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology — EUROCRYPT 2001*, B. Pfitzmann, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 93–118.

[3] D. Boneh, S. Halevi, M. Hamburg, and R. Ostrovsky, "Circular-secure encryption from decision diffie-hellman," in *Advances in Cryptology – CRYPTO 2008*, D. Wagner, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 108–125.

[4] A. Akavia, C. Gentry, S. Halevi, and M. Vald, "Achievable cca2 relaxation for homomorphic encryption," in *Theory of Cryptography Conference*. Springer, 2022, pp. 70–99.

[5] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, ser. STOC '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 169–178.

[6] Y. Dodis, S. Halevi, and D. Wichs, "Security with functional re-encryption from cpa," in *Theory of Cryptography*, G. Rothblum and H. Wee, Eds. Cham: Springer Nature Switzerland, 2023, pp. 279–305.

[7] T. Shinozaki, K. Tanaka, M. Tezuka, and Y. Yoshida, "On the relationship between FuncCPA and FuncCPA+," Cryptology ePrint Archive, Paper 2024/1166, 2024.

[8] K. Nuida, "How to handle invalid queries for malicious-private protocols based on homomorphic encryption," in *Proceedings of the 9th ACM on ASIA Public-Key Cryptography Workshop*, ser. APKC '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 15–25.

[9] B. Barak, I. Haitner, D. Hofheinz, and Y. Ishai, "Bounded key-dependent message security," in *Advances in Cryptology – EUROCRYPT 2010*, H. Gilbert, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 423–444.

[10] B. Waters and D. Wichs, "Universal amplification of kdm security: From 1-key circular to multi-key kdm," in *Advances in Cryptology – CRYPTO 2023*, H. Handschuh and A. Lysyanskaya, Eds. Cham: Springer Nature Switzerland, 2023, pp. 674–693.

[11] A. C.-C. Yao, "How to generate and exchange secrets (extended abstract)," in *IEEE Annual Symposium on Foundations of Computer Science*, 1986, pp. 162–167.

[12] F. Kitagawa and T. Matsuda, "Circular security is complete for kdm security," in *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I 26*. Springer, 2020, pp. 253–285.

[13] B. Applebaum, "Key-dependent message security: Generic amplification and completeness," *Journal of cryptology*, vol. 27, no. 3, pp. 429–451, 2014.

Acknowledgement

This research was partially conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)," which was supported by the Ministry of Internal Affairs and Communications, Japan. This research was partially supported by JSPS KAKENHI Grant Numbers JP23H00468, JP24K20776, JST-CREST JPMJCR22M1, and JST-CREST JPMJCR22U5, Japan.

Appendix

Here we recap the definition of the (single-key) funcCPA security [4] and funcCPA$^+$ security [7] for PKE schemes, respectively. It is already known that funcCPA$^+$ security implies funcCPA security [7].

Definition 9 (FuncCPA Security for PKE)**.** *Let* $\Pi = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a PKE scheme, and let* $\mathcal{F} = \{f : (\mathcal{M} \cup \{\perp\})^n \to \mathcal{M} | n \in \mathbb{N}\}$ *be a function family. The scheme* Π *is said to be funcCPA secure for the function family* $\mathcal{F}$ *if, for every sufficiently large security parameter* λ*, every PPT adversary* $\mathcal{A}$*, and the function family* $\mathcal{F}$*, it holds that* $|\Pr[\mathsf{ExpfuncCPA}_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda) = 1] - 1/2| \leq \mathsf{negl}(\lambda)$ *where* $\mathsf{ExpfuncCPA}_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda)$ *is the experiment defined as follows.*

$\mathsf{ExpfuncCPA}_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda)$
$b \leftarrow \{0,1\}$; $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}(1^\lambda)$;
$(m_0, m_1) \leftarrow \mathcal{A}^{\mathsf{O}_{\mathsf{ReEnc}}}(\mathsf{pk})$;
$c^* \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$;
$b' \leftarrow \mathcal{A}^{\mathsf{O}_{\mathsf{ReEnc}}}(\mathsf{pk}, c^*)$:
output 1 if $b' = b$ otherwise 0

The oracle $\mathsf{O}_{\mathsf{ReEnc}}$ *takes a function* $f \in \mathcal{F}$ *and* l *ciphertexts* $c_1, \ldots, c_l$ *where* l *is the input size of* f *as input and outputs* $c \leftarrow \mathsf{Enc}(\mathsf{pk}, f(\mathsf{Dec}(\mathsf{sk}, c_1), \ldots, \mathsf{Dec}(\mathsf{sk}, c_l)))$.

Definition 10 (FuncCPA$^+$ Security for PKE)**.** *Let* $\Pi = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *be a PKE scheme, and let* $\mathcal{F} = \{f : (\mathcal{M} \cup \{\perp\})^n \to \mathcal{M} | n \in \mathbb{N}\}$ *be a function family. The scheme* Π *is said to be funcCPA$^+$ secure for the function family* $\mathcal{F}$ *if, for every sufficiently large security parameter* λ*, every PPT adversary* $\mathcal{A}$*, and the function family* $\mathcal{F}$*, it holds that* $|\Pr[\mathsf{ExpfuncCPA}^+_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda) = 1] - 1/2| \leq \mathsf{negl}(\lambda)$ *where* $\mathsf{ExpfuncCPA}^+_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda)$ *is the experiment defined as follows.*

$\mathsf{ExpfuncCPA}^+_{\Pi,\mathcal{A},\mathcal{F}}(1^\lambda)$
$b \leftarrow \{0,1\}$; $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}(1^\lambda)$;
$b' \leftarrow \mathcal{A}^{\mathsf{O}^b_{\mathsf{ReEnc}}}(\mathsf{pk})$:
output 1 if $b' = b$ otherwise 0

The oracle $\mathsf{O}^b_{\mathsf{ReEnc}}$ *a function* $f \in \mathcal{F}$ *and* l *ciphertexts* $c_1, \ldots, c_l$ *where* l *is the input size of* f *as input and and operates as follows.*

- $\mathsf{O}^1_{\mathsf{ReEnc}}$ *returns* $c \leftarrow \mathsf{Enc}(\mathsf{pk}, f(\mathsf{Dec}(\mathsf{sk}, c_1), \ldots, \mathsf{Dec}(\mathsf{sk}, c_l)))$.
- $\mathsf{O}^0_{\mathsf{ReEnc}}$ *returns* $c^* \leftarrow \mathsf{Enc}(\mathsf{pk}, 0^{|f(\mathsf{Dec}(\mathsf{sk},c_1),\ldots,\mathsf{Dec}(\mathsf{sk},c_l)))|})$.