Super-Strong RKA Secure MAC, PKE and SE from Tag-based Hash Proof System

Shuai Han, Shengli Liu, and Lin Lyu

Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200240, China
{dalen17,slliu,lvlin}@sjtu.edu.cn

Abstract. $\mathcal{F}$-Related-Key Attacks (RKA) on cryptographic systems consider adversaries who can observe the outcome of a system under not only the original key, say k, but also related keys $f(k)$, with f adaptively chosen from $\mathcal{F}$ by the adversary.

In this paper, we define new RKA security notions for several cryptographic primitives including message authentication code (MAC), public-key encryption (PKE) and symmetric encryption (SE). This new kind of RKA notions are called *super-strong* RKA securities, which stipulate minimal restrictions on the adversary's forgery or oracle access, thus turn out to be the strongest ones among existing RKA security requirements. We present paradigms for constructing super-strong RKA secure MAC, PKE and SE from a common ingredient, namely *Tag-based Hash Proof System* (THPS). We also present constructions for THPS based on the k-Linear and the DCR assumptions.

When instantiating our paradigms with concrete THPS constructions, we obtain super-strong RKA secure MAC, PKE and SE schemes for the class of restricted affine functions $\mathcal{F}_{\text{raff}}$, of which the class of linear functions $\mathcal{F}_{\text{lin}}$ is a subset. To the best of our knowledge, our MACs, PKEs and SEs are the first ones possessing super-strong RKA securities for a non-claw-free function class $\mathcal{F}_{\text{raff}}$ in the standard model and under standard assumptions. Our constructions are free of pairing and are as efficient as those proposed in previous works. In particular, the keys, tags of MAC and ciphertexts of PKE & SE all consist of only a constant number of group elements.

Keywords: related-key attack, hash proof system, message authentication code, public-key encryption, symmetric encryption

1 Introduction

Traditional security model assumes that cryptographic algorithms are black boxes to adversaries, so an adversary only sees (or controls) some input and obtains the outcome of the algorithm. In reality, the development of tampering and fault injection techniques [BDL97, BS97, GLM$^+$04] enables the adversary to modify or influence the keys stored in the system, thus observe the input/output behavior of the system under the modified keys. Such attacks were first formalized as *Related-Key Attacks* (RKAs) by Bellare and Kohno [BK03]. In practice, the key subject to RKAs might be an authentication/verification key of a message authentication code (MAC), a signing key of a digital signature (Sig) scheme, a secret key of a public-key encryption (PKE) or an encryption/decryption key of a symmetric encryption (SE). RKA security studies how to maintain security of the system even if the adversary is able to modify the underlying key to some extent. Requirements for RKA security go across a variety of primitives, like block cipher [Knu92, Bih93], pseudorandom function and permutation (PRF and PRP) [BC10, ABPP14], MAC [Xag13, BR13], PKE [BCM11, BPT12, Wee12], SE [BCM11, BPT12], etc.

In the formulation of RKA security, a class of functions $\mathcal{F} : \mathcal{K} \longrightarrow \mathcal{K}$ must be specified, which characterizes the ability of adversaries to modify the key $k \in \mathcal{K}$, where $\mathcal{K}$ is the key space of the underlying cryptographic primitive. The function class $\mathcal{F}$ was referred to as a class of *related-key deriving functions* (RKDFs) in [BK03]. In the RKA security model of a system, an adversary is allowed to choose a function $f \in \mathcal{F}$ and access the input and output of the system under not only the original key k, but also modified keys $f(k)$. Typical classes of RKDFs include the class of linear functions $\mathcal{F}_{\text{lin}}$, the class of affine functions $\mathcal{F}_{\text{aff}}$ and the class of polynomial functions $\mathcal{F}^d_{\text{poly}}$ of bounded degree d.

1.1 Related Works

(Strong) RKA secure MAC. The standard security notion for MAC is existential unforgeability under chosen-message attacks (EU-CMA), where the adversary has access to a tag generation oracle Tag and aims to generate a valid tag for a message never queried in Tag. A stronger notion called *existential unforgeability under chosen-message and chosen-verification attacks* (EU-CMVA) was proposed in [DKPW12], where the adversary has also access to a verification oracle Vrfy.

Xagawa [Xag13] initialized the theoretical study on RKA security for MAC, and defined two RKA security notions for MAC, namely *EU-$\mathcal{F}$-RK-CMVA* and *strong EU-$\mathcal{F}$-RK-CMVA*. EU-$\mathcal{F}$-RK-CMVA security captures the EU-CMVA security under $\mathcal{F}$-related-key attacks, where the adversary can query Tag and Vrfy oracles under any $\mathcal{F}$-related authentication/verification key. Strong EU-$\mathcal{F}$-RK-CMVA security also guarantees that, even for a message m already queried in Tag, it is still hard for the adversary to generate a *new* valid tag for m.

Two general frameworks were proposed to construct EU-$\mathcal{F}_{\text{lin}}$-RK-CMVA secure MACs in [Xag13], one is from an extended Hash Proof System (HPS) [CS02], another one is from a tag-based adaptive trapdoor relation [KMO10] and a strong one-time secure signature scheme. The frameworks can be instantiated under a number of standard assumptions, such as the factoring (FAC), the decisional Diffie-Hellman (DDH) and the decisional bilinear Diffie-Hellman (DBDH) assumptions. Xagawa [Xag13] also showed that the resulting MACs can be transformed to strong EU-$\mathcal{F}_{\text{lin}}$-RK-CMVA secure ones with the help of a strong one-time secure signature scheme.

Note that a PRF itself is a (deterministic) MAC. In particular, for a claw-free[1] function class $\mathcal{F}$ (such as $\mathcal{F}_{\text{lin}}$), an $\mathcal{F}$-RKA secure PRF itself is a strong EU-$\mathcal{F}$-RK-CMVA secure MAC. Then the DDH-based $\mathcal{F}_{\text{lin}}$-RKA secure PRF in [BC10] also gives a strong EU-$\mathcal{F}_{\text{lin}}$-RK-CMVA secure MAC.

(Strong) RKA secure PKE and SE. The traditional security requirement for PKE and SE is indistinguishability under chosen-plaintext and chosen-ciphertext attacks (IND-CCA2). IND-CCA2 security under $\mathcal{F}$-related-key attacks, called *IND-$\mathcal{F}$-RK-CCA2*, was defined for PKE and SE in [BCM11]. IND-$\mathcal{F}$-RK-CCA2 security for PKE allows the adversary to make decryption queries under any $\mathcal{F}$-related secret key, while IND-$\mathcal{F}$-RK-CCA2 security for SE allows the adversary to make both encryption and decryption queries under any $\mathcal{F}$-related encryption/decryption key.

For *canonical* PKE, a stronger version of IND-$\mathcal{F}$-RK-CCA2 security, namely *strong IND-$\mathcal{F}$-RK-CCA2*, was defined by Bellare et al. [BPT12]. By canonical, we mean that the key generation algorithm of PKE first samples a secret key sk randomly and then computes the public key pk as a deterministic function of sk, i.e., $\mathsf{pk} = \mathsf{PKE.PK}(\mathsf{sk})$. Strong IND-$\mathcal{F}$-RK-CCA2 for (canonical) PKE also allows the adversary to make encryption queries and obtain a challenge ciphertext encrypted under any public key deriving from $\mathcal{F}$-related secret key, i.e., $\mathsf{pk}' = \mathsf{PKE.PK}(f(\mathsf{sk}))$.

[1] A function class $\mathcal{F}$ from $\mathcal{K}$ to $\mathcal{K}$ is called claw-free [BC10], if for all $f \neq f' \in \mathcal{F}$ and all $k \in \mathcal{K}$, $f(k) \neq f'(k)$. Note that $\mathcal{F}_{\text{lin}}$ is claw-free, while $\mathcal{F}_{\text{aff}}$ and $\mathcal{F}^d_{\text{poly}}$ are not.

Wee [Wee12] presented a general framework for constructing IND-$\mathcal{F}$-RK-CCA2 secure PKE from a tag-based adaptive trapdoor relation [KMO10] and a strong one-time secure signature scheme. When instantiated under the FAC and the DBDH assumptions, IND-$\mathcal{F}_{\text{lin}}$-RK-CCA2 secure PKE schemes were obtained. Wee [Wee12] also gave two PKE constructions based on the DDH and the learning with errors (LWE) assumptions, but the schemes only achieve a weak version of IND-$\mathcal{F}_{\text{lin}}$-RK-CCA2 security, where the adversary is prohibited to submit the challenge ciphertext to the decryption oracle.

Bellare et al. [BCM11] studied the relations between various RKA secure primitives, and in particular, showed that $\mathcal{F}$-RKA secure PRF enables transformations from (traditional) IND-CCA2 secure PKE and SE to strong IND-$\mathcal{F}$-RK-CCA2 secure PKE and IND-$\mathcal{F}$-RK-CCA2 secure SE respectively. Their work immediately implies (strong) IND-$\mathcal{F}_{\text{lin}}/\mathcal{F}_{\text{aff}}/\mathcal{F}^{d}_{\text{poly}}$-RK-CCA2 secure PKEs and SEs, when instantiating the transformations with (1) the DDH-based $\mathcal{F}_{\text{lin}}$-RKA secure PRF in [BC10], (2) the DDH-based $\mathcal{F}_{\text{aff}}$-RKA secure PRF but with an exponential-time security reduction or (3) the non-standard decisional d-Diffie-Hellman inversion (d-DDHI)-based $\mathcal{F}^{d}_{\text{poly}}$-RKA secure PRF in [ABPP14].

Bellare et al. [BPT12] showed that the CHK transformation [CHK04] converts a strong $\mathcal{F}$-RKA secure IBE and a strong one-time secure signature scheme to a strong IND-$\mathcal{F}$-RK-CCA2 secure PKE, and showed that the natural transformation converting (canonical) PKE to SE turns a strong IND-$\mathcal{F}$-RK-CCA2 secure PKE to an IND-$\mathcal{F}$-RK-CCA2 secure SE. Bellare et al. [BPT12] also constructed a strong $\mathcal{F}_{\text{aff}}$-RKA secure IBE based on the DBDH assumption and a strong $\mathcal{F}^{d}_{\text{poly}}$-RKA secure IBE based on the non-standard d-extended DBDH (d-EDBDH) assumption. Consequently, they obtained (strong) IND-$\mathcal{F}_{\text{aff}}/\mathcal{F}^{d}_{\text{poly}}$-RK-CCA2 secure PKEs and SEs.

Another work by Damgård et al. [DFMV13] presented a PKE construction which is RKA secure against arbitrary key relations and thus goes beyond the algebraic barrier inherent in previous works. However, the RKA security they achieved is only in a bounded form, i.e., the number of RKA queries made by the adversary is restricted.

Recently, Jia et al. [JLLM13, JLLM14] proposed a general framework for constructing IND-$\mathcal{F}$-RK-CCA2 secure PKE from HPS [CS02] and a 4-wise independent hash function [KPSY09], and instantiated their framework for the class of affine functions $\mathcal{F}_{\text{aff}}$ under a collection of standard assumptions, including the DDH, the quadratic residuosity (QR) and the decisional composite residuosity (DCR) assumptions. Lu et al. [LLJ14] constructed IND-$\mathcal{F}$-RK-CCA2 secure PKE following the key encapsulation mechanism (KEM) + data encapsulation mechanism (DEM) paradigm [CS04]. Specifically, they combined a KEM enjoying the properties of $\mathcal{F}$-key malleability and $\mathcal{F}$-key fingerprint with a tag-based DEM. The $\mathcal{F}$-key malleability for KEM is rather strong to achieve, and there were only instantiations for the class of linear functions $\mathcal{F}_{\text{lin}}$ in [LLJ14] under the DDH and the FAC assumptions.

1.2 Motivation and Observation

If we take a closer look at RKA security notions considered in previous works, we will find that some unrealistic and artificial restrictions are imposed on adversary's forgeries or tampering queries.

As an example, let us see the strong EU-$\mathcal{F}$-RK-CMVA security for MAC defined by Xagawa [Xag13]. An adversary may obtain a cryptographic device from a user and implement RKAs via tampering or fault injection. In particular, the adversary does not see the target authentication/verification key k stored in the hardware device, but might have the ability to tamper with the target key k by specifying functions f, and consequently observe the input/output behavior of the device under (not only the original target key k but also) related keys $f(\mathsf{k})$. Specifically, the adversary might implement two kinds of RKAs in the context of MAC.

- $\textsc{Tag}(f, m)$: The adversary can specify a function f, which transforms the target key k stored in the device to a related key $f(\mathsf{k})$, submit a message m to the device, and obtain a tag σ of m under $f(\mathsf{k})$. We refer to this as a tag generation query, denoted by $\textsc{Tag}(f, m)$.
- $\textsc{Vrfy}(f, m, \sigma)$: The adversary can specify a function f, which transforms the target key k stored in the device to a related key $f(\mathsf{k})$, submit a message m together with a tag σ to the device, and obtain a verification bit indicating whether or not σ is a valid tag for m under $f(\mathsf{k})$. We refer to this as a verification query, denoted by $\textsc{Vrfy}(f, m, \sigma)$.

Finally, the adversary outputs a message-tag pair (m', σ') as a forgery.

- **Winning condition.** ([Xag13]) The adversary wins, if the forgery (m', σ') is fresh and valid under the *original target key* k.

The above formalization of strong EU-$\mathcal{F}$-RK-CMVA security reflects some RKAs to some extent. However, the requirements for the adversary to be successful is too restricted to capture the scenario of real life. More specifically, it does not consider the ability of the adversary to modify the target key in the forgery. The adversary might use f' to tamper with the target key k stored in the hardware device and return the device back to the owner. The owner might not realize that the key k stored in the device has been modified. After that, the adversary might forge (m', σ') hoping that the tampered device verifies (m', σ') w.r.t. $f'(\mathsf{k})$.

As such, a more reasonable winning condition for an adversary to be successful is that:

- **Relaxed winning condition.** The adversary can also designate a function f' for its forgery (m', σ'). The adversary wins if the forgery (m', σ') is fresh and valid under the *related key* $f'(\mathsf{k})$.

We improve the strong EU-$\mathcal{F}$-RK-CMVA to *super-strong* EU-$\mathcal{F}$-RK-CMVA security by relaxing the winning condition. This super-strong RKA security provides more security guarantees against RKAs for MAC and is closer to reality than the strong EU-$\mathcal{F}$-RK-CMVA considered in [Xag13].

Similarly, in the (strong) IND-$\mathcal{F}$-RK-CCA2 security model for PKE and SE [BCM11, BPT12], an adversary can make (tampering) decryption queries, but only in a restricted way. The restrictions are rather artificial and do not capture the realistic scenario. We refer to Subsection 5.1 for a detailed discussion about the restrictions on oracle access in the (strong) IND-$\mathcal{F}$-RK-CCA2 security model. We would also like to define *super-strong* IND-$\mathcal{F}$-RK-CCA2 security for PKE and SE by relaxing those restrictions.

An interesting and natural question is:

> *Can we construct cryptographic primitives possessing the "super-strong" RKA securities for an RKDF class $\mathcal{F}$ as large as possible?*

1.3 Our Contributions

In this paper, we answer the above question affirmatively, and dedicate to formalizations of super-strong RKA security notions and constructions of super-strong RKA secure cryptographic primitives (MAC, PKE and SE), in the standard model and under standard assumptions.

- We formalize *super-strong* EU-RK-$\mathcal{F}$-CMVA for MAC, and *super-strong* IND-$\mathcal{F}$-RK-CCA2 for PKE and SE. These securities remove some artificial restrictions (and only pose minimal restrictions) on the adversary's forgery or oracle access, and turn out to be the strongest ones among existing RKA security requirements for MAC, PKE and SE.
- To construct cryptographic primitives satisfying our *super-strong* RKA securities, we resort to a common underlying building block, i.e., *Tag-based Hash Proof System* (THPS) [CS02, QLC15].
  - We define for THPS new statistical properties, including *$\mathcal{F}$-Public-Key-Homomorphism* and *$\mathcal{F}$-Poly-Bounded Collisions*.
  - We introduce for THPS a new computational problem called *Public-Key Collision Problem*.

  THPS equipped with these new properties is termed as *$\mathcal{F}$-tailored THPS*.
- We show that $\mathcal{F}$-tailored THPS is quite useful in constructing super-strong RKA secure cryptographic primitives.
  - We present a paradigm for constructing super-strong EU-RK-$\mathcal{F}$-CMVA secure MAC from $\mathcal{F}$-tailored THPS.
  - We present a paradigm for constructing super-strong IND-RK-$\mathcal{F}$-CCA2 secure PKE from $\mathcal{F}$-tailored THPS with the help of an authenticated encryption scheme.
  - We apply the natural transformation converting PKE to SE to our super-strong IND-RK-$\mathcal{F}$-CCA2 secure PKE and get a super-strong IND-RK-$\mathcal{F}$-CCA2 secure SE. Thus the latter can also be constructed from $\mathcal{F}$-tailored THPS.
- We give instantiations of $\mathcal{F}_{\text{raff}}$-tailored THPS based on the Matrix DDH assumption (including the DDH and the k-Linear assumptions) [EHK$^+$13] and the DCR assumption [DJ01] respectively, where $\mathcal{F}_{\text{raff}}$ is the class of restricted affine functions. Typically, for a key space $\mathcal{K}$ which is a vector space, a function $f_{(a,\mathsf{b})}$ in $\mathcal{F}_{\text{raff}}$ is parameterized by $a \in \mathbb{Z}$ and $\mathsf{b} = (b_i) \in \mathcal{K}$, and maps $\mathsf{k} = (k_i) \in \mathcal{K}$ to $f_{(a,\mathsf{b})}(\mathsf{k}) = (a \cdot k_i + b_i) \in \mathcal{K}$. Different from $\mathcal{F}_{\text{lin}}$, the class $\mathcal{F}_{\text{raff}}$ is not claw-free[2] and lies between $\mathcal{F}_{\text{lin}}$ and $\mathcal{F}_{\text{aff}}$, i.e., $\mathcal{F}_{\text{lin}} \subsetneq \mathcal{F}_{\text{raff}} \subseteq \mathcal{F}_{\text{aff}}$.
- When instantiating our paradigms with our concrete $\mathcal{F}_{\text{raff}}$-tailored THPSs, we immediately obtain MACs, PKEs and SEs possessing the super-strong $\mathcal{F}_{\text{raff}}$-RKA securities from the Matrix DDH and the DCR assumptions.
  - Our MACs, PKEs and SEs are the first ones achieving super-strong RKA securities for a non-claw-free function class $\mathcal{F}_{\text{raff}}$ (larger than $\mathcal{F}_{\text{lin}}$).
  - Our MACs, PKEs and SEs are free of pairing and are as efficient as those proposed in previous works. In particular, the keys, tags of MAC and ciphertexts of PKE & SE all consist of only a constant number of group elements.

In Table 1, we compare our MACs, PKEs and SEs with known RKA secure schemes which are both under standard assumptions and in the standard model.

[2] We note that our *super-strong* IND-$\mathcal{F}$-RK-CCA2 for PKE and SE is reduced to the (strong) IND-$\mathcal{F}$-RK-CCA2 security when the function class $\mathcal{F}$ is claw-free.

Table 1. Top: comparison among known MACs with EU-$\mathcal{F}$-RK-CMVA security under standard assumptions in the standard model; Middle and Bottom: comparison among known PKEs and SEs with IND-$\mathcal{F}$-RK-CCA2 security under standard assumptions in the standard model. "strong OT-Sig" stands for strong one-time secure signature scheme. $\mathcal{F}_{\text{lin}}$, $\mathcal{F}_{\text{aff}}$ and $\mathcal{F}_{\text{raff}}$ denote the class of linear functions, the class of affine functions and the class of restricted affine functions, respectively. "sup-str" is short for super-strong. $|\mathsf{pk}|$ and $|\mathsf{sk}|$ show the size of public key and secret key for PKE, $|\mathsf{k}|$ the size of key for MAC & SE, $|\mathsf{tag}|$ the size of tag for MAC and $|\mathsf{ct}|$ the size of ciphertext for PKE & SE. Here the size means the number of group elements in the underlying groups. ℓ denotes the security parameter. "FAC" and "k-LIN" ($k \geq 1$) are short for the factoring and the k-Linear assumption respectively. 1-LIN is the DDH assumption

	Scheme	Set	RKA Security		$\lvert\mathsf{pk}\rvert$ for PKE	$\lvert\mathsf{k}\rvert$ for MAC & SE, $\lvert\mathsf{sk}\rvert$ for PKE	$\lvert\mathsf{tag}\rvert$ for MAC, $\lvert\mathsf{ct}\rvert$ for PKE & SE	Assumption
MAC	[Xag13]	$\mathcal{F}_{\text{lin}}$		EU-RK-CMVA	–	$O(1)$	$O(1)$	FAC/DDH/DBDH
	[Xag13] + strong OT-Sig	$\mathcal{F}_{\text{lin}}$	strong	EU-RK-CMVA	–	$O(1)$	$O(1)$	FAC/DDH/DBDH
	[BC10]	$\mathcal{F}_{\text{lin}}$	sup-str	EU-RK-CMVA*	–	$O(\ell)$	$O(1)$	DDH
	Ours	$\mathcal{F}_{\text{raff}}$	sup-str	EU-RK-CMVA	–	$O(1)$	$O(1)$	DDH/DCR
					–	$O(k)$	$O(k)$	k-LIN
PKE	[Wee12]	$\mathcal{F}_{\text{lin}}$		IND-RK-CCA2	$O(1)$	$O(1)$	$O(1)$	FAC/DBDH
	[BCM11] + [BC10] + [KD04]	$\mathcal{F}_{\text{lin}}$	sup-str	IND-RK-CCA2**	$O(1)$	$O(\ell)$	$O(1)$	DDH
	[LLJ14]	$\mathcal{F}_{\text{lin}}$		IND-RK-CCA2	$O(1)$	$O(1)$	$O(1)$	DDH/FAC
	[BPT12] + strong OT-Sig	$\mathcal{F}_{\text{aff}}$	strong	IND-RK-CCA2	$O(1)$	$O(1)$	$O(1)$	DBDH
	[JLLM13, JLLM14]	$\mathcal{F}_{\text{aff}}$		IND-RK-CCA2	$O(1)$	$O(1)$	$O(1)$	DDH/DCR
					$O(\ell)$	$O(\ell)$	$O(1)$	QR
	Ours	$\mathcal{F}_{\text{raff}}$	sup-str	IND-RK-CCA2	$O(1)$	$O(1)$	$O(1)$	DDH/DCR
					$O(k)$	$O(k)$	$O(k)$	k-LIN
SE	[BCM11] + [BC10] + [KD04]	$\mathcal{F}_{\text{lin}}$	sup-str	IND-RK-CCA2**	–	$O(\ell)$	$O(1)$	DDH
	[BPT12] + strong OT-Sig	$\mathcal{F}_{\text{aff}}$		IND-RK-CCA2	–	$O(1)$	$O(1)$	DBDH
	Ours	$\mathcal{F}_{\text{raff}}$	sup-str	IND-RK-CCA2	–	$O(1)$	$O(1)$	DDH/DCR
					–	$O(k)$	$O(k)$	k-LIN

* We observe that the $\mathcal{F}_{\text{lin}}$-RKA secure PRF proposed in [BC10] is actually a (deterministic) MAC possessing our super-strong security.

** We note that our *super-strong* IND-$\mathcal{F}$-RK-CCA2 for PKE and SE is reduced to the (strong) IND-$\mathcal{F}$-RK-CCA2 security when the function class $\mathcal{F}$ is claw-free [BC10]. Recall that $\mathcal{F}_{\text{lin}}$ is claw-free, while $\mathcal{F}_{\text{aff}}$ is not.

1.4 Organization

The rest of the paper is organized as follows. After a brief preliminaries section, we formalize the concept of $\mathcal{F}$-tailored THPS in Section 3. In Section 4, we introduce the super-strong EU-$\mathcal{F}$-RK-CMVA security for MAC and present a paradigm for constructing super-strong secure MAC from $\mathcal{F}$-tailored THPS. In Section 5, we introduce the super-strong IND-$\mathcal{F}$-RK-CCA2 security for PKE and SE, and propose paradigms for constructing super-strong RKA secure PKE and SE from $\mathcal{F}$-tailored THPS, respectively. In Sections 6 and 7, we give instantiations of $\mathcal{F}_{\text{raff}}$-tailored THPS from the MDDH and the DCR assumptions respectively, and consequently, we obtain MDDH-based and DCR-based MACs, PKEs and SEs with super-strong RKA securities for the class of restricted affine functions $\mathcal{F}_{\text{raff}}$.

2 Preliminaries

Let $\ell \in \mathbb{N}$ denote the security parameter. For $i, j \in \mathbb{N}$ with $i < j$, define $[i, j] := \{i, i+1, \cdots, j\}$ and $[j] := \{1, 2, \cdots, j\}$. Let $|\mathcal{S}|$ denote the size of set $\mathcal{S}$. Denote by $s \leftarrow_{\$} \mathcal{S}$ the operation of picking an element s from set $\mathcal{S}$ uniformly at random. For an algorithm $\mathcal{A}$, denote by $y \leftarrow_{\$} \mathcal{A}(x;r)$, or simply $y \leftarrow_{\$} \mathcal{A}(x)$, the operation of running $\mathcal{A}$ with input x and randomness r and assigning output to y. Denote by $\mathsf{U}_{\mathcal{S}}$ the uniform distribution over set $\mathcal{S}$. Let ε denote the empty string. For a primitive XX and a security notion YY, we typically denote the advantage of a PPT adversary $\mathcal{A}$ by $\mathsf{Adv}^{\mathrm{YY}}_{\mathrm{XX},\mathcal{A}}(\ell)$ and define $\mathsf{Adv}^{\mathrm{YY}}_{\mathrm{XX}}(\ell) := \max_{\mathrm{PPT}\mathcal{A}} \mathsf{Adv}^{\mathrm{YY}}_{\mathrm{XX},\mathcal{A}}(\ell)$. 'PPT' is short for Probabilistic Polynomial-Time and 'DPT' Deterministic Polynomial-Time. For random variables X and Y over set $\mathcal{X}$, the guessing probability of X is defined as $\max_{x\in\mathcal{X}} \Pr[X = x]$, and the statistical distance between X and Y is defined as $\Delta(X,Y) := \frac{1}{2} \cdot \sum_{x\in\mathcal{X}} |\Pr[X = x] - \Pr[Y = x]|$.

Games. Our security proof will be game-based security reductions. A game G starts with an Initialize procedure and ends with a Finalize procedure. There are also some optional procedures $\textsc{Proc}_1, \cdots, \textsc{Proc}_n$ performing as oracles. All procedures are described using pseudo-code, where initially all variables are empty strings ε and all sets are empty. An adversary $\mathcal{A}$ is executed in game G suggests the following procedure: $\mathcal{A}$ first calls Initialize, obtaining the corresponding output; then it may make arbitrary oracle-queries to procedures $\textsc{Proc}_i$ according to their specification, and obtain their outputs; finally it makes one single call to Finalize. By $\mathsf{G}^{\mathcal{A}} \Rightarrow b$ we mean that the game G outputs b after interacting with $\mathcal{A}$, and b is in fact the output of Finalize. By $a \overset{\mathsf{G}}{=} b$ we mean that a equals b or is computed as b in G.

2.1 Message Authentication Code

A message authentication code (MAC) is made up of four PPT algorithms $\mathsf{MAC} = (\mathsf{MAC.Setup}, \mathsf{MAC.Gen}, \mathsf{MAC.Tag}, \mathsf{MAC.Vrfy})$: $\mathsf{MAC.Setup}(1^\ell)$ generates a system parameter prm, which implicitly defines a key space $\mathcal{K}_{\mathsf{MAC}}$ and a message space $\mathcal{M}$; $\mathsf{MAC.Gen}(\mathsf{prm})$ takes as input the parameter prm and outputs a key $\mathsf{k} \in \mathcal{K}_{\mathsf{MAC}}$; $\mathsf{MAC.Tag}(\mathsf{k}, m)$ is a *probabilistic* algorithm, it takes as input a key $\mathsf{k} \in \mathcal{K}_{\mathsf{MAC}}$ and a message $m \in \mathcal{M}$, and outputs a tag σ; $\mathsf{MAC.Vrfy}(\mathsf{k}, m, \sigma)$ takes as input a key $\mathsf{k} \in \mathcal{K}_{\mathsf{MAC}}$, a message $m \in \mathcal{M}$ and a tag σ, and outputs a verification bit $\beta \in \{0, 1\}$. Correctness of MAC requires that, for all possible $\mathsf{prm} \leftarrow_{\$} \mathsf{MAC.Setup}(1^\ell)$, $\mathsf{k} \leftarrow_{\$} \mathsf{MAC.Gen}(\mathsf{prm})$ and $m \in \mathcal{M}$, it holds that $\mathsf{MAC.Vrfy}(\mathsf{k}, m, \mathsf{MAC.Tag}(\mathsf{k}, m)) = 1$.

The standard security notion for MAC is existential unforgeability under chosen-message attacks (EU-CMA), where the adversary has access to a tag generation oracle Tag and aims to generate a valid tag for a message never queried in Tag. A stronger security notion, namely *existential unforgeability under chosen-message and chosen-verification attacks* (EU-CMVA), was defined in [DKPW12], where the adversary has also access to a verification oracle Vrfy.

Let $\mathcal{F}$ be a class of functions from $\mathcal{K}_{\mathsf{MAC}}$ to $\mathcal{K}_{\mathsf{MAC}}$, which was referred to as a class of *related-key deriving functions* in [BK03] to characterize the ability of an adversary to modify the key. Two RKA-security notions for MAC, i.e., *EU-$\mathcal{F}$-RK-CMVA* and *strong EU-$\mathcal{F}$-RK-CMVA*, were defined in [Xag13]. The EU-$\mathcal{F}$-RK-CMVA security extends the EU-CMVA security under $\mathcal{F}$-related-key attacks, where the adversary can query Tag and Vrfy oracles under any $\mathcal{F}$-related key. The strong EU-$\mathcal{F}$-RK-CMVA security requires more than EU-$\mathcal{F}$-RK-CMVA, and it stipulates that it is hard for the adversary to generate a new valid tag even for a message already queried in Tag. Formally, we define the strong EU-$\mathcal{F}$-RK-CMVA via the security game in Fig. 1 according to [Xag13].

Definition 1 (Strong EU-$\mathcal{F}$-RK-CMVA Security for MAC). MAC *is strong EU-$\mathcal{F}$-RK-CMVA secure, if for any PPT adversary $\mathcal{A}$, the advantage* $\mathsf{Adv}^{\mathit{str\text{-}eu\text{-}rk\text{-}cmva}}_{\mathsf{MAC},\mathcal{F},\mathcal{A}}(\ell) := \Pr[\mathsf{strong\text{-}EU\text{-}}\mathcal{F}\mathsf{\text{-}RK\text{-}CMVA}^{\mathcal{A}} \Rightarrow 1]$ *is negligible in ℓ, where game* $\mathsf{strong\text{-}EU\text{-}}\mathcal{F}\mathsf{\text{-}RK\text{-}CMVA}$ *is specified in Fig. 1.*

Procedure INITIALIZE:	**Procedure** TAG$(f \in \mathcal{F}, m)$:	**Proc.** VRFY$(f \in \mathcal{F}, m, \sigma)$:	**Procedure** FINALIZE(m, σ):
$\mathsf{prm} \leftarrow_{\$} \mathsf{MAC.Setup}(1^\ell)$. $\mathsf{k} \leftarrow_{\$} \mathsf{MAC.Gen}(\mathsf{prm})$. Return prm.	$\mathsf{k}' := f(\mathsf{k}) \in \mathcal{K}_{\mathsf{MAC}}$. $\sigma \leftarrow_{\$} \mathsf{MAC.Tag}(\mathsf{k}', m)$. $\mathcal{Q}_{\mathcal{TAG}} := \mathcal{Q}_{\mathcal{TAG}} \cup \{(\mathsf{k}', m, \sigma)\}$. Return σ.	$\mathsf{k}' := f(\mathsf{k}) \in \mathcal{K}_{\mathsf{MAC}}$. $\beta \leftarrow \mathsf{MAC.Vrfy}(\mathsf{k}', m, \sigma)$. Return β.	$\beta \leftarrow \mathsf{MAC.Vrfy}(\mathsf{k}, m, \sigma)$. If $\beta = 1 \land (\mathsf{k}, m, \sigma) \notin \mathcal{Q}_{\mathcal{TAG}}$, Set $\mathsf{forge} := \mathsf{true}$. Return forge.

Fig. 1. strong-EU-$\mathcal{F}$-RK-CMVA security game for MAC.

2.2 Public-Key Encryption

A public-key encryption (PKE) scheme consists of four PPT algorithms $\mathsf{PKE} = (\mathsf{PKE.Setup}, \mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$: $\mathsf{PKE.Setup}(1^\ell)$ outputs a system parameter prm, which implicitly defines a public key space $\mathcal{PK}$, a secret key space $\mathcal{SK}$ and a message space $\mathcal{M}$; $\mathsf{PKE.Gen}(\mathsf{prm})$ takes as input the parameter prm, and outputs a public/secret key pair $(\mathsf{pk}, \mathsf{sk}) \in \mathcal{PK} \times \mathcal{SK}$; $\mathsf{PKE.Enc}(\mathsf{pk}, m)$ takes as input a public key $\mathsf{pk} \in \mathcal{PK}$ and a message $m \in \mathcal{M}$, and outputs a ciphertext c; $\mathsf{PKE.Dec}(\mathsf{sk}, c)$ takes as input a secret key $\mathsf{sk} \in \mathcal{SK}$ and a ciphertext c, and outputs a message $m \in \mathcal{M}$ or a rejection symbol $\perp$. Correctness of PKE requires that, for all $\mathsf{prm} \leftarrow_{\$} \mathsf{PKE.Setup}(1^\ell)$, $(\mathsf{pk}, \mathsf{sk}) \leftarrow_{\$} \mathsf{PKE.Gen}(\mathsf{prm})$ and $m \in \mathcal{M}$, we have that $\mathsf{PKE.Dec}(\mathsf{sk}, \mathsf{PKE.Enc}(\mathsf{pk}, m)) = m$.

Let $\mathcal{F}$ be a class of functions from $\mathcal{SK}$ to $\mathcal{SK}$. In [BCM11], the indistinguishability under $\mathcal{F}$-related-key chosen-ciphertext attacks (IND-$\mathcal{F}$-RK-CCA2) was defined and studied. It captures the IND-CCA2 security under $\mathcal{F}$-related-key attacks, and allows the adversary to make decryption queries under any $\mathcal{F}$-related secret key. For *canonical* PKE, a stronger version of IND-$\mathcal{F}$-RK-CCA2 security, namely *strong IND-$\mathcal{F}$-RK-CCA2*, was defined in [BPT12]. By canonical, we require that $\mathsf{PKE.Gen}(\mathsf{prm})$ first samples sk from $\mathcal{SK}$ via a PPT algorithm $\mathsf{sk} \leftarrow_{\$} \mathsf{PKE.SK}(\mathsf{prm})$, then computes pk as a deterministic function of sk via a DPT algorithm $\mathsf{pk} := \mathsf{PKE.PK}(\mathsf{sk}) \in \mathcal{PK}$. The strong IND-$\mathcal{F}$-RK-CCA2 also allows the adversary to make encryption queries under any $\mathcal{F}$-related public key, i.e., $\mathsf{pk}' = \mathsf{PKE.PK}(f(\mathsf{sk}))$, and obtain a challenge ciphertext encrypted under any $\mathcal{F}$-related public key. We formalize the strong IND-$\mathcal{F}$-RK-CCA2 security via the security game in Fig. 2.

Procedure INITIALIZE:	**Proc.** LR$(f^* \in \mathcal{F}, m_0, m_1)$:	**Proc.** ENC$(f \in \mathcal{F}, m)$:	**Procedure** DEC$(f \in \mathcal{F}, c)$:
$\mathsf{prm} \leftarrow_{\$} \mathsf{PKE.Setup}(1^\ell)$. $\mathsf{sk} \leftarrow_{\$} \mathsf{PKE.SK}(\mathsf{prm})$. $\mathsf{pk} := \mathsf{PKE.PK}(\mathsf{sk}) \in \mathcal{PK}$. $b \leftarrow_{\$} \{0, 1\}$. Return $(\mathsf{prm}, \mathsf{pk})$.	// one query $\mathsf{sk}'^* := f^*(\mathsf{sk}) \in \mathcal{SK}$. $\mathsf{pk}'^* := \mathsf{PKE.PK}(\mathsf{sk}'^*) \in \mathcal{PK}$. $c^* \leftarrow_{\$} \mathsf{PKE.Enc}(\mathsf{pk}'^*, m_b)$. $\mathcal{Q}_{\mathcal{ENC}} := \{(\mathsf{sk}'^*, c^*)\}$. Return c^*.	$\mathsf{sk}' := f(\mathsf{sk}) \in \mathcal{SK}$. $\mathsf{pk}' := \mathsf{PKE.PK}(\mathsf{sk}') \in \mathcal{PK}$. $c \leftarrow_{\$} \mathsf{PKE.Enc}(\mathsf{pk}', m)$. Return c.	$\mathsf{sk}' := f(\mathsf{sk}) \in \mathcal{SK}$. If $(\mathsf{sk}', c) \in \mathcal{Q}_{\mathcal{ENC}}$, Return $\perp$. Return $\mathsf{PKE.Dec}(\mathsf{sk}', c)$. **Procedure** FINALIZE$(b')$: Return $(b' = b)$.

Fig. 2. strong-IND-$\mathcal{F}$-RK-CCA2 security game for PKE.

Definition 2 (Strong IND-$\mathcal{F}$-RK-CCA2 Security for PKE). PKE *is strong IND-$\mathcal{F}$-RK-CCA2 secure, if for any PPT adversary $\mathcal{A}$, the advantage* $\mathsf{Adv}^{str\text{-}ind\text{-}rk\text{-}cca2}_{\mathsf{PKE},\mathcal{F},\mathcal{A}}(\ell) := \big| \Pr[\text{strong-IND-}\mathcal{F}\text{-RK-CCA2}^{\mathcal{A}} \Rightarrow 1] - \frac{1}{2} \big|$ *is negligible in ℓ, where game* strong-IND-$\mathcal{F}$-RK-CCA2 *is specified in Fig. 2.*

2.3 Tag-based Hash Proof System

Hash proof system (HPS) and extended HPS (a.k.a. labeled HPS) were introduced by Cramer and Shoup [CS02]. In [QLC15], a useful variant, namely *tag-based HPS* (THPS), was defined and studied. Here we recall its definition.

Definition 3 (Tag-based Hash Proof System). *A tag-based hash proof system* $\mathsf{THPS} = (\mathsf{THPS.Setup}, \mathsf{THPS.Pub}, \mathsf{THPS.Priv})$ *consists of three PPT algorithms:*

- *The parameter generation algorithm* $\mathsf{THPS.Setup}(1^\ell)$ *outputs parameterized instances* $\mathsf{prm}_{\mathsf{THPS}}$*, which implicitly defines* $(\mathcal{K}, \mathcal{C}, \mathcal{V}, \mathcal{T}, \mathcal{SK}, \mathcal{PK}, \Lambda_{(\cdot)}, \mu)$*, where* $\mathcal{K}, \mathcal{C}, \mathcal{V}, \mathcal{T}, \mathcal{SK}, \mathcal{PK}$ *are all finite sets with* $\mathcal{V} \subseteq \mathcal{C}$*,* $\Lambda_{(\cdot)} : \mathcal{C} \times \mathcal{T} \longrightarrow \mathcal{K}$ *is a family of hash functions indexed by a hashing key* $\mathsf{sk} \in \mathcal{SK}$ *and* $\mu : \mathcal{SK} \longrightarrow \mathcal{PK}$ *is a function. We assume that* μ *is efficiently computable, and there are PPT algorithms sampling* $\mathsf{sk} \in \mathcal{SK}$ *uniformly, sampling* $C \in \mathcal{V}$ *uniformly together with a witness* w*, sampling* $C \in \mathcal{C}$ *uniformly, and checking membership in* $\mathcal{C}$*.*

  We require THPS *to be* projective *in the sense that for every* $\mathsf{sk} \in \mathcal{SK}$*, every* $(C, t) \in \mathcal{V} \times \mathcal{T}$*,* $\Lambda_{\mathsf{sk}}(C, t)$ *is determined by* $\mathsf{pk} = \mu(\mathsf{sk})$ *and* (C, t) *completely.*
- *The public evaluation algorithm* $\mathsf{THPS.Pub}(\mathsf{pk}, C, w, t)$ *takes as input a public key* $\mathsf{pk} = \mu(\mathsf{sk}) \in \mathcal{PK}$*, an element* $C \in \mathcal{V}$ *together with a witness* w *and a tag* $t \in \mathcal{T}$*, and outputs the hash value* $K = \Lambda_{\mathsf{sk}}(C, t) \in \mathcal{K}$*.*
- *The private evaluation algorithm* $\mathsf{THPS.Priv}(\mathsf{sk}, C, t)$ *takes as input a hashing key* $\mathsf{sk} \in \mathcal{SK}$*, an element* $C \in \mathcal{C}$ *and a tag* $t \in \mathcal{T}$*, and outputs the hash value* $K = \Lambda_{\mathsf{sk}}(C, t) \in \mathcal{K}$ *without knowing a witness.*

THPS is associated with a subset membership problem. Informally speaking, the subset membership problem states that it is hard to distinguish uniform distribution over $\mathcal{V}$ from uniform distribution over $\mathcal{C} \setminus \mathcal{V}$.

Definition 4 (Subset Membership Problem related to THPS). *The subset membership problem (SMP) related to* THPS *is called hard, if for any PPT adversary* $\mathcal{A}$*, the following advantage is negligible in* ℓ*:*

$$\mathsf{Adv}^{smp}_{\mathsf{THPS},\mathcal{A}}(\ell) := \big| \Pr\left[\mathcal{A}(\mathsf{prm}_{\mathsf{THPS}}, C) = 1\right] - \Pr\left[\mathcal{A}(\mathsf{prm}_{\mathsf{THPS}}, C') = 1\right] \big|,$$

where $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^\ell)$*,* $C \leftarrow_{\$} \mathcal{V}$ *and* $C' \leftarrow_{\$} \mathcal{C} \setminus \mathcal{V}$*.*

Definition 5 (Strongly-Universal$_1$). THPS *is called* strongly-universal$_1$*, if for all* $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^\ell)$*, the following is negligible in* ℓ*:*

$$\epsilon^{str\text{-}u_1}_{\mathsf{THPS}}(\ell) := \max_{C,t} \Delta\big(\ (\mathsf{pk}, \Lambda_{\mathsf{sk}}(C, t))\ ,\ (\mathsf{pk}, \mathsf{U}_{\mathcal{K}})\ \big),$$

where the maximum is over all $C \in \mathcal{C} \setminus \mathcal{V}$ *and all* $t \in \mathcal{T}$*, and the probability is over* $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$ *and* $\mathsf{pk} := \mu(\mathsf{sk})$*.*

Definition 6 (Universal$_2$). THPS *is called* universal$_2$*, if for all* $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^\ell)$*, the following is negligible in* ℓ*:*

$$\epsilon^{u_2}_{\mathsf{THPS}}(\ell) := \max_{\mathsf{pk}, C, C', t, t', K, K'} \Pr\left[\ \Lambda_{\mathsf{sk}}(C', t') = K'\ \middle|\ \mu(\mathsf{sk}) = \mathsf{pk},\ \Lambda_{\mathsf{sk}}(C, t) = K\ \right],$$

where the maximum is over all $\mathsf{pk} \in \mathcal{PK}$*, all* $C \in \mathcal{C}$*, all* $C' \in \mathcal{C} \setminus \mathcal{V}$*, all* $t, t' \in \mathcal{T}$ *with* $t \neq t'$ *and all* $K, K' \in \mathcal{K}$*, and the probability is over* $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$*.*

Note that the key difference between THPS and extended HPS is universal$_2$ property [QLC15]. Extended HPS requires universal$_2$ property hold for $(C,t) \neq (C',t')$, while THPS only requires for $t \neq t'$. Hence, any (universal$_2$) extended HPS is also a (universal$_2$) THPS, but not vice versa. THPS is essentially a weaker variant of extended HPS, and admits more constructions.

In [DKPW12], extracting property was defined for extended HPS, and it requires the hash value $\Lambda_{\mathsf{sk}}(C,t)$ to be uniformly distributed over $\mathcal{K}$ for any $(C,t) \in \mathcal{C} \times \mathcal{T}$, as long as sk is uniformly chosen from $\mathcal{SK}$. Here we give a relaxed version for THPS, i.e., we only require the guessing probability of $\Lambda_{\mathsf{sk}}(C,t)$ to be negligible.

Definition 7 (Extracting). *THPS is called* extracting*, if for all $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^\ell)$, the following is negligible in ℓ:*

$$\epsilon^{ext}_{\mathsf{THPS}}(\ell) := \max_{C,t,K} \Pr[\Lambda_{\mathsf{sk}}(C,t) = K],$$

where the maximum is over all $C \in \mathcal{C}$, all $t \in \mathcal{T}$ and all $K \in \mathcal{K}$, and the probability is over $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$.

2.4 Collision-Resistant Hashing and Universal Hashing

Definition 8 (Collision-Resistant Hashing). *A family of functions $\mathcal{H} = \{\mathsf{H} : \mathcal{X} \longrightarrow \mathcal{Y}\}$ is called* collision-resistant*, if for any PPT adversary $\mathcal{A}$, the following advantage is negligible in ℓ:*

$$\mathsf{Adv}^{cr}_{\mathcal{H},\mathcal{A}}(\ell) := \Pr\left[\mathsf{H} \leftarrow_{\$} \mathcal{H},\ (x,x') \leftarrow_{\$} \mathcal{A}(\mathsf{H})\ :\ \mathsf{H}(x) = \mathsf{H}(x')\ \wedge\ x \neq x'\right].$$

Definition 9 (Universal Hashing [WC81]). *A family of functions $\mathcal{H} = \{\mathsf{H} : \mathcal{X} \longrightarrow \mathcal{Y}\}$ is called* universal*, if all distinct $x, x' \in \mathcal{X}$, it follows that*

$$\Pr\left[\mathsf{H} \leftarrow_{\$} \mathcal{H}\ :\ \mathsf{H}(x) = \mathsf{H}(x')\right] \leq 1/|\mathcal{Y}|.$$

We recall the well-known Leftover Hash Lemma according to [HILL99].

Lemma 1 (Leftover Hash Lemma). *Let $\mathcal{H} = \{\mathsf{H} : \mathcal{X} \longrightarrow \mathcal{Y}\}$ be a family of universal hash functions and let X be a random variable on $\mathcal{X}$. Then for $\mathsf{H} \leftarrow_{\$} \mathcal{H}$, where H and X are independent, it holds that*

$$\Delta\big(\ (\mathsf{H}, \mathsf{H}(X)),\ (\mathsf{H}, \mathsf{U}_{\mathcal{Y}})\ \big) \leq \sqrt{|\mathcal{Y}| \cdot \max_{x \in \mathcal{X}} \Pr[X = x]},$$

where $\mathsf{U}_{\mathcal{Y}}$ is the uniform distribution over $\mathcal{Y}$ and $\max_{x\in\mathcal{X}} \Pr[X = x]$ is the guessing probability of X.

3 $\mathcal{F}$-Tailored Tag-based Hash Proof System

In this section, we introduce an enhanced version of THPS, namely *$\mathcal{F}$-Tailored THPS*, by generalizing the Strongly-Universal$_1$, Universal$_2$ and Extracting properties of THPS, and defining additional properties for THPS, including *Public-Key-Homomorphism* and *Poly-Bounded Collisions*. We also introduce a new computational problem for THPS, namely *Public-Key Collision Problem*.

Let $\mathcal{F}$ be a class of functions from $\mathcal{SK}$ to $\mathcal{SK}$. We first generalize the traditional properties defined in Subsection 2.3 (i.e., strongly-universal$_1$, universal$_2$ and extracting) to the following three $\mathcal{F}$-related properties, which stipulate the traditional properties hold even for any $\mathcal{F}$-related hashing key.

Definition 10 ($\mathcal{F}$-Strongly-Universal$_1$). THPS *is called* $\mathcal{F}$-strongly-universal$_1$*, if for all* $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^{\ell})$*, the following is negligible in* ℓ*:*

$$\epsilon^{str\text{-}u_1}_{\mathsf{THPS},\mathcal{F}}(\ell) := \max_{f,C,t} \Delta\big(\ (\mathsf{pk}, \Lambda_{f(\mathsf{sk})}(C,t))\ ,\ (\mathsf{pk}, \mathsf{U}_{\mathcal{K}})\ \big), \tag{1}$$

where the maximum is over all $f \in \mathcal{F}$*, all* $C \in \mathcal{C} \setminus \mathcal{V}$ *and all* $t \in \mathcal{T}$*, and the probability is over* $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$ *and* $\mathsf{pk} := \mu(\mathsf{sk})$*.*

Definition 11 ($\mathcal{F}$-Universal$_2$). THPS *is called* $\mathcal{F}$-universal$_2$*, if for all* $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^{\ell})$*, the following is negligible in* ℓ*:*

$$\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell) := \max_{f,f',\mathsf{pk},C,C',t,t',K,K'} \Pr\big[\Lambda_{f'(\mathsf{sk})}(C',t') = K' \ \big|\ \mu(\mathsf{sk}) = \mathsf{pk},\ \Lambda_{f(\mathsf{sk})}(C,t) = K\big],$$

where the maximum is over all $f, f' \in \mathcal{F}$*, all* $\mathsf{pk} \in \mathcal{PK}$*, all* $C \in \mathcal{C}$*, all* $C' \in \mathcal{C} \setminus \mathcal{V}$*, all* $t, t' \in \mathcal{T}$ *with* $t \neq t'$ *and all* $K, K' \in \mathcal{K}$*, and the probability is over* $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$*.*

Definition 12 ($\mathcal{F}$-Extracting). THPS *is called* $\mathcal{F}$-extracting*, if for all* $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^{\ell})$*, the following is negligible in* ℓ*:*

$$\epsilon^{ext}_{\mathsf{THPS},\mathcal{F}}(\ell) := \max_{f,C,t,K} \Pr[\Lambda_{f(\mathsf{sk})}(C,t) = K],$$

where the maximum is over all $f \in \mathcal{F}$*, all* $C \in \mathcal{C}$*, all* $t \in \mathcal{T}$ *and all* $K \in \mathcal{K}$*, and the probability is over* $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$*.*

We define a weaker version of $\mathcal{F}$-Strongly-Universal$_1$, namely *Average-Case $\mathcal{F}$-Strongly-Universal$_1$*. Loosely speaking, it only requires the statistical distance (1) to be negligible for an *overwhelming fraction* of C in $\mathcal{C} \setminus \mathcal{V}$, rather than for *all* C in $\mathcal{C} \setminus \mathcal{V}$. We note that $\mathcal{F}$-strongly-universal$_1$ implies average-case $\mathcal{F}$-strongly-universal$_1$.

Definition 13 (Average-Case $\mathcal{F}$-Strongly-Universal$_1$). THPS *is called* average-case $\mathcal{F}$-strongly-universal$_1$*, if for all* $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^{\ell})$*, the following is negligible in* ℓ*:*

$$\epsilon^{ac\text{-}str\text{-}u_1}_{\mathsf{THPS},\mathcal{F}}(\ell) := \max_{f,t} \Delta\big(\ (\mathsf{pk}, C, \Lambda_{f(\mathsf{sk})}(C,t))\ ,\ (\mathsf{pk}, C, \mathsf{U}_{\mathcal{K}})\ \big),$$

where the maximum is over all $f \in \mathcal{F}$ *and all* $t \in \mathcal{T}$*, and the probability is over* $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$, $\mathsf{pk} := \mu(\mathsf{sk})$ *and* $C \leftarrow_{\$} \mathcal{C} \setminus \mathcal{V}$*.*

Definition 14 ($\mathcal{F}$-Public-Key-Homomorphism). THPS *is called* $\mathcal{F}$-public-key-homomorphic*, if for all* $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^{\ell})$*, there is a DPT $\mathcal{F}$-public-key transformer* $\mathsf{THPS.PKTran} : \mathcal{PK} \times \mathcal{F} \longrightarrow \mathcal{PK}$*, such that for all* $f \in \mathcal{F}$ *and all* $\mathsf{sk} \in \mathcal{SK}$*, it holds that*

$$\mu\big(f(\mathsf{sk})\big) = \mathsf{THPS.PKTran}(\mu(\mathsf{sk}), f).$$

Remark 1. In [Xag13], a similar property called μ's homomorphism was defined for extended HPS. Our $\mathcal{F}$-public-key homomorphism property can be viewed as a generalization of theirs. That is, their requirement is dedicated to linear function class $\mathcal{F}_{\text{lin}}$, while ours is defined for a general function class $\mathcal{F}$.

Definition 15 ($\mathcal{F}$-Poly-Bounded Collisions). THPS *is said to have* $\mathcal{F}$-poly-bounded collisions, *if for all* $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^\ell)$, *there is a polynomial bound* $p(\ell)$, *such that*

$$\max_{f \neq f' \in \mathcal{F}} \left|\{\mathsf{sk} \in \mathcal{SK} \mid f(\mathsf{sk}) = f'(\mathsf{sk})\}\right| \leq p(\ell).$$

We refer to a THPS possessing all the $\mathcal{F}$-related properties above as being an $\mathcal{F}$-*Tailored* THPS. It will serve as the core building block in constructing RKA secure MAC, PKE and SE later, where the property of average-case $\mathcal{F}$-strongly-universal$_1$, rather than (worst-case) $\mathcal{F}$-strongly-universal$_1$, is enough for the applications.

Definition 16 ($\mathcal{F}$-Tailored THPS). THPS *is called an* $\mathcal{F}$-tailored THPS, *if it is (1) average-case $\mathcal{F}$-strongly-universal$_1$, (2) $\mathcal{F}$-universal$_2$, (3) $\mathcal{F}$-extracting, (4) $\mathcal{F}$-public-key-homomorphic and (5) has $\mathcal{F}$-poly-bounded collisions.*

Definition 17 (Public-Key Collision Problem related to THPS). *The public-key collision problem (PKCP) related to* THPS *is called hard, if for any PPT adversary $\mathcal{A}$, the following advantage is negligible in ℓ:*

$$\mathsf{Adv}^{pkcp}_{\mathsf{THPS},\mathcal{A}}(\ell) := \Pr\left[\begin{array}{c}\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^\ell), \\ (\mathsf{sk}, \mathsf{sk}') \leftarrow_{\$} \mathcal{A}(\mathsf{prm}_{\mathsf{THPS}})\end{array} : \ \mathsf{sk} \neq \mathsf{sk}' \wedge \mu(\mathsf{sk}) = \mu(\mathsf{sk}')\right].$$

Remark 2. The PKCP essentially captures the collision-resistance of μ. In [Xag13], a similar problem called μ's $\mathcal{F}$-collision resistance was defined for extended HPS w.r.t. a function class $\mathcal{F}$, where the adversary is given $\mathsf{prm}_{\mathsf{THPS}}$, sk and aims to find a function $f \in \mathcal{F}$ such that $f(\mathsf{sk}) \neq \mathsf{sk}$ but $\mu(f(\mathsf{sk})) = \mu(\mathsf{sk})$. Their problem is tightly related to the function class $\mathcal{F}$ and is defined in a target collision flavor, while ours is intrinsic to the THPS.

We present a simple lemma and postpone its proof in Appendix B.

Lemma 2. *If* THPS *is $\mathcal{F}$-universal$_2$, then for all* $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^\ell)$, *all* $\mathsf{pk} \in \mathcal{PK}$, *the conditional guessing probability of* sk *is at most* $\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$, *i.e.,*

$$\max_{\mathsf{sk}' \in \mathcal{SK}} \Pr[\mathsf{sk} = \mathsf{sk}' \mid \mu(\mathsf{sk}) = \mathsf{pk}] \leq \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell),$$

where the probability is over $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$.

4 Super-Strong RKA secure MAC from THPS

In this section, we present a new RKA security notion for MAC, namely *super-strong EU-$\mathcal{F}$-RK-CMVA*, which is even stronger than the strong EU-$\mathcal{F}$-RK-CMVA security defined in [Xag13]. Then we show a paradigm for constructing MAC from THPS. The obtained MAC satisfies our new security when the THPS is an $\mathcal{F}$-tailored one.

4.1 Super-Strong EU-$\mathcal{F}$-RK-CMVA Security for MAC

Let $\mathcal{F}$ be a class of functions from $\mathcal{K}_{\mathsf{MAC}}$ to $\mathcal{K}_{\mathsf{MAC}}$. The strong EU-$\mathcal{F}$-RK-CMVA security notion for MAC (cf. Definition 1) allows the adversary to query TAG and VRFY multiple times under $\mathcal{F}$-related keys, whilst regarding the adversary's forgery (m', σ') as a successful one only if it passes the verification algorithm under *the original unmodified key* k.

Now we strengthen strong EU-$\mathcal{F}$-RK-CMVA to *super-strong EU-$\mathcal{F}$-RK-CMVA security* by relaxing the requirements for an adversary to be successful. Specifically,

- The adversary can designate a function $f' \in \mathcal{F}$ for its forgery (m', σ') and the forgery (f', m', σ') is valid as long as $\mathsf{MAC.Vrfy}(f'(\mathsf{k}), m', \sigma') = 1$. Recall that strong EU-$\mathcal{F}$-RK-CMVA always uses the original key k to test the validity of forgery (m', σ') using $\mathsf{MAC.Vrfy}(\mathsf{k}, m', \sigma')$.
- The adversary cannot submit a queried tuple (f', m', σ') with $\sigma' \leftarrow_{\$} \textsc{Tag}(f', m')$ as a forgery. That is, we consider the adversary's forgery (f', m', σ') as a successful one even if it has queried $\textsc{Tag}(f, m)$ such that $(f'(\mathsf{k}), m', \sigma') = (f(\mathsf{k}), m, \sigma)$, as long as $(f', m', \sigma') \neq (f, m, \sigma)$. However, this corner case is disallowed in the strong EU-$\mathcal{F}$-RK-CMVA security. Recall that strong EU-$\mathcal{F}$-RK-CMVA requires a forgery (m', σ') satisfies $(\mathsf{k}, m', \sigma') \neq (f(\mathsf{k}), m, \sigma)$ for all $\textsc{Tag}(f, m)$ queries.

We stress that our super-strong EU-$\mathcal{F}$-RK-CMVA is defined in a very strong flavor. In fact, it is the strongest among all RKA security notions for MAC.

```
Procedure INITIALIZE:
  $\mathsf{prm} \leftarrow_{\$} \mathsf{MAC.Setup}(1^{\ell})$.
  $\mathsf{k} \leftarrow_{\$} \mathsf{MAC.Gen}(\mathsf{prm})$.
  Return $\mathsf{prm}$.

Procedure TAG($f \in \mathcal{F}, m$):
  $\mathsf{k}' := f(\mathsf{k}) \in \mathcal{K}_{\mathsf{MAC}}$.
  $\sigma \leftarrow_{\$} \mathsf{MAC.Tag}(\mathsf{k}', m)$.
  $\mathcal{Q}_{\mathcal{TAG}} := \mathcal{Q}_{\mathcal{TAG}} \cup \{(f, m, \sigma)\}$.
  Return $\sigma$.

Proc. VRFY($f \in \mathcal{F}, m, \sigma$):
  $\mathsf{k}' := f(\mathsf{k}) \in \mathcal{K}_{\mathsf{MAC}}$.
  $\beta \leftarrow \mathsf{MAC.Vrfy}(\mathsf{k}', m, \sigma)$.
  If $\beta = 1$, Return 1.
      If $(f, m, \sigma) \notin \mathcal{Q}_{\mathcal{TAG}}$,
          Set $\mathsf{forge} := \mathsf{true}$.
  Else, Return 0.

Procedure FINALIZE:
  Return $\mathsf{forge}$.
```

Fig. 3. super-strong-EU-$\mathcal{F}$-RK-CMVA security game for MAC.

Definition 18 (Super-Strong EU-$\mathcal{F}$-RK-CMVA Security for MAC). MAC *is super-strong EU-$\mathcal{F}$-RK-CMVA secure, if for any PPT adversary $\mathcal{A}$, the advantage* $\mathsf{Adv}^{sup\text{-}str\text{-}eu\text{-}rk\text{-}cmva}_{\mathsf{MAC},\mathcal{F},\mathcal{A}}(\ell) := \Pr[\mathsf{super\text{-}strong\text{-}EU\text{-}}\mathcal{F}\mathsf{\text{-}RK\text{-}CMVA}^{\mathcal{A}} \Rightarrow 1]$ *is negligible in ℓ, where game* super-strong-EU-$\mathcal{F}$-RK-CMVA *is shown in Fig. 3.*

4.2 The Construction

Let $\mathsf{THPS} = (\mathsf{THPS.Setup}, \mathsf{THPS.Pub}, \mathsf{THPS.Priv})$ be a tag-based hash proof system with instance space $\mathcal{C}$, tag space $\mathcal{T}$, key space $\mathcal{K}$, public key space $\mathcal{PK}$, and hashing key space $\mathcal{SK}$. Let $\mathcal{M}$ be an arbitrary set, and let $\mathcal{H} = \big\{\mathsf{H} : \mathcal{PK} \times \mathcal{M} \times \mathcal{C} \longrightarrow \mathcal{T}\big\}$ be a family of hash functions. The proposed MAC $\mathsf{MAC[THPS]} = (\mathsf{MAC.Setup}, \mathsf{MAC.Gen}, \mathsf{MAC.Tag}, \mathsf{MAC.Vrfy})$ with key space $\mathcal{K}_{\mathsf{MAC}} := \mathcal{SK}$ and message space $\mathcal{M}$ is defined in Fig. 4. It is easy to check the correctness of $\mathsf{MAC[THPS]}$.

Remark 3. Our construction of $\mathsf{MAC[THPS]}$ from THPS is similar to the MAC construction from extended HPS in [Xag13]. However, the security of our $\mathsf{MAC[THPS]}$ is stronger than theirs and our RKA function class is also larger than theirs.

```
$\mathsf{prm} \leftarrow_{\$} \mathsf{MAC.Setup}(1^{\ell})$:
$\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^{\ell})$.
$\mathsf{H} \leftarrow_{\$} \mathcal{H}$.
Return $\mathsf{prm} := (\mathsf{prm}_{\mathsf{THPS}}, \mathsf{H})$.

$\mathsf{sk} \leftarrow_{\$} \mathsf{MAC.Gen}(\mathsf{prm})$:
$\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$.
Return $\mathsf{sk}$.
```

```
$\langle C, K\rangle \leftarrow_{\$} \mathsf{MAC.Tag}(\mathsf{sk}, m)$:
$\mathsf{pk} := \mu(\mathsf{sk}) \in \mathcal{PK}$.
$C \leftarrow_{\$} \mathcal{V}$ together with
  witness $w$.
$t := \mathsf{H}(\mathsf{pk}, m, C) \in \mathcal{T}$.
$K := \Lambda_{\mathsf{sk}}(C, t) \in \mathcal{K}$.
Return $\langle C, K\rangle$.
```

```
$0/1 \leftarrow \mathsf{MAC.Vrfy}\big(\mathsf{sk}, m, \langle C, K'\rangle\big)$:
$\mathsf{pk} := \mu(\mathsf{sk}) \in \mathcal{PK}$.
If $C \notin \mathcal{C}$, Return 0.
$t := \mathsf{H}(\mathsf{pk}, m, C) \in \mathcal{T}$.
$K := \Lambda_{\mathsf{sk}}(C, t) \in \mathcal{K}$.
If $K' = K$, Return 1;
Else, Return 0.
```

Fig. 4. Construction of $\mathsf{MAC}[\mathsf{THPS}]$.

- The MAC from extended HPS in [Xag13] was specific to the class of linear functions $\mathcal{F}_{\text{lin}}$, and the resulting MAC was only proved to be EU-$\mathcal{F}_{\text{lin}}$-RK-CMVA secure. To promote the security to strong EU-$\mathcal{F}_{\text{lin}}$-RK-CMVA, the MAC needs another building block of strong one-time secure signature, which makes the construction quite involved.
- Our MAC from THPS achieves the super-strong EU-$\mathcal{F}$-RK-CMVA security directly for a general function class $\mathcal{F}$, by imposing some requirements (cf. Section 3) on THPS. We stress that those requirements do not narrow the instantiations of THPS. In fact we can instantiate THPS from the Matrix DDH (including DDH, k-LIN) and the DCR assumptions for the class of restricted affine functions $\mathcal{F}_{\text{raff}}$, of which $\mathcal{F}_{\text{lin}}$ is a subset.

Theorem 1. *If $\mathcal{H}$ is collision-resistant, THPS is an $\mathcal{F}$-tailored THPS, and the SMP and PKCP related to THPS are both hard, then the $\mathsf{MAC}[\mathsf{THPS}]$ in Fig. 4 is super-strong EU-$\mathcal{F}$-RK-CMVA secure.*

Proof of Theorem 1. Suppose that $\mathcal{A}$ is a PPT adversary against the super-strong EU-$\mathcal{F}$-RK-CMVA security of $\mathsf{MAC}[\mathsf{THPS}]$, who makes at most Q_t times of TAG queries and Q_v times of VRFY queries. We prove the theorem by defining a sequence of games as shown in Fig. 5, and proving the adjacent games indistinguishable.

- Game G_0: This is the $\mathsf{super\text{-}strong\text{-}EU\text{-}}\mathcal{F}\mathsf{\text{-}RK\text{-}CMVA}$ security game (cf. Fig. 3). Let Forge denote the event that FINALIZE outputs 1, i.e., the adversary $\mathcal{A}$ ever queries VRFY such that $(f, m, \langle C, K'\rangle) \notin \mathcal{Q}_{\mathcal{TAG}}$ and $\text{VRFY}\big(f \in \mathcal{F}, m, \langle C, K'\rangle\big) = 1$. Then by definition, $\mathsf{Adv}^{\textit{sup-str-eu-rk-cmva}}_{\mathsf{MAC}[\mathsf{THPS}],\mathcal{F},\mathcal{A}}(\ell) = \Pr_0[\mathsf{Forge}]$.

- Game G_1: This game is the same as game G_0, except that, the challenger changes the way it computes pk'_λ in TAG and pk' in VRFY.

  In game G_0, the challenger computes $\mathsf{pk}'_\lambda := \mu(\mathsf{sk}'_\lambda)$ with $\mathsf{sk}'_\lambda := f_\lambda(\mathsf{sk})$ in $\text{TAG}(f_\lambda, m_\lambda)$ and $\mathsf{pk}' := \mu(\mathsf{sk}')$ with $\mathsf{sk}' := f(\mathsf{sk})$ in $\text{VRFY}\big(f, m, \langle C, K'\rangle\big)$. Now in game G_1, it simply invokes the $\mathcal{F}$-public-key transformer $\mathsf{THPS.PKTran}$ (cf. Definition 14) to compute $\mathsf{pk}'_\lambda := \mathsf{THPS.PKTran}(\mathsf{pk}, f_\lambda)$ in TAG and $\mathsf{pk}' := \mathsf{THPS.PKTran}(\mathsf{pk}, f)$ in VRFY.

  Since THPS is $\mathcal{F}$-public-key-homomorphic, this change is conceptual. Therefore G_0 and G_1 are essentially the same, and $\Pr_0[\mathsf{Forge}] = \Pr_1[\mathsf{Forge}]$.

Next, through the following games G_2–G_5, the challenger will answer VRFY queries $\big(f, m, \langle C, K'\rangle\big)$ in different ways (and finally avoid using the key sk), as long as $t = t_\lambda$ for some λ, where $t = \mathsf{H}(\mathsf{pk}', m, C)$ and $t_\lambda = \mathsf{H}(\mathsf{pk}'_\lambda, m_\lambda, C_\lambda)$.

More precisely, we divide the event that $t = t_\lambda$ for some λ into four cases:

```
INITIALIZE:    // $\mathsf{G}_0$–$\mathsf{G}_6$
$\mathsf{prm}_{\mathsf{THPS}} \leftarrow_\$ \mathsf{THPS.Setup}(1^\ell)$.
$\mathsf{H} \leftarrow_\$ \mathcal{H}$.
$\mathsf{sk} \leftarrow_\$ \mathcal{SK}$.
$\mathsf{pk} := \mu(\mathsf{sk}) \in \mathcal{PK}$.
Return $\mathsf{prm} := (\mathsf{prm}_{\mathsf{THPS}}, \mathsf{H})$.

TAG($f_\lambda \in \mathcal{F}, m_\lambda$):    // the $\lambda$-th query
    // $\mathsf{G}_0$, $\boxed{\mathsf{G}_1 - \mathsf{G}_6}$, $\mathsf{G}_6$
$\mathsf{sk}'_\lambda := f_\lambda(\mathsf{sk}) \in \mathcal{SK}$.
$\mathsf{pk}'_\lambda := \mu(\mathsf{sk}'_\lambda) \in \mathcal{PK}$.
$\boxed{\mathsf{pk}'_\lambda := \mathsf{THPS.PKTran}(\mathsf{pk}, f_\lambda) \in \mathcal{PK}.}$
$C_\lambda \leftarrow_\$ \mathcal{V}$ with witness $w_\lambda$.
$t_\lambda := \mathsf{H}(\mathsf{pk}'_\lambda, m_\lambda, C_\lambda) \in \mathcal{T}$.
$K_\lambda := \Lambda_{\mathsf{sk}'_\lambda}(C_\lambda, t_\lambda) \in \mathcal{K}$.
$K_\lambda \leftarrow_\$ \mathcal{K}$.
$\mathcal{Q}_{\mathcal{TAG}} := \mathcal{Q}_{\mathcal{TAG}} \cup \{\ (f_\lambda, m_\lambda, \langle C_\lambda, K_\lambda\rangle)\ \}$.
Return $\langle C_\lambda, K_\lambda\rangle$.

FINALIZE:    // $\mathsf{G}_0$–$\mathsf{G}_6$
Return $\mathsf{forge}$.

VRFY($f \in \mathcal{F}, m, \langle C, K'\rangle$):
  // $\mathsf{G}_0$, $\boxed{\mathsf{G}_1 - \mathsf{G}_6}$, $\mathsf{G}_2 - \mathsf{G}_6$, $\mathsf{G}_3 - \mathsf{G}_6$, $\boxed{\boxed{\mathsf{G}_4 - \mathsf{G}_6}}$, $\mathsf{G}_5 - \mathsf{G}_6$
$\mathsf{sk}' := f(\mathsf{sk}) \in \mathcal{SK}$.   $\mathsf{pk}' := \mu(\mathsf{sk}') \in \mathcal{PK}$.
$\boxed{\mathsf{pk}' := \mathsf{THPS.PKTran}(\mathsf{pk}, f) \in \mathcal{PK}.}$
If $C \notin \mathcal{C}$, Return 0.
$t := \mathsf{H}(\mathsf{pk}', m, C) \in \mathcal{T}$.
If $t = t_\lambda$ for some $\lambda$,
    If $(f, m, C) = (f_\lambda, m_\lambda, C_\lambda)$,
        $K := K_\lambda \in \mathcal{K}$.
    If $(m, C) \neq (m_\lambda, C_\lambda) \vee$
      $((m, C) = (m_\lambda, C_\lambda) \wedge \mathsf{pk}' \neq \mathsf{pk}'_\lambda)$,
        Return 0.
    If $(m, C) = (m_\lambda, C_\lambda) \wedge \mathsf{pk}' = \mathsf{pk}'_\lambda \wedge \mathsf{sk}' \neq \mathsf{sk}'_\lambda$,
        Return 0.
    If $(m, C) = (m_\lambda, C_\lambda) \wedge \mathsf{sk}' = \mathsf{sk}'_\lambda \wedge f \neq f_\lambda$,
        Return 0.
Else $t \neq t_\lambda$ for all $\lambda$,
    $K := \Lambda_{\mathsf{sk}'}(C, t) \in \mathcal{K}$.
If $K' = K$, Return 1.
    If $(f, m, \langle C, K'\rangle) \notin \mathcal{Q}_{\mathcal{TAG}}$, Set $\mathsf{forge} := \mathsf{true}$.
Else, Return 0.
```

Fig. 5. Games G_0–G_6 for super-strong EU-$\mathcal{F}$-RK-CMVA security of $\mathsf{MAC[THPS]}$.

- Case 1: $t = t_\lambda \wedge (f, m, C) = (f_\lambda, m_\lambda, C_\lambda)$ for some λ
- Case 2: $t = t_\lambda \wedge \big((m, C) \neq (m_\lambda, C_\lambda) \vee ((m, C) = (m_\lambda, C_\lambda) \wedge \mathsf{pk}' \neq \mathsf{pk}'_\lambda)\big)$ for some λ
- Case 3: $t = t_\lambda \wedge (m, C) = (m_\lambda, C_\lambda) \wedge \mathsf{pk}' = \mathsf{pk}'_\lambda \wedge \mathsf{sk}' \neq \mathsf{sk}'_\lambda$ for some λ
- Case 4: $t = t_\lambda \wedge (m, C) = (m_\lambda, C_\lambda) \wedge \mathsf{sk}' = \mathsf{sk}'_\lambda \wedge f \neq f_\lambda$ for some λ

In the next four games, the challenger will handle these cases one by one.

– Game G_2: This game is the same as game G_1, except that, when answering $\textsc{Vrfy}\big(f, m, \langle C, K'\rangle\big)$, if Case 1 occurs, i.e., $t = t_\lambda \wedge (f, m, C) = (f_\lambda, m_\lambda, C_\lambda)$ for some λ, the challenger directly sets $K := K_\lambda$ instead of computing $K := \Lambda_{\mathsf{sk}'}(C, t)$.

Suppose that Case 1 holds. Clearly, $f = f_\lambda$ leads to $\mathsf{sk}' = \mathsf{sk}'_\lambda$. Thus in game G_1, we have

$$K = \Lambda_{\mathsf{sk}'}(C, t) = \Lambda_{\mathsf{sk}'_\lambda}(C_\lambda, t_\lambda) = K_\lambda.$$

Therefore in Case 1, $K = K_\lambda$ holds both in G_1 and G_2. Then G_2 is identical to G_1, and $\Pr_1[\mathsf{Forge}] = \Pr_2[\mathsf{Forge}]$.

– Game G_3: This game is the same as game G_2, except that, when answering $\textsc{Vrfy}\big(f, m, \langle C, K'\rangle\big)$, if Case 2 occurs, i.e., $t = t_\lambda \wedge \big((m, C) \neq (m_\lambda, C_\lambda) \vee ((m, C) = (m_\lambda, C_\lambda) \wedge \mathsf{pk}' \neq \mathsf{pk}'_\lambda)\big)$ for some λ, the challenger returns 0 directly.

Since $t = \mathsf{H}(\mathsf{pk}', m, C)$ and $t_\lambda = \mathsf{H}(\mathsf{pk}'_\lambda, m_\lambda, C_\lambda)$, any difference between G_2 and G_3 will imply a collision of $\mathcal{H}$. Thus $\big|\Pr_2[\mathsf{Forge}] - \Pr_3[\mathsf{Forge}]\big| \leq \mathsf{Adv}^{cr}_{\mathcal{H}}(\ell)$.

- Game G_4: This game is the same as game G_3, except that, when answering $\textsc{Vrfy}\big(f, m, \langle C, K'\rangle\big)$, if Case 3 occurs, i.e., $t = t_\lambda \wedge (m, C) = (m_\lambda, C_\lambda) \wedge \mathsf{pk}' = \mathsf{pk}'_\lambda \wedge \mathsf{sk}' \neq \mathsf{sk}'_\lambda$ for some λ, the challenger simply returns 0.

  Let PKColl denote the event that $\mathcal{A}$ ever queries $\textsc{Vrfy}\big(f, m, \langle C, K'\rangle\big)$, such that $\mathsf{pk}' = \mathsf{pk}'_\lambda$ but $\mathsf{sk}' \neq \mathsf{sk}'_\lambda$ for some λ. Clearly G_3 and G_4 are the same unless PKColl occurs. We have that $\big|\Pr_3[\mathsf{Forge}] - \Pr_4[\mathsf{Forge}]\big| \leq \Pr_4[\mathsf{PKColl}]$.

  Since $\mathsf{pk}' = \mu(\mathsf{sk}')$ and $\mathsf{pk}'_\lambda = \mu(\mathsf{sk}'_\lambda)$, it is straightforward to construct a PPT adversary which can employ the occurrence of PKColl to solve the PKCP related to THPS. So $\Pr_4[\mathsf{PKColl}] \leq \mathsf{Adv}^{pkcp}_{\mathsf{THPS}}(\ell)$ and $\big|\Pr_3[\mathsf{Forge}] - \Pr_4[\mathsf{Forge}]\big| \leq \mathsf{Adv}^{pkcp}_{\mathsf{THPS}}(\ell)$.

- Game G_5: This game is the same as game G_4, except that, when answering $\textsc{Vrfy}\big(f, m, \langle C, K'\rangle\big)$, if Case 4 occurs, i.e., $t = t_\lambda \wedge (m, C) = (m_\lambda, C_\lambda) \wedge \mathsf{sk}' = \mathsf{sk}'_\lambda \wedge f \neq f_\lambda$ for some λ, the challenger directly returns 0.

  Let Guess denote the event that $\mathcal{A}$ ever queries $\textsc{Vrfy}\big(f, m, \langle C, K'\rangle\big)$, such that $\mathsf{sk}' = \mathsf{sk}'_\lambda$ but $f \neq f_\lambda$ for some λ. Clearly G_4 and G_5 are the same unless Guess occurs. Therefore, we have that

$$\big|\Pr_4[\mathsf{Forge}] - \Pr_5[\mathsf{Forge}]\big| \leq \Pr_5[\mathsf{Guess}]. \qquad (2)$$

We will give an upper bound on $\Pr_5[\mathsf{Guess}]$. However, the analysis of $\Pr_5[\mathsf{Guess}]$ is not an easy task, and we will defer it to the following game G'_5.

– Game G'_5: It is the same as game G_5, except that, when answering $\textsc{Vrfy}\big(f, m, \langle C, K'\rangle\big)$, if $t \neq t_\lambda$ for all λ and $C \in \mathcal{C} \setminus \mathcal{V}$, the challenger returns 0 directly instead of checking whether or not $K' = K$.

Let Bad denote the event that $\mathcal{A}$ ever queries $\textsc{Vrfy}\big(f, m, \langle C, K'\rangle\big)$, such that $C \in \mathcal{C} \setminus \mathcal{V}$ but $K' = K$. Clearly G_5 and G'_5 are the same until Bad happens, thus

$$\big|\Pr_5[\mathsf{Guess}] - \Pr'_5[\mathsf{Guess}]\big| \leq \Pr'_5[\mathsf{Bad}]. \qquad (3)$$

We give an upper bound on $\Pr'_5[\mathsf{Bad}]$ via the following lemma.

Lemma 3. $\Pr'_5[\mathsf{Bad}] \leq Q_v \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

Proof. We consider the information about sk that $\mathcal{A}$ may obtain in G'_5.

- For $\textsc{Tag}(f_\lambda, m_\lambda)$, the challenger can use $\mathsf{pk} = \mu(\mathsf{sk})$ to compute pk'_λ and K_λ. More precisely, $\mathsf{pk}'_\lambda = \mathsf{THPS.PKTran}(\mathsf{pk}, f_\lambda)$ and

$$\begin{aligned} K_\lambda &= \Lambda_{\mathsf{sk}'_\lambda}(C_\lambda, t_\lambda) && : \ C_\lambda \leftarrow_\$ \mathcal{V} \text{ with witness } w_\lambda \\ &= \mathsf{THPS.Pub}(\mathsf{pk}'_\lambda, C_\lambda, w_\lambda, t_\lambda) && : \ \text{via projective property.} \end{aligned}$$

- For $\textsc{Vrfy}\big(f, m, \langle C, K'\rangle\big)$, the challenger uses pk to compute $\mathsf{pk}' = \mathsf{THPS.PKTran}(\mathsf{pk}, f)$.
  - If $t = t_\lambda \wedge (f, m, C) = (f_\lambda, m_\lambda, C_\lambda)$ for some λ, i.e., Case 1 occurs, the challenger does not use sk at all but simply sets $K = K_\lambda$.

- If $t = t_\lambda \wedge (f, m, C) \neq (f_\lambda, m_\lambda, C_\lambda)$ for some λ, i.e., Case 2 or Case 3 or Case 4 occurs, the challenger does not use sk and returns 0 directly.
- If $t \neq t_\lambda$ for all λ and $C \in \mathcal{C} \setminus \mathcal{V}$, the challenger returns 0 directly.
- If $t \neq t_\lambda$ for all λ and $C \in \mathcal{V}$, the challenger computes $K = \Lambda_{\mathsf{sk}'}(C, t)$. Since THPS is projective, the value of K will leak at most pk' to $\mathcal{A}$.

Thus the only information about sk that $\mathcal{A}$ may get in G_5' is $\mathsf{pk} = \mu(\mathsf{sk})$.

The event Bad occurs in G_5' means that $\mathcal{A}$ ever queries $\textsc{Vrfy}\big(f, m, \langle C, K' \rangle\big)$ such that $C \in \mathcal{C} \setminus \mathcal{V}$ but $K' = K$, where $K := \Lambda_{\mathsf{sk}'}(C, t) = \Lambda_{f(\mathsf{sk})}(C, t)$.

Since $C \in \mathcal{C} \setminus \mathcal{V}$, by the $\mathcal{F}$-universal$_2$ property of THPS, the guessing probability of $K = \Lambda_{f(\mathsf{sk})}(C, t)$ is at most $\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$ conditioned on $\mathsf{pk} = \mu(\mathsf{sk})$. Then $K' = K$ will hold with probability at most $\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

By a union bound, $\Pr_5'[\mathsf{Bad}] \leq Q_v \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$ and the lemma follows. ▌

Finally, we analyze $\Pr_5'[\mathsf{Guess}]$. Recall that in the proof of Lemma 3, we observe that the only information about sk that the adversary $\mathcal{A}$ may get in game G_5' is $\mathsf{pk} = \mu(\mathsf{sk})$. Since THPS is $\mathcal{F}$-universal$_2$, by Lemma 2, given pk, the conditional guessing probability of sk is at most $\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

Because THPS has $\mathcal{F}$-poly-bounded collisions, i.e.,

$$\max_{f \neq f_\lambda \in \mathcal{F}} \big|\{\mathsf{sk} \in \mathcal{SK} \mid f(\mathsf{sk}) = f_\lambda(\mathsf{sk})\}\big| \leq p(\ell),$$

for some polynomial $p(\ell)$, in one $\textsc{Vrfy}$ query $\big(f, m, \langle C, K' \rangle\big)$, the event $\mathsf{sk}' = f(\mathsf{sk}) = f_\lambda(\mathsf{sk}) = \mathsf{sk}'_\lambda$ but $f \neq f_\lambda$ for some $\lambda \in [Q_t]$ can hold with probability at most $Q_t \cdot p(\ell) \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$. By a union bound over Q_v times of $\textsc{Vrfy}$ queries,

$$\Pr_5'[\mathsf{Guess}] \leq Q_v \cdot Q_t \cdot p(\ell) \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell). \tag{4}$$

By combining Eqs. (2)-(4) and Lemma 3, we get that $\big|\Pr_4[\mathsf{Forge}] - \Pr_5[\mathsf{Forge}]\ \big| \leq Q_v \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell) + Q_v \cdot Q_t \cdot p(\ell) \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

Next, we consider a sequence of games $\{\mathsf{G}_{5,i,0}\text{–}\mathsf{G}_{5,i,4}\}_{i \in [Q_t]}$ shown in Fig. 6.

- Game $\mathsf{G}_{5,i,0}$, $i \in [Q_t + 1]$: This game is the same as game G_5, except that, in the λ-th ($\lambda \in [i-1]$) $\textsc{Tag}$ query, the challenger does not use the key sk to compute K_λ, and instead, it simply picks K_λ from $\mathcal{K}$ uniformly. The challenger still answers the λ-th ($\lambda \in [i, Q_t]$) $\textsc{Tag}$ query by computing $K_\lambda := \Lambda_{\mathsf{sk}'_\lambda}(C_\lambda, t_\lambda)$ the same as in game G_5.

  Clearly $\mathsf{G}_{5,1,0}$ is identical to G_5, thus $\Pr_5[\mathsf{Forge}] = \Pr_{5,1,0}[\mathsf{Forge}]$.

- Game $\mathsf{G}_{5,i,1}$, $i \in [Q_t]$: This game is the same as game $\mathsf{G}_{5,i,0}$, except that, in the i-th $\textsc{Tag}$ query, the challenger samples C_i uniformly from $\mathcal{C} \setminus \mathcal{V}$ instead of $\mathcal{V}$.

  It is straightforward to bound the difference between $\mathsf{G}_{5,i,0}$ and $\mathsf{G}_{5,i,1}$ by constructing a PPT adversary to solve the SMP related to THPS, such that $\big|\Pr_{5,i,0}[\mathsf{Forge}] - \Pr_{5,i,1}[\mathsf{Forge}]\ \big| \leq \mathsf{Adv}^{smp}_{\mathsf{THPS}}(\ell)$.

- Game $\mathsf{G}_{5,i,2}$, $i \in [Q_t]$: This game is the same as game $\mathsf{G}_{5,i,1}$, except that, when answering $\textsc{Vrfy}\big(f, m, \langle C, K' \rangle\big)$, if $t \neq t_\lambda$ for all λ and $C \in \mathcal{C} \setminus \mathcal{V}$, the challenger directly returns 0 instead of checking whether or not $K' = K$.

```
$\underline{\textsc{Tag}(f_\lambda \in \mathcal{F}, m_\lambda):}$    // the $\lambda$-th query
  // $\mathsf{G}_{5,i,0}$, $\boxed{\mathsf{G}_{5,i,1},\ \mathsf{G}_{5,i,2},\ \boxed{\mathsf{G}_{5,i,3},\ \mathsf{G}_{5,i,4}}}$
$\mathsf{pk}'_\lambda := \mathsf{THPS.PKTran}(\mathsf{pk}, f_\lambda) \in \mathcal{PK}$.
If $1 \le \lambda < i$,
    $C_\lambda \leftarrow_\$ \mathcal{V}$ with witness $w_\lambda$.
    $K_\lambda \leftarrow_\$ \mathcal{K}$.
If $\lambda = i$,
    $C_i \leftarrow_\$ \mathcal{V}$ with witness $w_i$.
    $\boxed{C_i \leftarrow_\$ \mathcal{C} \setminus \mathcal{V}.}$
    $t_i := \mathsf{H}(\mathsf{pk}'_i, m_i, C_i) \in \mathcal{T}$.
    $K_i := \Lambda_{\mathsf{sk}'_i}(C_i, t_i) \in \mathcal{K}$.
    $\boxed{K_i \leftarrow_\$ \mathcal{K}.}$
If $i < \lambda \le Q_t$,
    $C_\lambda \leftarrow_\$ \mathcal{V}$ with witness $w_\lambda$.
    $t_\lambda := \mathsf{H}(\mathsf{pk}'_\lambda, m_\lambda, C_\lambda) \in \mathcal{T}$.
    $K_\lambda := \Lambda_{\mathsf{sk}'_\lambda}(C_\lambda, t_\lambda) \in \mathcal{K}$.
$\mathcal{Q}_{\mathcal{TAG}} := \mathcal{Q}_{\mathcal{TAG}} \cup \{\ (f_\lambda, m_\lambda, \langle C_\lambda, K_\lambda \rangle)\ \}$.
Return $\langle C_\lambda, K_\lambda \rangle$.
```

```
$\underline{\textsc{Vrfy}\big(f \in \mathcal{F}, m, \langle C, K' \rangle\big):}$
    // $\mathsf{G}_{5,i,0}$, $\mathsf{G}_{5,i,1}$, $\mathsf{G}_{5,i,2}$, $\mathsf{G}_{5,i,3}$, $\mathsf{G}_{5,i,4}$
$\mathsf{pk}' := \mathsf{THPS.PKTran}(\mathsf{pk}, f) \in \mathcal{PK}$.
If $C \notin \mathcal{C}$, Return 0.
$t := \mathsf{H}(\mathsf{pk}', m, C) \in \mathcal{T}$.
If $t = t_\lambda$ for some $\lambda$,
    If $(f, m, C) = (f_\lambda, m_\lambda, C_\lambda)$,
        $K := K_\lambda \in \mathcal{K}$.
    If $(f, m, C) \neq (f_\lambda, m_\lambda, C_\lambda)$,
        Return 0.
Else $t \neq t_\lambda$ for all $\lambda$,
    If $C \in \mathcal{C} \setminus \mathcal{V}$, Return 0.
    Else $C \in \mathcal{V}$,
        $K := \Lambda_{\mathsf{sk}'}(C, t) \in \mathcal{K}$.
If $K' = K$, Return 1.
    If $(f, m, \langle C, K' \rangle) \notin \mathcal{Q}_{\mathcal{TAG}}$, Set $\mathsf{forge} := \mathsf{true}$.
Else, Return 0.

$\underline{\textsc{Initialize} \ \&\ \textsc{Finalize}.}$    // same as in Fig. 5
```

Fig. 6. Games $\{\mathsf{G}_{5,i,0}–\mathsf{G}_{5,i,4}\}_{i\in[Q_t]}$, $\mathsf{G}_{5,Q_t+1,0}$ for super-strong EU-$\mathcal{F}$-RK-CMVA security of $\mathsf{MAC}[\mathsf{THPS}]$.

Let $\widetilde{\mathsf{Bad}}$ denote the event that $\mathcal{A}$ ever queries $\textsc{Vrfy}(f, m, \langle C, K' \rangle)$, such that $t \neq t_\lambda$ for all λ and $C \in \mathcal{C} \setminus \mathcal{V}$ but $K' = K$. Clearly games $\mathsf{G}_{5,i,1}$ and $\mathsf{G}_{5,i,2}$ are the same until $\widetilde{\mathsf{Bad}}$ occurs, thus $\big|\Pr_{5,i,1}[\mathsf{Forge}] - \Pr_{5,i,2}[\mathsf{Forge}]\big| \le \Pr_{5,i,2}[\widetilde{\mathsf{Bad}}]$.

We give an upper bound on $\Pr_{5,i,2}[\widetilde{\mathsf{Bad}}]$ via the following lemma.

Lemma 4. *For all* $i \in [Q_t]$, $\Pr_{5,i,2}[\widetilde{\mathsf{Bad}}] \le Q_v \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

Proof. It adapts a similar proofing technique used in the proof of Lemma 3. We analyze the information about sk that $\mathcal{A}$ may obtain in $\mathsf{G}_{5,i,2}$.

- For $\textsc{Tag}(f_\lambda, m_\lambda)$, the challenger uses $\mathsf{pk} = \mu(\mathsf{sk})$ to compute $\mathsf{pk}'_\lambda = \mathsf{THPS.PKTran}(\mathsf{pk}, f_\lambda)$.
  - If $1 \le \lambda < i$, the challenger does not use sk to compute K_λ since K_λ is randomly chosen from $\mathcal{K}$.
  - If $i < \lambda \le Q_t$, the challenger can use pk'_λ to compute K_λ:

$$\begin{aligned} K_\lambda &= \Lambda_{\mathsf{sk}'_\lambda}(C_\lambda, t_\lambda) && : \ C_\lambda \leftarrow_\$ \mathcal{V} \text{ with witness } w_\lambda \\ &= \mathsf{THPS.Pub}(\mathsf{pk}'_\lambda, C_\lambda, w_\lambda, t_\lambda) && : \ \text{via projective property.} \end{aligned}$$

  - If $\lambda = i$, the challenger may leak the value of $K_i = \Lambda_{\mathsf{sk}'_i}(C_i, t_i) = \Lambda_{f_i(\mathsf{sk})}(C_i, t_i)$ to $\mathcal{A}$, where $C_i \leftarrow_\$ \mathcal{C} \setminus \mathcal{V}$.
- For $\textsc{Vrfy}\big(f, m, \langle C, K' \rangle\big)$, the challenger uses pk to compute $\mathsf{pk}' = \mathsf{THPS.PKTran}(\mathsf{pk}, f)$.
  - If $t = t_\lambda \wedge (f, m, C) = (f_\lambda, m_\lambda, C_\lambda)$ for some λ, the challenger does not use sk at all but simply sets $K = K_\lambda$.

- If $t = t_\lambda \wedge (f, m, C) \neq (f_\lambda, m_\lambda, C_\lambda)$ for some λ, the challenger does not use sk and returns 0 directly.
- If $t \neq t_\lambda$ for all λ and $C \in \mathcal{C} \setminus \mathcal{V}$, the challenger returns 0 directly.
- If $t \neq t_\lambda$ for all λ and $C \in \mathcal{V}$, the challenger computes $K = \Lambda_{\mathsf{sk}'}(C, t)$, which leaks at most pk' to $\mathcal{A}$ since THPS is projective.

Thus the only information about sk that $\mathcal{A}$ may get in game $\mathsf{G}_{5,i,2}$ is $\mathsf{pk} = \mu(\mathsf{sk})$ and $K_i = \Lambda_{f_i(\mathsf{sk})}(C_i, t_i)$, where $C_i \leftarrow_{\$} \mathcal{C} \setminus \mathcal{V}$.

The event $\widetilde{\mathsf{Bad}}$ occurs in game $\mathsf{G}_{5,i,2}$ means that $\mathcal{A}$ ever queries $\textsc{Vrfy}(f, m, \langle C, K' \rangle)$ such that $t \neq t_\lambda$ for all λ and $C \in \mathcal{C} \setminus \mathcal{V}$ but $K' = K$, where $K := \Lambda_{\mathsf{sk}'}(C, t) = \Lambda_{f(\mathsf{sk})}(C, t)$.

Since $C \in \mathcal{C} \setminus \mathcal{V}$ and $t \neq t_\lambda$ for all λ, particularly $t \neq t_i$, by the $\mathcal{F}$-universal$_2$ property of THPS, the guessing probability of $K = \Lambda_{f(\mathsf{sk})}(C, t)$ is at most $\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$ conditioned on $\mathsf{pk} = \mu(\mathsf{sk})$ and $K_i = \Lambda_{f_i(\mathsf{sk})}(C_i, t_i)$. Thus $K' = K$ will hold with probability at most $\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$. By a union bound, we get that $\Pr_{5,i,2}[\widetilde{\mathsf{Bad}}] \leq Q_v \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$ and the lemma follows. ▌

Therefore, $\big|\Pr_{5,i,1}[\mathsf{Forge}] - \Pr_{5,i,2}[\mathsf{Forge}]\,\big| \leq \Pr_{5,i,2}[\widetilde{\mathsf{Bad}}] \leq Q_v \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

- Game $\mathsf{G}_{5,i,3}$, $i \in [Q_t]$: This game is the same as game $\mathsf{G}_{5,i,2}$, except that, in the i-th $\textsc{Tag}$ query, the challenger samples K_i uniformly from $\mathcal{K}$ instead of computing $K_i := \Lambda_{\mathsf{sk}'_i}(C_i, t_i) = \Lambda_{f_i(\mathsf{sk})}(C_i, t_i)$.

  Recall that in the proof of Lemma 4, we observe that the only information about sk that $\mathcal{A}$ may get in game $\mathsf{G}_{5,i,2}$ is $\mathsf{pk} = \mu(\mathsf{sk})$ and $K_i = \Lambda_{f_i(\mathsf{sk})}(C_i, t_i)$, where $C_i \leftarrow_{\$} \mathcal{C} \setminus \mathcal{V}$. By the average-case $\mathcal{F}$-strongly-universal$_1$ property of THPS, the joint distribution of $(\mathsf{pk}, C_i, K_i = \Lambda_{f_i(\mathsf{sk})}(C_i, t_i))$ in game $\mathsf{G}_{5,i,2}$ is statistically close to $(\mathsf{pk}, C_i, K_i = \mathsf{U}_{\mathcal{K}})$, and the statistical distance is upper-bounded by $\epsilon^{\mathit{ac\text{-}str\text{-}u_1}}_{\mathsf{THPS},\mathcal{F}}(\ell)$. The latter distribution is exactly the one used in game $\mathsf{G}_{5,i,3}$.

  Thus, games $\mathsf{G}_{5,i,2}$ and $\mathsf{G}_{5,i,3}$ are statistically close with statistical distance up to $\epsilon^{\mathit{ac\text{-}str\text{-}u_1}}_{\mathsf{THPS},\mathcal{F}}(\ell)$, i.e., $\big|\Pr_{5,i,2}[\mathsf{Forge}] - \Pr_{5,i,3}[\mathsf{Forge}]\,\big| \leq \epsilon^{\mathit{ac\text{-}str\text{-}u_1}}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

- Game $\mathsf{G}_{5,i,4}$, $i \in [Q_t]$: This game is the same as game $\mathsf{G}_{5,i,3}$, except that, when answering $\textsc{Vrfy}\big(f, m, \langle C, K' \rangle\big)$, if $t \neq t_\lambda$ for all λ and $C \in \mathcal{C} \setminus \mathcal{V}$, the challenger checks whether or not $K' = K$ again, instead of returning 0 directly. That is, the challenger will check whether or not $K' = K$ no matter $C \in \mathcal{V}$ or $C \in \mathcal{C} \setminus \mathcal{V}$.

  The analysis of the difference between games $\mathsf{G}_{5,i,3}$ and $\mathsf{G}_{5,i,4}$ is analogous to that between $\mathsf{G}_{5,i,1}$ and $\mathsf{G}_{5,i,2}$, thus we omit it here. Similarly, we can get that $\big|\Pr_{5,i,3}[\mathsf{Forge}] - \Pr_{5,i,4}[\mathsf{Forge}]\,\big| \leq Q_v \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

Next we analyze the difference between games $\mathsf{G}_{5,i,4}$ and $\mathsf{G}_{5,i+1,0}$. The only divergence is the distribution of C_i in the i-th query of $\textsc{Tag}$. In game $\mathsf{G}_{5,i,4}$, C_i is uniformly chosen from $\mathcal{C} \setminus \mathcal{V}$, while in game $\mathsf{G}_{5,i+1,0}$, it is uniformly chosen from $\mathcal{V}$. It is easy to construct a PPT adversary to solve the SMP related to THPS, such that $\big|\Pr_{5,i,4}[\mathsf{Forge}] - \Pr_{5,i+1,0}[\mathsf{Forge}]\,\big| \leq \mathsf{Adv}^{\mathit{smp}}_{\mathsf{THPS}}(\ell)$.

- Game G_6: This game is the same as game $\mathsf{G}_{5,Q_t+1,0}$. Then $\Pr_{5,Q_t+1,0}[\mathsf{Forge}] = \Pr_6[\mathsf{Forge}]$. Finally we give an upper bound on $\Pr_6[\mathsf{Forge}]$ as follows.

  In game G_6, each K_λ ($\lambda \in [Q_t]$) is randomly chosen from $\mathcal{K}$ and the challenger does not use sk at all in $\textsc{Tag}$, hence sk is totally uniformly random to the adversary until $\mathcal{A}$ makes the first $\textsc{Vrfy}$ query.

  Suppose that $\mathcal{A}$ submits the first $\textsc{Vrfy}$ query $(f, m, \langle C, K' \rangle)$, then Forge occurs if and only if $t \neq t_\lambda$ for all λ, $K' = K$ and $(f, m, \langle C, K' \rangle) \notin \mathcal{Q}_{\mathcal{TAG}}$, where $K := \Lambda_{\mathsf{sk}'}(C, t) = \Lambda_{f(\mathsf{sk})}(C, t)$.

According to the $\mathcal{F}$-extracting property of THPS, the guessing probability of $K = \Lambda_{f(\mathsf{sk})}(C, t)$ is at most $\epsilon^{ext}_{\mathsf{THPS},\mathcal{F}}(\ell)$ for $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$. Thus $K' = K$ will hold with probability at most $\epsilon^{ext}_{\mathsf{THPS},\mathcal{F}}(\ell)$. By a hybrid argument over Q_v times of $\textsc{Vrfy}$ queries, $\Pr_6[\mathsf{Forge}] \le Q_v \cdot \epsilon^{ext}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

Taking all things together, we have that

$$\begin{aligned}\mathsf{Adv}^{sup\text{-}str\text{-}eu\text{-}rk\text{-}cmva}_{\mathsf{MAC[THPS]},\mathcal{F},\mathcal{A}}(\ell) \le{}& \mathsf{Adv}^{cr}_{\mathcal{H}}(\ell) + \mathsf{Adv}^{pkcp}_{\mathsf{THPS}}(\ell) + 2Q_t \cdot \mathsf{Adv}^{smp}_{\mathsf{THPS}}(\ell) + Q_t \cdot \epsilon^{ac\text{-}str\text{-}u_1}_{\mathsf{THPS},\mathcal{F}}(\ell) \\ &+ (Q_v + Q_v \cdot Q_t \cdot p(\ell) + 2Q_t \cdot Q_v) \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell) + Q_v \cdot \epsilon^{ext}_{\mathsf{THPS},\mathcal{F}}(\ell),\end{aligned}$$

thus the super-strong EU-$\mathcal{F}$-RK-CMVA security of $\mathsf{MAC[THPS]}$ follows. ▮

5 Super-Strong RKA secure PKE and SE from THPS

In this section, we propose a new RKA security notion for (canonical) PKE, called *super-strong IND-$\mathcal{F}$-RK-CCA2*, which is even stronger than the strong IND-$\mathcal{F}$-RK-CCA2 security defined in [BPT12]. Then we give a paradigm for constructing PKE from THPS with the help of Authenticated Encryption (AE). The obtained PKE possesses our new RKA security when the THPS is an $\mathcal{F}$-tailored one.

We also show that the natural transformation from PKE to Symmetric Encryption (SE) converts a super-strong IND-$\mathcal{F}$-RK-CCA2 secure PKE scheme to a SE scheme possessing a new RKA security, which we call it *super-strong IND-$\mathcal{F}$-RK-CCA2*. The super-strong IND-$\mathcal{F}$-RK-CCA2 security for SE is stronger than the IND-$\mathcal{F}$-RK-CCA2 security defined in [BCM11].

5.1 Super-Strong IND-$\mathcal{F}$-RK-CCA2 Security for PKE

Let $\mathcal{F}$ be a class of functions from $\mathcal{SK}$ to $\mathcal{SK}$. The strong IND-$\mathcal{F}$-RK-CCA2 security notion for (canonical) PKE (cf. Definition 2) allows the adversary to get a challenge ciphertext c^* through $\mathrm{LR}(f^*, m_0, m_1)$, which encrypts m_b under $\mathcal{F}$-related public key $\mathsf{pk}'^* = \mathsf{PKE.PK}(\mathsf{sk}'^*)$, where $\mathsf{sk}'^* = f^*(\mathsf{sk})$. However, the decryption oracle $\textsc{Dec}(f, c)$ is a bit restricted: it prohibits decryption of the challenger ciphertext c^* under the corresponding $\mathcal{F}$-related secret key sk'^*. In other words, if the adversary queries $\textsc{Dec}(f, c)$ such that $(f(\mathsf{sk}), c) = (\mathsf{sk}'^*, c^*)$, the decryption oracle does not work. But this restriction is by no means reasonable. The adversary does not own the secret key sk, thus it might not even realize $(f(\mathsf{sk}), c) = (\mathsf{sk}'^*, c^*)$.

Here we relax the decryption restriction, and define an enhanced security notion for PKE, namely *super-strong IND-$\mathcal{F}$-RK-CCA2 security*. That is, we allow the adversary to query $\textsc{Dec}(f, c)$ even if it has queried $\mathrm{LR}(f^*, m_0, m_1)$ such that $(f(\mathsf{sk}), c) = (f^*(\mathsf{sk}), c^*)$, as long as $(f, c) \neq (f^*, c^*)$.

```
Procedure Initialize:
    $\mathsf{prm} \leftarrow_{\$} \mathsf{PKE.Setup}(1^\ell)$.
    $\mathsf{sk} \leftarrow_{\$} \mathsf{PKE.SK}(\mathsf{prm})$.
    $\mathsf{pk} := \mathsf{PKE.PK}(\mathsf{sk}) \in \mathcal{PK}$.
    $b \leftarrow_{\$} \{0, 1\}$.
    Return $(\mathsf{prm}, \mathsf{pk})$.

Proc. LR($f^* \in \mathcal{F}, m_0, m_1$):
    // one query
    $\mathsf{sk}'^* := f^*(\mathsf{sk}) \in \mathcal{SK}$.
    $\mathsf{pk}'^* := \mathsf{PKE.PK}(\mathsf{sk}'^*) \in \mathcal{PK}$.
    $c^* \leftarrow_{\$} \mathsf{PKE.Enc}(\mathsf{pk}'^*, m_b)$.
    $\mathcal{Q_{ENC}} := \{(f^*, c^*)\}$.
    Return $c^*$.

Procedure Enc($f \in \mathcal{F}, m$):
    $\mathsf{sk}' := f(\mathsf{sk}) \in \mathcal{SK}$.
    $\mathsf{pk}' := \mathsf{PKE.PK}(\mathsf{sk}') \in \mathcal{PK}$.
    $c \leftarrow_{\$} \mathsf{PKE.Enc}(\mathsf{pk}', m)$.
    Return $c$.

Procedure Dec($f \in \mathcal{F}, c$):
    If $(f, c) \in \mathcal{Q_{ENC}}$, Return $\perp$.
    $\mathsf{sk}' := f(\mathsf{sk}) \in \mathcal{SK}$.
    Return $\mathsf{PKE.Dec}(\mathsf{sk}', c)$.

Procedure Finalize($b'$):
    Return $(b' = b)$.
```

Fig. 7. super-strong-IND-$\mathcal{F}$-RK-CCA2 security game for PKE.

Definition 19 (Super-Strong IND-$\mathcal{F}$-RK-CCA2 Security for PKE). PKE *is super-strong IND-$\mathcal{F}$-RK-CCA2 secure, if for any PPT adversary $\mathcal{A}$, the advantage* $\mathsf{Adv}^{\textit{sup-str-ind-rk-cca2}}_{\mathsf{PKE},\mathcal{F},\mathcal{A}}(\ell) := \big|\Pr[\mathsf{super\text{-}strong\text{-}IND\text{-}}\mathcal{F}\mathsf{\text{-}RK\text{-}CCA2}^{\mathcal{A}} \Rightarrow 1] - \frac{1}{2}\big|$ *is negligible in ℓ, where game* $\mathsf{super\text{-}strong\text{-}IND\text{-}}\mathcal{F}\mathsf{\text{-}RK\text{-}CCA2}$ *is shown in Fig. 7.*

5.2 The Construction

Let $\mathsf{THPS} = (\mathsf{THPS.Setup}, \mathsf{THPS.Pub}, \mathsf{THPS.Priv})$ be a tag-based hash proof system with instance space $\mathcal{C}$, tag space $\mathcal{T}$, key space $\mathcal{K}$, public key space $\mathcal{PK}$, and hashing key space $\mathcal{SK}$. Let $\mathsf{AE} = (\mathsf{AE.Enc}, \mathsf{AE.Dec})$ be an authenticated encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}_{\mathsf{AE}}$ (cf. Appendix A.1). Let $\mathcal{H}_1 = \{\mathsf{H}_1 : \mathcal{PK} \times \mathcal{C} \longrightarrow \mathcal{T}\}$ and $\mathcal{H}_2 = \{\mathsf{H}_2 : \mathcal{K} \longrightarrow \mathcal{K}_{\mathsf{AE}}\}$ be families of hash functions. The proposed PKE scheme $\mathsf{PKE}[\mathsf{THPS}, \mathsf{AE}] = (\mathsf{PKE.Setup}, \mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ with secret key space $\mathcal{SK}$ ad message space $\mathcal{M}$ is defined in Fig. 8. The correctness of $\mathsf{PKE}[\mathsf{THPS}, \mathsf{AE}]$ follows from the projectiveness of THPS and the correctness of AE directly.

```
$\mathsf{prm} \leftarrow_{\$} \mathsf{PKE.Setup}(1^\ell)$:
$\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^\ell)$.
$\mathsf{H}_1 \leftarrow_{\$} \mathcal{H}_1$.    $\mathsf{H}_2 \leftarrow_{\$} \mathcal{H}_2$.
Return $\mathsf{prm} := (\mathsf{prm}_{\mathsf{THPS}}, \mathsf{H}_1, \mathsf{H}_2)$.

$(\mathsf{pk}, \mathsf{sk}) \leftarrow_{\$} \mathsf{PKE.Gen}(\mathsf{prm})$:
$\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$.    $\mathsf{pk} := \mu(\mathsf{sk}) \in \mathcal{PK}$.
Return $(\mathsf{pk}, \mathsf{sk})$.
```

```
$\langle C, \chi \rangle \leftarrow_{\$} \mathsf{PKE.Enc}(\mathsf{pk}, m)$:
$C \leftarrow_{\$} \mathcal{V}$ together with witness $w$.
$t := \mathsf{H}_1(\mathsf{pk}, C) \in \mathcal{T}$.
$K := \mathsf{THPS.Pub}(\mathsf{pk}, C, w, t) \in \mathcal{K}$.
$\kappa := \mathsf{H}_2(K) \in \mathcal{K}_{\mathsf{AE}}$.
$\chi \leftarrow_{\$} \mathsf{AE.Enc}(\kappa, m)$.
Return $\langle C, \chi \rangle$.
```

```
$m/\perp \leftarrow \mathsf{PKE.Dec}(\mathsf{sk}, \langle C, \chi \rangle)$:
$\mathsf{pk} := \mu(\mathsf{sk}) \in \mathcal{PK}$.
If $C \notin \mathcal{C}$, Return $\perp$.
$t := \mathsf{H}_1(\mathsf{pk}, C) \in \mathcal{T}$.
$K := \mathsf{THPS.Priv}(\mathsf{sk}, C, t) \in \mathcal{K}$.
$\kappa := \mathsf{H}_2(K) \in \mathcal{K}_{\mathsf{AE}}$.
$m/\perp \leftarrow \mathsf{AE.Dec}(\kappa, \chi)$.
Return $m/\perp$.
```

Fig. 8. Construction of $\mathsf{PKE}[\mathsf{THPS}, \mathsf{AE}]$.

Obviously, $\mathsf{PKE}[\mathsf{THPS}, \mathsf{AE}]$ is canonical, where $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$ and $\mathsf{pk} := \mu(\mathsf{sk})$.

Theorem 2. *If $\mathcal{H}_1$ is collision-resistant, $\mathcal{H}_2$ is universal,* AE *is OT-secure (cf. Definition 23 in Appendix A.1),* THPS *is an $\mathcal{F}$-tailored THPS*[3] *such that $|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$ and $|\mathcal{K}_{\mathsf{AE}}|/|\mathcal{K}|$ are both negligible in ℓ, and the SMP and PKCP related to* THPS *are both hard, then the* $\mathsf{PKE}[\mathsf{THPS}, \mathsf{AE}]$ *in Fig. 8 is super-strong IND-$\mathcal{F}$-RK-CCA2 secure.*

Proof of Theorem 2. Suppose that $\mathcal{A}$ is a PPT adversary against the super-strong IND-$\mathcal{F}$-RK-CCA2 security of $\mathsf{PKE}[\mathsf{THPS}, \mathsf{AE}]$, who makes at most Q_d times of Dec queries. We prove the theorem by defining a sequence of games as in Fig. 9, and proving the adjacent games indistinguishable.

- Game G_0: This is the $\mathsf{super\text{-}strong\text{-}IND\text{-}}\mathcal{F}\mathsf{\text{-}RK\text{-}CCA2}$ game (cf. Fig. 7). Let Win denote the event that $b' = b$. Then by definition, $\mathsf{Adv}^{\textit{sup-str-ind-rk-cca2}}_{\mathsf{PKE}[\mathsf{THPS},\mathsf{AE}],\mathcal{F},\mathcal{A}}(\ell) = \big|\Pr_0[\mathsf{Win}] - \frac{1}{2}\big|$.

- Games $\mathsf{G}_1 - \mathsf{G}_6$: These games are defined similarly to that in the proof of Theorem 1. We put the detailed description and analysis in Appendix C. Here we just sketch each game.

[3] We note that the $\mathcal{F}$-extracting property is not necessary here, since in the proof of the theorem, the adversary always knows the public key pk in the scenario of PKE.

```
INITIALIZE:                         // $\mathsf{G}_0$–$\mathsf{G}_9$
$\mathsf{prm}_{\mathsf{THPS}} \leftarrow\$ \mathsf{THPS.Setup}(1^\ell)$.
$\mathsf{H}_1 \leftarrow\$ \mathcal{H}_1$.   $\mathsf{H}_2 \leftarrow\$ \mathcal{H}_2$.
$\mathsf{sk} \leftarrow\$ \mathcal{SK}$.   $\mathsf{pk} := \mu(\mathsf{sk}) \in \mathcal{PK}$.
$b \leftarrow\$ \{0,1\}$.                 // challenge bit
Return $(\mathsf{prm} := (\mathsf{prm}_{\mathsf{THPS}}, \mathsf{H}_1, \mathsf{H}_2), \mathsf{pk})$.

DEC$\big(f \in \mathcal{F}, \langle C, \chi \rangle\big)$: // $\mathsf{G}_0$, $\boxed{\mathsf{G}_1\text{–}\mathsf{G}_9}$, $\boxed{\mathsf{G}_2\text{–}\mathsf{G}_9}$
    // $\boxed{\mathsf{G}_3\text{–}\mathsf{G}_9}$, $\boxed{\mathsf{G}_4\text{–}\mathsf{G}_9}$, $\mathsf{G}_5\text{–}\mathsf{G}_9$, $\boxed{\mathsf{G}_8\text{–}\mathsf{G}_9}$
If $(f, \langle C, \chi \rangle) \in \mathcal{Q}_{\mathcal{ENC}}$, Return $\perp$.
$\mathsf{sk}' := f(\mathsf{sk}) \in \mathcal{SK}$.   $\mathsf{pk}' := \mu(\mathsf{sk}') \in \mathcal{PK}$.
$\boxed{\mathsf{pk}' := \mathsf{THPS.PKTran}(\mathsf{pk}, f) \in \mathcal{PK}.}$
If $C \notin \mathcal{C}$, Return $\perp$.
$t := \mathsf{H}_1(\mathsf{pk}', C) \in \mathcal{T}$.
If $t = t^*$,
    If $(f, C) = (f^*, C^*)$,
        $\kappa := \kappa^* \in \mathcal{K}_{\mathsf{AE}}$.
        $\boxed{\text{Return } \perp.}$
    $\boxed{\text{If } C \neq C^* \vee (C = C^* \wedge \mathsf{pk}' \neq \mathsf{pk}'^*),}$
        $\boxed{\text{Return } \perp.}$
    $\boxed{\text{If } C = C^* \wedge \mathsf{pk}' = \mathsf{pk}'^* \wedge \mathsf{sk}' \neq \mathsf{sk}'^*,}$
        $\boxed{\text{Return } \perp.}$
    If $C = C^* \wedge \mathsf{sk}' = \mathsf{sk}'^* \wedge f \neq f^*$,
        Return $\perp$.
Else $t \neq t^*$,
    $K := \Lambda_{\mathsf{sk}'}(C, t) \in \mathcal{K}$.
    $\kappa := \mathsf{H}_2(K) \in \mathcal{K}_{\mathsf{AE}}$.
Return $\mathsf{AE.Dec}(\kappa, \chi)$.

LR$(f^* \in \mathcal{F}, m_0, m_1)$:        // one query
    // $\mathsf{G}_0$, $\boxed{\mathsf{G}_1\text{–}\mathsf{G}_9}$, $\boxed{\mathsf{G}_6\text{–}\mathsf{G}_9}$, $\boxed{\mathsf{G}_7\text{–}\mathsf{G}_9}$, $\mathsf{G}_9$
$\mathsf{sk}'^* := f^*(\mathsf{sk}) \in \mathcal{SK}$.   $\mathsf{pk}'^* := \mu(\mathsf{sk}'^*) \in \mathcal{PK}$.
$\boxed{\mathsf{pk}'^* := \mathsf{THPS.PKTran}(\mathsf{pk}, f^*) \in \mathcal{PK}.}$
$C^* \leftarrow\$ \mathcal{V}$ together with witness $w^*$.
$t^* := \mathsf{H}_1(\mathsf{pk}'^*, C^*) \in \mathcal{T}$.
$K^* := \mathsf{THPS.Pub}(\mathsf{pk}'^*, C^*, w^*, t^*) \in \mathcal{K}$.
$\boxed{K^* := \Lambda_{\mathsf{sk}'^*}(C^*, t^*) \in \mathcal{K}.}$
$\boxed{K^* \leftarrow\$ \mathcal{K}.}$
$\kappa^* := \mathsf{H}_2(K^*) \in \mathcal{K}_{\mathsf{AE}}$.
$\boxed{\kappa^* \leftarrow\$ \mathcal{K}_{\mathsf{AE}}.}$
$\chi^* \leftarrow\$ \mathsf{AE.Enc}(\kappa^*, m_b)$.
$\chi^* \leftarrow\$ \mathsf{AE.Enc}(\kappa^*, 0^{|m_0|})$.
$\mathcal{Q}_{\mathcal{ENC}} := \big\{(f^*, \langle C^*, \chi^* \rangle)\big\}$.
Return $\langle C^*, \chi^* \rangle$.

ENC$(f \in \mathcal{F}, m)$:           // $\mathsf{G}_0$, $\boxed{\mathsf{G}_1\text{–}\mathsf{G}_9}$
$\mathsf{sk}' := f(\mathsf{sk}) \in \mathcal{SK}$.   $\mathsf{pk}' := \mu(\mathsf{sk}') \in \mathcal{PK}$.
$\boxed{\mathsf{pk}' := \mathsf{THPS.PKTran}(\mathsf{pk}, f) \in \mathcal{PK}.}$
$C \leftarrow\$ \mathcal{V}$ together with witness $w$.
$t := \mathsf{H}_1(\mathsf{pk}', C) \in \mathcal{T}$.
$K := \mathsf{THPS.Pub}(\mathsf{pk}', C, w, t) \in \mathcal{K}$.
$\kappa := \mathsf{H}_2(K) \in \mathcal{K}_{\mathsf{AE}}$.
$\chi \leftarrow\$ \mathsf{AE.Enc}(\kappa, m)$.
Return $\langle C, \chi \rangle$.

FINALIZE$(b')$:                  // $\mathsf{G}_0$–$\mathsf{G}_9$
Return $(b' = b)$.
```

Fig. 9. Games G_0–G_9 for super-strong IND-$\mathcal{F}$-RK-CCA2 security of $\mathsf{PKE}[\mathsf{THPS}, \mathsf{AE}]$.

In game G_1, the challenger changes the way it computes pk'^*, K^* in LR and pk' in ENC and DEC. More precisely, the challenger simply invokes the $\mathcal{F}$-public-key transformer $\mathsf{THPS.PKTran}$ to compute $\mathsf{pk}'^* := \mathsf{THPS.PKTran}(\mathsf{pk}, f^*)$ in LR and $\mathsf{pk}' := \mathsf{THPS.PKTran}(\mathsf{pk}, f)$ in ENC and DEC. Besides, it computes $K^* := \Lambda_{\mathsf{sk}'^*}(C^*, t^*)$ rather than $K^* := \mathsf{THPS.Pub}(\mathsf{pk}'^*, C^*, w^*, t^*)$ in LR. By the $\mathcal{F}$-public-key-homomorphic property of THPS and the projectiveness of THPS, the change is conceptual. Then $\Pr_0[\mathsf{Win}] = \Pr_1[\mathsf{Win}]$.

In game G_2, when answering DEC$\big(f, \langle C, \chi \rangle\big)$, if $t = t^* \wedge (f, C) = (f^*, C^*)$, the challenger directly sets $\kappa := \kappa^*$ instead of computing $\kappa := \mathsf{H}_2(K)$. Since κ (resp. κ^*) is uniquely determined by (f, C, t) (resp. (f^*, C^*, t^*)) and sk, the change is conceptual. Then $\Pr_1[\mathsf{Win}] = \Pr_2[\mathsf{Win}]$.

In game G_3, when answering DEC$\big(f, \langle C, \chi \rangle\big)$, if $t = t^* \wedge \big(C \neq C^* \vee (C = C^* \wedge \mathsf{pk}' \neq \mathsf{pk}'^*)\big)$, the challenger returns $\perp$ directly. Since $\mathcal{H}_1$ is collision-resistant, $\big|\Pr_2[\mathsf{Win}] - \Pr_3[\mathsf{Win}]\big| \leq \mathsf{Adv}^{cr}_{\mathcal{H}_1}(\ell)$.

In game G_4, when answering $\textsc{Dec}\big(f, \langle C, \chi\rangle\big)$, if $t = t^* \wedge C = C^* \wedge \mathsf{pk}' = \mathsf{pk}'^* \wedge \mathsf{sk}' \neq \mathsf{sk}'^*$, the challenger simply returns $\perp$. Since the PKCP related to THPS is hard, $\big|\Pr_3[\mathsf{Win}] - \Pr_4[\mathsf{Win}]\,\big| \leq \mathsf{Adv}^{pkcp}_{\mathsf{THPS}}(\ell)$.

In game G_5, when answering $\textsc{Dec}\big(f, \langle C, \chi\rangle\big)$, if $t = t^* \wedge C = C^* \wedge \mathsf{sk}' = \mathsf{sk}'^* \wedge f \neq f^*$, the challenger directly returns $\perp$. Through a deferred analysis similar to that in the proof of Theorem 1, by the INT-OT security of AE and the fact that THPS has $\mathcal{F}$-poly-bounded collisions, we can get that $\big|\Pr_4[\mathsf{Win}] - \Pr_5[\mathsf{Win}]\,\big| \leq Q_d \cdot \big(\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)\big) + Q_d \cdot p(\ell) \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$ for some polynomial $p(\ell)$.

In game G_6, in $\mathrm{LR}(f^*, m_0, m_1)$, the challenger picks K^* randomly from $\mathcal{K}$. By introducing a sequence of games $\{\mathsf{G}_{5,1}\text{–}\mathsf{G}_{5,4}\}$ between G_5 and G_6 a similar way as that in the proof of Theorem 1, we can obtain that $\big|\Pr_5[\mathsf{Win}] - \Pr_6[\mathsf{Win}]\,\big| \leq 2 \cdot \mathsf{Adv}^{smp}_{\mathsf{THPS}}(\ell) + 2Q_d \cdot \big(\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)\big) + \epsilon^{ac\text{-}str\text{-}u_1}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

Note that in G_6, the challenger answers LR query by sampling K^* randomly from $\mathcal{K}$ and can answer $\textsc{Dec}$ queries without using the secret key sk at all in the case of $t = t^*$.

- Game G_7: This game is the same as game G_6, except that, in $\mathrm{LR}(f^*, m_0, m_1)$, the challenger simply samples $\kappa^* \leftarrow_\$ \mathcal{K}_{\mathsf{AE}}$ randomly instead of computing $\kappa^* := \mathsf{H}_2(K^*)$ where $K^* \leftarrow_\$ \mathcal{K}$.

  In game G_6, K^* is randomly chosen from $\mathcal{K}$ in LR. By the Leftover Hash Lemma (i.e., Lemma 1), since H_2 is universal, $\kappa^* := \mathsf{H}_2(K^*)$ is statistically close to the uniform distribution over $\mathcal{K}_{\mathsf{AE}}$, with statistical distance $\sqrt{|\mathcal{K}_{\mathsf{AE}}|/|\mathcal{K}|}$.

  Therefore G_6 and G_7 are statistically close with statistical distance $\sqrt{|\mathcal{K}_{\mathsf{AE}}|/|\mathcal{K}|}$, i.e., $\big|\Pr_6[\mathsf{Win}] - \Pr_7[\mathsf{Win}]\,\big| \leq \sqrt{|\mathcal{K}_{\mathsf{AE}}|/|\mathcal{K}|}$.

- Game G_8: This game is the same as game G_7, except that, when answering $\textsc{Dec}\big(f, \langle C, \chi\rangle\big)$, if $t = t^* \wedge (f, C) = (f^*, C^*)$, the challenger outputs $\perp$ directly instead of invoking $\mathsf{AE.Dec}(\kappa^*, \chi)$.

  Let Forge denote the event that $\mathcal{A}$ ever queries $\textsc{Dec}\big(f, \langle C, \chi\rangle\big)$, such that $t = t^* \wedge (f, C) = (f^*, C^*) \wedge \chi \neq \chi^*$ but $\mathsf{AE.Dec}(\kappa^*, \chi) \neq \perp$. Note that G_7 and G_8 are the same unless Forge occurs, since $\textsc{Dec}$ queries $(f, \langle C, \chi\rangle) = (f^*, \langle C^*, \chi^*\rangle)$ are rejected both in G_7 and G_8. Then we have that $\big|\Pr_7[\mathsf{Win}] - \Pr_8[\mathsf{Win}]\,\big| \leq \Pr_8[\mathsf{Forge}]$.

  Since $\chi^* \leftarrow_\$ \mathsf{AE.Enc}(\kappa^*, m_b)$ for $\kappa^* \leftarrow_\$ \mathcal{K}_{\mathsf{AE}}$, the event that $\mathcal{A}$ can submit χ such that $\chi \neq \chi^*$ but $\mathsf{AE.Dec}(\kappa^*, \chi) \neq \perp$ directly violates the INT-OT security of AE. It is straightforward to construct a PPT adversary against the INT-OT security of AE, such that $\Pr_8[\mathsf{Forge}] \leq Q_d \cdot \mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)$. Therefore, $\big|\Pr_7[\mathsf{Win}] - \Pr_8[\mathsf{Win}]\,\big| \leq Q_d \cdot \mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)$.

- Game G_9: This game is the same as game G_8, except that, in $\mathrm{LR}(f^*, m_0, m_1)$, the challenger encrypts a constant message $0^{|m_0|}$ instead of m_b.

  Since κ^* is randomly distributed and independent of the other parts of the game, by the IND-OT security of AE, the encryption $\chi^* \leftarrow_\$ \mathsf{AE.Enc}(\kappa^*,\, m_b)$ is computationally indistinguishable from $\chi^* \leftarrow_\$ \mathsf{AE.Enc}(\kappa^*, 0^{|m_0|})$. Thus we can construct a PPT adversary against the IND-OT security of AE, such that $\big|\Pr_8[\mathsf{Win}] - \Pr_9[\mathsf{Win}]\,\big| \leq \mathsf{Adv}^{ind\text{-}ot}_{\mathsf{AE}}(\ell)$.

Finally in game G_9, the challenger encrypts the constant message, thus the challenge bit b is completely hidden. Then $\Pr_9[\mathsf{Win}] = \frac{1}{2}$.

Taking all things together, we have that

$$\begin{aligned}\mathsf{Adv}^{\textit{sup-str-ind-rk-cca2}}_{\mathsf{PKE[THPS,AE]},\mathcal{F},\mathcal{A}}(\ell) \leq \mathsf{Adv}^{cr}_{\mathcal{H}_1}(\ell) + \mathsf{Adv}^{pkcp}_{\mathsf{THPS}}(\ell) + 2\cdot\mathsf{Adv}^{smp}_{\mathsf{THPS}}(\ell) + 4Q_d\cdot\mathsf{Adv}^{\textit{int-ot}}_{\mathsf{AE}}(\ell) + \mathsf{Adv}^{\textit{ind-ot}}_{\mathsf{AE}}(\ell)\\ + \epsilon^{\textit{ac-str-u}_1}_{\mathsf{THPS},\mathcal{F}}(\ell) + Q_d\cdot p(\ell)\cdot\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell) + 3Q_d\cdot\sqrt{|\mathcal{K}_{\mathsf{AE}}|\cdot\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)}\\ + \sqrt{|\mathcal{K}_{\mathsf{AE}}|/|\mathcal{K}|},\end{aligned}$$

thus the super-strong IND-$\mathcal{F}$-RK-CCA2 security of $\mathsf{PKE[THPS,AE]}$ follows assuming that both $|\mathcal{K}_{\mathsf{AE}}|\cdot\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$ and $|\mathcal{K}_{\mathsf{AE}}|/|\mathcal{K}|$ are negligible in ℓ. ▌

5.3 Super-Strong IND-$\mathcal{F}$-RK-CCA2 secure SE from THPS

A (canonical) PKE can be used as a Symmetric Encryption (SE) by setting the secret key sk of PKE as the encryption/decryption key of SE.

In [BCM11], IND-$\mathcal{F}$-RK-CCA2 security was defined for SE. Strong IND-$\mathcal{F}$-RK-CCA2 secure PKE is naturally an IND-$\mathcal{F}$-RK-CCA2 secure SE, as shown in [BPT12]. Given the super-strong IND-$\mathcal{F}$-RK-CCA2 secure PKE scheme $\mathsf{PKE[THPS,AE]}$ constructed in the previous subsection (cf. Fig. 8), we immediately obtain an SE scheme $\mathsf{SE[THPS,AE]}$ with super-strong IND-$\mathcal{F}$-RK-CCA2 security (cf. Fig. 16). Here we point out that the super-strongness property of SE is inherited from PKE.

The syntax and the IND-$\mathcal{F}$-RK-CCA2 security of SE are recalled in Appendix A.2. In Appendix D, we define super-strong IND-$\mathcal{F}$-RK-CCA2 security for SE[4] and present the paradigm for constructing a super-strong IND-$\mathcal{F}$-RK-CCA2 secure SE from any super-strong IND-$\mathcal{F}$-RK-CCA2 secure (canonical) PKE. See Fig. 16 for the paradigm and Theorem 7 for the security analysis. By combining Theorem 2 and Theroem 7, we get the following corollary which shows the super-strong IND-$\mathcal{F}$-RK-CCA2 security of the resulting $\mathsf{SE[THPS,AE]}$.

Corollary 1. *If $\mathcal{H}_1$ is collision-resistant, $\mathcal{H}_2$ is universal,* AE *is OT-secure,* THPS *is an $\mathcal{F}$-tailored THPS such that $|\mathcal{K}_{\mathsf{AE}}|\cdot\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$ and $|\mathcal{K}_{\mathsf{AE}}|/|\mathcal{K}|$ are both negligible in ℓ, and the SMP and PKCP related to* THPS *are both hard, then the* $\mathsf{SE[THPS,AE]}$ *in Fig. 16 is super-strong IND-$\mathcal{F}$-RK-CCA2 secure.*

6 Instantiation of THPS from the Matrix DDH Assumption

In this section, we give an instantiation of $\mathcal{F}_{\mathrm{raff}}$-tailored THPS from the Matrix DDH Assumption, where $\mathcal{F}_{\mathrm{raff}}$ is the class of restricted affine functions. We show that the instantiation enjoys all of the properties required in the paradigms for constructing super-strong RKA secure MAC, PKE and SE.

6.1 GenG, MDDH and KerMDH Assumptions

Let $\mathsf{GenG}(1^\ell)$ be a PPT algorithm outputting $\mathcal{G} = (\mathbb{G}, p, g)$, where p is a 2ℓ-bit prime number, $\mathbb{G}$ is a cyclic (multiplicative) group of order p, and g is a generator of $\mathbb{G}$. We assume that the multiplication in $\mathbb{G}$ is efficiently computable and there is a PPT algorithm for checking membership in $\mathbb{G}$.

[4] There is no strong IND-$\mathcal{F}$-RK-CCA2 security defined for SE. Up to now, the IND-$\mathcal{F}$-RK-CCA2 security defined in [BCM11] is the strongest RKA security notion for SE (before our work). For consistency, we name our new RKA security notion as super-strong IND-$\mathcal{F}$-RK-CCA2.

For a matrix $\mathbf{A}$ over $\mathbb{Z}_p$, denote by $g^{\mathbf{A}}$ the matrix over $\mathbb{G}$ with $(g^{\mathbf{A}})_{i,j} := g^{(\mathbf{A})_{i,j}}$. Obviously, given $\mathbf{A}$, $g^{\mathbf{B}}$, $g^{\mathbf{C}}$ and $\mathbf{D}$ with appropriate dimensions, we can efficiently compute $g^{\mathbf{A}\cdot\mathbf{B}}$, $g^{\mathbf{B}+\mathbf{C}}$ and $g^{\mathbf{C}\cdot\mathbf{D}}$.

Let $s', s \geq 1$ be integers with $s' > s$. A probabilistic distribution $\mathcal{D}_{s',s}$ is called a *matrix distribution*, if it outputs matrices in $\mathbb{Z}_p^{s'\times s}$ of full rank s in polynomial time. Without loss of generality, we assume that the first s rows of $\mathbf{A} \leftarrow\!\$\ \mathcal{D}_{s',s}$ are linearly independent. We define the MDDH assumption according to [EHK$^+$13].

Definition 20 ($\mathcal{D}_{s',s}$-MDDH Assumption). *The $\mathcal{D}_{s',s}$-Matrix DDH ($\mathcal{D}_{s',s}$-MDDH) Assumption holds w.r.t.* GenG*, if for any PPT adversary $\mathcal{A}$, the following advantage is negligible in ℓ:*

$$\mathsf{Adv}^{\mathcal{D}_{s',s}\text{-}mddh}_{\mathsf{GenG},\mathcal{A}}(\ell) := \Big| \Pr\left[\mathcal{A}(\mathcal{G}, g^{\mathbf{A}}, g^{\mathbf{A}\cdot\mathbf{w}}) = 1\right] - \Pr\left[\mathcal{A}(\mathcal{G}, g^{\mathbf{A}}, g^{\mathbf{r}}) = 1\right] \Big|,$$

where $\mathcal{G} = (\mathbb{G}, p, g) \leftarrow\!\$\ \mathsf{GenG}(1^\ell)$, $\mathbf{A} \leftarrow\!\$\ \mathcal{D}_{s',s}$, $\mathbf{w} \leftarrow\!\$\ \mathbb{Z}_p^s$ and $\mathbf{r} \leftarrow\!\$\ \mathbb{Z}_p^{s'}$.

The $\mathcal{D}_{s',s}$-MDDH assumption covers many well-studied assumptions, such as the DDH and the k-LIN assumptions [EHK$^+$13].

We recall the definition of the KerMDH assumption from [MRV15], which is introduced as a computational analogue of the MDDH assumption.

Definition 21 ($\mathcal{D}_{s',s}$-KerMDH Assumption). *The $\mathcal{D}_{s',s}$-Kernel Diffie-Hellman ($\mathcal{D}_{s',s}$-KerMDH) Assumption holds w.r.t.* GenG*, if for any PPT adversary $\mathcal{A}$, the following advantage is negligible in ℓ:*

$$\mathsf{Adv}^{\mathcal{D}_{s',s}\text{-}kmdh}_{\mathsf{GenG},\mathcal{A}}(\ell) := \Pr\left[\mathbf{c} \leftarrow\!\$\ \mathcal{A}(\mathcal{G}, g^{\mathbf{A}}) \ :\ \mathbf{c} \neq \mathbf{0} \ \wedge\ \mathbf{A}^\top \cdot \mathbf{c} = \mathbf{0}\right],$$

where $\mathcal{G} = (\mathbb{G}, p, g) \leftarrow\!\$\ \mathsf{GenG}(1^\ell)$ and $\mathbf{A} \leftarrow\!\$\ \mathcal{D}_{s',s}$.

Lemma 5 ($\mathcal{D}_{s',s}$-MDDH $\Rightarrow$ $\mathcal{D}_{s',s}$-KerMDH [MRV15]). *If the $\mathcal{D}_{s',s}$-MDDH assumption holds w.r.t.* GenG*, so does the $\mathcal{D}_{s',s}$-KerMDH assumption.*

The proof is quite straightforward: given $g^{\mathbf{r}}$ and a non-zero vector $\mathbf{c}$ in the kernel of $\mathbf{A}^\top$, we can efficiently test whether or not $\mathbf{r}$ belongs to the column space of $\mathbf{A}$ by checking $g^{\mathbf{r}^\top\cdot\mathbf{c}} = g^0$.

6.2 THPS$_{\mathsf{MDDH}}$ from the Matrix DDH Assumption

In [QLC15], THPS was constructed based on the k-LIN assumption. Let $\mathcal{D}_{s',s}$ be a matrix distribution that outputs matrices $\mathbf{A}$ in $\mathbb{Z}_p^{s'\times s}$. Here we present an MDDH-based construction $\mathsf{THPS}_{\mathsf{MDDH}}$ in Fig. 10, whose subset membership and public-key collision problems are hard under the $\mathcal{D}_{s',s}$-MDDH assumption.

Theorem 3. *The* $\mathsf{THPS}_{\mathsf{MDDH}}$ *in Fig. 10 is an $\mathcal{F}_{raff}$-tailored THPS, where $\mathcal{F}_{raff} = \big\{ f_{(a,\mathsf{b})} : (\mathbf{k}_1, \mathbf{k}_2) \in \mathcal{SK} \longmapsto (a\mathbf{k}_1 + \mathbf{b}_1, a\mathbf{k}_2 + \mathbf{b}_2) \in \mathcal{SK} \ \big|\ a \in \mathbb{Z}_p^*,\ \mathsf{b} = (\mathbf{b}_1, \mathbf{b}_2) \in \mathcal{SK} \big\}$ is the class of restricted affine functions. More precisely, it is $\mathcal{F}_{raff}$-strongly-universal$_1$, $\mathcal{F}_{raff}$-universal$_2$, $\mathcal{F}_{raff}$-extracting, $\mathcal{F}_{raff}$-public-key-homomorphic and has $\mathcal{F}_{raff}$-poly-bounded collisions.*

Proof of Theorem 3.

[Projectiveness.] For all $\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2) \in \mathcal{SK}$, all $C = g^{\mathbf{A}\cdot\mathbf{w}} \in \mathcal{V}$ with witness $\mathbf{w}$ and all $t \in \mathcal{T}$, it follows that

$$\begin{aligned} \mathsf{THPS.Pub}(\mu(\mathsf{sk}), C, \mathbf{w}, t) &= g^{\mathbf{w}^\top\cdot(\mathbf{A}^\top\cdot\mathbf{k}_1 + t\mathbf{A}^\top\cdot\mathbf{k}_2)} \\ &= g^{(\mathbf{A}\cdot\mathbf{w})^\top\cdot(\mathbf{k}_1 + t\mathbf{k}_2)} = \mathsf{THPS.Priv}(\mathsf{sk}, C, t). \end{aligned}$$

$\underline{\mathsf{prm}_{\mathsf{THPS}} \leftarrow_\$ \mathsf{THPS.Setup}(1^\ell)\text{:}}$

$\mathcal{G} = (\mathbb{G}, p, g) \leftarrow_\$ \mathsf{GenG}(1^\ell)$. $\mathbf{A} \leftarrow_\$ \mathcal{D}_{s',s}$, where $\mathbf{A} \in \mathbb{Z}_p^{s' \times s}$.

Return $\mathsf{prm}_{\mathsf{THPS}} := (\mathcal{G}, g^{\mathbf{A}})$, which implicitly defines $(\mathcal{K}, \mathcal{C}, \mathcal{V}, \mathcal{T}, \mathcal{SK}, \mathcal{PK}, \Lambda_{(\cdot)}, \mu)$:

$\mathcal{K} := \mathbb{G}$. $\quad \mathcal{C} := \mathbb{G}^{s'} \backslash \{g^{\mathbf{0}}\}$. $\quad \mathcal{V} := \{\ g^{\mathbf{A} \cdot \mathbf{w}} \mid \mathbf{w} \in \mathbb{Z}_p^s \backslash \{\mathbf{0}\}\ \}$.

$\mathcal{T} := \mathbb{Z}_p$. $\quad \mathcal{SK} := \mathbb{Z}_p^{s'} \times \mathbb{Z}_p^{s'}$. $\quad \mathcal{PK} := \mathbb{G}^s \times \mathbb{G}^s$.

For $\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2) \in \mathcal{SK}$, $\ C = g^{\mathbf{r}} \in \mathcal{C}$, $\ t \in \mathcal{T}$, $\ \Lambda_{\mathsf{sk}}(C, t) := g^{\mathbf{r}^\top \cdot (\mathbf{k}_1 + t\mathbf{k}_2)} \in \mathcal{K}$.

For $\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2) \in \mathcal{SK}$, $\ \mathsf{pk} = \mu(\mathsf{sk}) := (\ g^{\mathbf{A}^\top \cdot \mathbf{k}_1}\ ,\ g^{\mathbf{A}^\top \cdot \mathbf{k}_2}\ ) \in \mathcal{PK}$.

$\underline{K \leftarrow \mathsf{THPS.Pub}(\mathsf{pk}, C, \mathbf{w}, t)\text{:}}$	$\underline{K \leftarrow \mathsf{THPS.Priv}(\mathsf{sk}, C, t)\text{:}}$
Parse $\mathsf{pk} = (g^{\mathbf{h}_1}, g^{\mathbf{h}_2}) \in \mathcal{PK}$.	Parse $\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2) \in \mathcal{SK}$ and $C = g^{\mathbf{r}} \in \mathcal{C}$.
Return $K := g^{\mathbf{w}^\top \cdot (\mathbf{h}_1 + t\mathbf{h}_2)}$.	Return $K := g^{\mathbf{r}^\top \cdot (\mathbf{k}_1 + t\mathbf{k}_2)}$.

Fig. 10. Construction of $\mathsf{THPS}_{\mathsf{MDDH}}$.

[**$\mathcal{F}_{\text{raff}}$-Strongly-Universal$_1$ & $\mathcal{F}_{\text{raff}}$-Universal$_2$.**] Suppose that $f_{(a,\mathsf{b})}, f_{(a',\mathsf{b}')} \in \mathcal{F}_{\text{raff}}$ with $\mathsf{b} = (\mathbf{b}_1, \mathbf{b}_2)$ and $\mathsf{b}' = (\mathbf{b}_1', \mathbf{b}_2')$, $C = g^{\mathbf{r}} \in \mathcal{C}$, $C' = g^{\mathbf{r}'} \in \mathcal{C} \setminus \mathcal{V}$ and $t, t' \in \mathcal{T}$ with $t \neq t'$. For $\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2) \leftarrow_\$ \mathcal{SK}$, we consider the distribution of $\Lambda_{f_{(a',\mathsf{b}')}(\mathsf{sk})}(C', t')$ conditioned on $\mathsf{pk} = \mu(\mathsf{sk})$ and $\Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$.

Let $\mathbf{a}^\perp \in \mathbb{Z}_p^{s'}$ be a non-zero vector in the kernel of $\mathbf{A}^\top$, such that $\mathbf{A}^\top \cdot \mathbf{a}^\perp = \mathbf{0}$. Note that we can sample $\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2) \leftarrow_\$ \mathcal{SK}$ equivalently via

$$\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2) = (\hat{k}_1 \mathbf{a}^\perp + \hat{\mathbf{k}}_1, \hat{k}_2 \mathbf{a}^\perp + \hat{\mathbf{k}}_2)$$

where $\hat{k}_1, \hat{k}_2 \leftarrow_\$ \mathbb{Z}_p$ and $\hat{\mathbf{k}}_1, \hat{\mathbf{k}}_2 \leftarrow_\$ \mathbb{Z}_p^{s'}$.

Firstly $\mathsf{pk} = \mu(\mathsf{sk}) = (\ g^{\mathbf{A}^\top \cdot \mathbf{k}_1}\ ,\ g^{\mathbf{A}^\top \cdot \mathbf{k}_2}\ ) = (\ g^{\mathbf{A}^\top \cdot \hat{\mathbf{k}}_1}\ ,\ g^{\mathbf{A}^\top \cdot \hat{\mathbf{k}}_2}\ )$, which may leak $\hat{\mathbf{k}}_1, \hat{\mathbf{k}}_2$, but the values of $\hat{k}_1, \hat{k}_2$ are totally hidden.

Next

$$\begin{aligned} \Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t) &= \Lambda_{(a\mathbf{k}_1 + \mathbf{b}_1, a\mathbf{k}_2 + \mathbf{b}_2)}(C, t) = g^{\mathbf{r}^\top \cdot ((a\mathbf{k}_1 + \mathbf{b}_1) + t(a\mathbf{k}_2 + \mathbf{b}_2))} \\ &= \left(g^{\mathbf{r}^\top \cdot (\mathbf{k}_1 + t\mathbf{k}_2)}\right)^a \cdot g^{\mathbf{r}^\top \cdot (\mathbf{b}_1 + t\mathbf{b}_2)} \\ &= \left(g^{\mathbf{r}^\top \mathbf{a}^\perp \cdot (\hat{k}_1 + t\hat{k}_2)}\right)^a \cdot \left(g^{\mathbf{r}^\top \cdot (\hat{\mathbf{k}}_1 + t\hat{\mathbf{k}}_2)}\right)^a \cdot g^{\mathbf{r}^\top \cdot (\mathbf{b}_1 + t\mathbf{b}_2)}, \end{aligned} \tag{5}$$

which may further leak the value of $\hat{k}_1 + t\hat{k}_2$.

Similarly,

$$\Lambda_{f_{(a',\mathsf{b}')}(\mathsf{sk})}(C', t') = \boxed{\left(g^{\mathbf{r}'^\top \mathbf{a}^\perp \cdot (\hat{k}_1 + t'\hat{k}_2)}\right)^{a'}} \cdot \left(g^{\mathbf{r}'^\top \cdot (\hat{\mathbf{k}}_1 + t'\hat{\mathbf{k}}_2)}\right)^{a'} \cdot g^{\mathbf{r}'^\top \cdot (\mathbf{b}_1' + t\mathbf{b}_2')}.$$

Since $t \neq t'$, it follows that $\hat{k}_1 + t'\hat{k}_2$ is independent of $\hat{k}_1 + t\hat{k}_2$ and uniformly distributed over $\mathbb{Z}_p$. Also note that $C' \in \mathcal{C} \setminus \mathcal{V}$ implies that $\mathbf{r}'^\top \mathbf{a}^\perp \neq 0$, and note the fact that $a' \in \mathbb{Z}_p^*$. Thus conditioned on pk and $\Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$, the term $\left(g^{\mathbf{r}'^\top \mathbf{a}^\perp \cdot (\hat{k}_1 + t'\hat{k}_2)}\right)^{a'}$ is randomly distributed over $\mathcal{K} = \mathbb{G}$, so is $\Lambda_{f_{(a',\mathsf{b}')}(\mathsf{sk})}(C', t')$.

This implies that $\mathsf{THPS}_{\mathsf{MDDH}}$ is $\mathcal{F}_{\text{raff}}$-strongly-universal$_1$ with $\epsilon^{\mathit{str}\text{-}u_1}_{\mathsf{THPS},\mathcal{F}_{\text{raff}}}(\ell) = 0$ and $\mathcal{F}_{\text{raff}}$-universal$_2$ with $\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}_{\text{raff}}}(\ell) = 1/p$, which is negligible in ℓ.

[$\mathcal{F}_{\mathbf{raff}}$-Extracting.] Suppose that $f_{(a,\mathsf{b})} \in \mathcal{F}_{\text{raff}}$ with $\mathsf{b} = (\mathbf{b}_1, \mathbf{b}_2)$, $C = g^{\mathbf{r}} \in \mathcal{C}$ with $\mathbf{r} \in \mathbb{Z}_p^{s'}\backslash\{\mathbf{0}\}$ and $t \in \mathcal{T}$. For $\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2) \leftarrow_\$ \mathcal{SK}$, we consider the distribution of $\Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$. By Eq. (5),

$$\Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C,t) = \boxed{\big(g^{\mathbf{r}^\top\cdot(\mathbf{k}_1+t\mathbf{k}_2)}\big)^a}\cdot g^{\mathbf{r}^\top\cdot(\mathbf{b}_1+t\mathbf{b}_2)}.$$

When sk is randomly chosen from $\mathcal{SK}$, $\mathbf{k}_1 + t\mathbf{k}_2$ is uniformly distributed over $\mathbb{Z}_p^{s'}$. Since $\mathbf{r} \neq \mathbf{0}$ and $a \in \mathbb{Z}_p^*$, the term $\big(g^{\mathbf{r}^\top\cdot(\mathbf{k}_1+t\mathbf{k}_2)}\big)^a$ is randomly distributed over $\mathcal{K} = \mathbb{G}$, so is $\Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$.

Therefore, $\mathsf{THPS}_{\mathsf{MDDH}}$ is $\mathcal{F}_{\text{raff}}$-extracting with $\epsilon^{ext}_{\mathsf{THPS},\mathcal{F}_{\text{raff}}}(\ell) = 1/p$, which is negligible in ℓ.

[$\mathcal{F}_{\mathbf{raff}}$-Public-Key-Homomorphism.] For all $f_{(a,\mathsf{b})} \in \mathcal{F}_{\text{raff}}$ with $\mathsf{b} = (\mathbf{b}_1, \mathbf{b}_2)$, and all $\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2) \in \mathcal{SK}$, observe that

$$\begin{aligned}\mu\big(f_{(a,\mathsf{b})}(\mathsf{sk})\big) &= \mu(a\mathbf{k}_1 + \mathbf{b}_1, a\mathbf{k}_2 + \mathbf{b}_2)\\ &= \big(\ g^{\mathbf{A}^\top\cdot(a\mathbf{k}_1+\mathbf{b}_1)}\ ,\ g^{\mathbf{A}^\top\cdot(a\mathbf{k}_2+\mathbf{b}_2)}\ \big)\\ &= \big(\ (g^{\mathbf{A}^\top\cdot\mathbf{k}_1})^a\cdot g^{\mathbf{A}^\top\cdot\mathbf{b}_1}\ ,\ (g^{\mathbf{A}^\top\cdot\mathbf{k}_2})^a\cdot g^{\mathbf{A}^\top\cdot\mathbf{b}_2}\ \big).\end{aligned} \tag{6}$$

We define the $\mathcal{F}_{\text{raff}}$-public-key transformer $\mathsf{THPS.PKTran} : \mathcal{PK} \times \mathcal{F}_{\text{raff}} \longrightarrow \mathcal{PK}$ as follows: for any $\mathsf{pk} = (g^{\mathbf{h}_1}, g^{\mathbf{h}_2}) \in \mathcal{PK}$,

$$\mathsf{THPS.PKTran}(\mathsf{pk}, f_{(a,\mathsf{b})}) := \big(\ (g^{\mathbf{h}_1})^a\cdot g^{\mathbf{A}^\top\cdot\mathbf{b}_1}\ ,\ (g^{\mathbf{h}_2})^a\cdot g^{\mathbf{A}^\top\cdot\mathbf{b}_2}\ \big).$$

Then according to Eq. (6), $\mu\big(f_{(a,\mathsf{b})}(\mathsf{sk})\big) = \mathsf{THPS.PKTran}(\mu(\mathsf{sk}), f_{(a,\mathsf{b})})$.

[$\mathcal{F}_{\mathbf{raff}}$-Poly-Bounded Collisions.] For any pair of distinct $f_{(a,\mathsf{b})}, f_{(a',\mathsf{b}')} \in \mathcal{F}_{\text{raff}}$ with $\mathsf{b} = (\mathbf{b}_1, \mathbf{b}_2)$ and $\mathsf{b}' = (\mathbf{b}'_1, \mathbf{b}'_2)$, we count the number of $\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2) \in \mathcal{SK}$, such that $f_{(a,\mathsf{b})}(\mathsf{sk}) = f_{(a',\mathsf{b}')}(\mathsf{sk})$, i.e.,

$$(a\mathbf{k}_1 + \mathbf{b}_1, a\mathbf{k}_2 + \mathbf{b}_2) = (a'\mathbf{k}_1 + \mathbf{b}'_1, a'\mathbf{k}_2 + \mathbf{b}'_2).$$

If $a = a'$ but $\mathsf{b} \neq \mathsf{b}'$, the equation can never be satisfied. If $a \neq a'$, there is exactly one sk satisfying the equation, i.e., $\mathsf{sk} = (\mathbf{k}_i)_{i=1}^2 = \big((\mathbf{b}'_i - \mathbf{b}_i)/(a - a')\big)_{i=1}^2$.

Therefore, $\max\limits_{f_{(a,\mathsf{b})}\neq f_{(a',\mathsf{b}')}\in\mathcal{F}_{\text{raff}}} \big|\{\mathsf{sk} \in \mathcal{SK} \mid f_{(a,\mathsf{b})}(\mathsf{sk}) = f_{(a',\mathsf{b}')}(\mathsf{sk})\}\big| \leq 1.$ ▮

Theorem 4. *For the* $\mathsf{THPS}_{\mathsf{MDDH}}$ *in Fig. 10, the SMP and PKCP are both hard under the* $\mathcal{D}_{s',s}$*-MDDH assumption w.r.t.* GenG.

Proof of Theorem 4.

[Subset Membership Problem.] Suppose that $\mathcal{A}$ is a PPT adversary against the SMP related to $\mathsf{THPS}_{\mathsf{MDDH}}$, we construct a PPT adversary $\mathcal{B}$ against the $\mathcal{D}_{s',s}$-MDDH assumption w.r.t. GenG by invoking $\mathcal{A}$.

On input $\big(\mathcal{G} = (\mathbb{G}, p, g), g^{\mathbf{A}}, g^{\mathbf{r}}\big)$, $\mathcal{B}$ aims to tell whether $\mathbf{r} = \mathbf{A}\cdot\mathbf{w}$ or $\mathbf{r} \leftarrow_\$ \mathbb{Z}_p^{s'}$, where $\mathbf{w} \leftarrow_\$ \mathbb{Z}_p^s$. $\mathcal{B}$ sets $\mathsf{prm}_{\mathsf{THPS}} := (\mathcal{G}, g^{\mathbf{A}})$ and $C := g^{\mathbf{r}}$. Then $\mathcal{B}$ invokes $\mathcal{A}(\mathsf{prm}_{\mathsf{THPS}}, C)$ and outputs whatever $\mathcal{A}$ outputs.

In the case of $\mathbf{r} = \mathbf{A}\cdot\mathbf{w}$ with $\mathbf{w} \leftarrow_\$ \mathbb{Z}_p^s$, $C = g^{\mathbf{0}}$ with probability of $1/p^s$ and C is randomly distributed over $\mathcal{V}$ with probability of $1 - 1/p^s$; in the case of $\mathbf{r} \leftarrow_\$ \mathbb{Z}_p^{s'}$, $C = g^{\mathbf{0}}$ with probability of $1/p^{s'}$, C is randomly distributed over $\mathcal{V}$ with probability of $(p^s - 1)/p^{s'}$, and C is randomly distributed over $\mathcal{C}\backslash\mathcal{V}$ with probability of $(p^{s'} - p^s)/p^{s'}$. Thus we have that

$$\mathsf{Adv}^{\mathcal{D}_{s',s}\text{-}mddh}_{\mathsf{GenG},\mathcal{B}}(\ell) \geq (1 - \tfrac{1}{p^{s'-s}})\cdot\mathsf{Adv}^{smp}_{\mathsf{THPS},\mathcal{A}}(\ell) - \tfrac{2}{p^s} \geq \tfrac{1}{2}\cdot\mathsf{Adv}^{smp}_{\mathsf{THPS},\mathcal{A}}(\ell) - \tfrac{2}{p^s},$$

and the SMP related to $\mathsf{THPS}_{\mathsf{MDDH}}$ is hard under the $\mathcal{D}_{s',s}$-MDDH assumption.

[Public-Key Collision problem.] By Lemma 5, the $\mathcal{D}_{s',s}$-MDDH assumption implies the $\mathcal{D}_{s',s}$-KerMDH assumption, thus it is sufficient to show that the PKCP is hard under the $\mathcal{D}_{s',s}$-KerMDH assumption w.r.t. GenG.

Suppose that $\mathcal{A}'$ is a PPT adversary against the PKCP related to $\mathsf{THPS}_{\mathsf{MDDH}}$, we construct a PPT adversary $\mathcal{B}'$ against the $\mathcal{D}_{s',s}$-KerMDH assumption w.r.t. GenG by invoking $\mathcal{A}'$.

On input $\big(\mathcal{G} = (\mathbb{G}, p, g), g^{\mathbf{A}}\big)$, $\mathcal{B}'$ aims to compute a non-zero $\mathbf{c}$ such that $\mathbf{A}^\top \cdot \mathbf{c} = \mathbf{0}$. $\mathcal{B}'$ sets $\mathsf{prm}_{\mathsf{THPS}} := (\mathcal{G}, g^{\mathbf{A}})$. Then $\mathcal{B}'$ feeds $\mathcal{A}'$ with $\mathsf{prm}_{\mathsf{THPS}}$ and gets back a pair of $\mathsf{sk} = (\mathbf{k}_1, \mathbf{k}_2)$ and $\mathsf{sk}' = (\mathbf{k}'_1, \mathbf{k}'_2)$.

Suppose that $\mathcal{A}'$ successfully solves the PKCP, i.e., $\mathsf{sk} \neq \mathsf{sk}'$ but $\mu(\mathsf{sk}) = \mu(\mathsf{sk}')$, then $(\ g^{\mathbf{A}^\top \cdot \mathbf{k}_1}\ ,\ g^{\mathbf{A}^\top \cdot \mathbf{k}_2}\ ) = (\ g^{\mathbf{A}^\top \cdot \mathbf{k}'_1}\ ,\ g^{\mathbf{A}^\top \cdot \mathbf{k}'_2}\ )$, i.e.,

$$(\ g^{\mathbf{A}^\top \cdot (\mathbf{k}_1 - \mathbf{k}'_1)}\ ,\ g^{\mathbf{A}^\top \cdot (\mathbf{k}_2 - \mathbf{k}'_2)}\ ) = (\ g^{\mathbf{0}}\ ,\ g^{\mathbf{0}}\ ).$$

Without loss of generality, suppose that $\mathbf{k}_1 \neq \mathbf{k}'_1$, then $\mathcal{B}'$ returns $\mathbf{c} := \mathbf{k}_1 - \mathbf{k}'_1$ as its final output. Obviously, $\mathcal{B}'$ succeeds, i.e., $\mathbf{A}^\top \cdot \mathbf{c} = \mathbf{A}^\top \cdot (\mathbf{k}_1 - \mathbf{k}'_1) = \mathbf{0}$, as long as $\mathcal{A}'$ succeeds. Therefore

$$\mathsf{Adv}^{\mathcal{D}_{s',s}\text{-}kmdh}_{\mathsf{GenG},\mathcal{B}'}(\ell) \geq \mathsf{Adv}^{pkcp}_{\mathsf{THPS},\mathcal{A}'}(\ell),$$

and the PKCP related to $\mathsf{THPS}_{\mathsf{MDDH}}$ is hard under the $\mathcal{D}_{s',s}$-KerMDH assumption. ▌

When plugging the $\mathsf{THPS}_{\mathsf{MDDH}}$ into the paradigms in Fig. 4, Fig. 8 and Fig. 16, we obtain a MAC $\mathsf{MAC}[\mathsf{THPS}_{\mathsf{MDDH}}]$, a PKE scheme $\mathsf{PKE}[\mathsf{THPS}_{\mathsf{MDDH}}, \mathsf{AE}]$ and a SE scheme $\mathsf{SE}[\mathsf{THPS}_{\mathsf{MDDH}}, \mathsf{AE}]$ respectively. The super-strong RKA securities of the resulting MAC, PKE and SE schemes are stated as follows.

Corollary 2. *If $\mathcal{H}$ is collision-resistant and the $\mathcal{D}_{s',s}$-MDDH assumption holds w.r.t.* GenG*, then the* $\mathsf{MAC}[\mathsf{THPS}_{\mathsf{MDDH}}]$ *is super-strong EU-$\mathcal{F}_{raff}$-RK-CMVA secure, where $\mathcal{F}_{raff}$ is specified in Theorem 3.*

If $\mathcal{H}_1$ is collision-resistant, $\mathcal{H}_2$ is universal, AE *is OT-secure with key space $\mathcal{K}_{\mathsf{AE}} = \{0,1\}^\ell$, and the $\mathcal{D}_{s',s}$-MDDH assumption holds w.r.t.* GenG*, then the* $\mathsf{PKE}[\mathsf{THPS}_{\mathsf{MDDH}}, \mathsf{AE}]$ *and* $\mathsf{SE}[\mathsf{THPS}_{\mathsf{MDDH}}, \mathsf{AE}]$ *are super-strong IND-$\mathcal{F}_{raff}$-RK-CCA2 secure, where $\mathcal{F}_{raff}$ is specified in Theorem 3.*

The above corollary follows from Theorems 1, 2, 3, 4 and Corollary 1, as well as the fact that $|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}_{\mathrm{raff}}}(\ell) = |\mathcal{K}_{\mathsf{AE}}|/|\mathcal{K}| = 2^\ell/p$ are negligible in ℓ since p is of 2ℓ-bit.

7 Instantiation of THPS from the DCR Assumption

In this section, we show how to construct $\mathcal{F}_{\mathrm{raff}}$-tailored THPS from the DCR Assumption, where $\mathcal{F}_{\mathrm{raff}}$ is the class of restricted affine functions. In our construction of THPS, we exploit a useful mapping χ defined over DCR groups. We study the actions of χ on various subsets of DCR groups. Finally we show that our DCR-based THPS enjoys all of the properties required in the paradigms for constructing super-strong RKA secure MAC, PKE and SE.

7.1 GenN and DCR Assumption

Let $\mathsf{GenN}(1^\ell)$ be a PPT algorithm outputting (N, p, q), where $N = pq$ and p, q are safe primes of 2ℓ bits. Let $s \geq 2$ be an integer.

Definition 22 (DCR Assumption). *The Decisional Composite Residuosity (DCR) Assumption holds w.r.t.* GenN*, if for any PPT adversary* $\mathcal{A}$*, the following advantage is negligible in* ℓ*:*

$$\mathsf{Adv}^{dcr}_{\mathsf{GenN},\mathcal{A}}(\ell) := \big|\Pr\left[\mathcal{A}(N,u)=1\right] - \Pr\left[\mathcal{A}(N,v)=1\right]\big|,$$

where $(N,p,q) \leftarrow_{\$} \mathsf{GenN}(1^\ell)$*,* $u \leftarrow_{\$} \mathbb{Z}^*_{N^s}$ *and* $v := u^{N^{s-1}}$ *mod* N^s*.*

For an integer a, denote by $(\frac{a}{N})$ the Jacobi symbol of a modulo N. We define $\mathbb{J}_{N^s} := \big\{\ a \ \big|\ a \in \mathbb{Z}^*_{N^s}, (\frac{a}{N}) = 1\big\}$, $\mathbb{CR}_{N^s} := \big\{\ a^{N^{s-1}} \ \big|\ a \in \mathbb{Z}^*_{N^s}, (\frac{a^{N^{s-1}}}{N}) = 1\big\}$, and $\mathbb{RU}_{N^s} := \big\{\ (1+N)^r \ \big|\ r \in \mathbb{Z}_{N^{s-1}}\big\}$. These sets are subgroups of $\mathbb{Z}^*_{N^s}$, with group operation $a \cdot b := a \cdot b \bmod N^s$. In particular, $\mathbb{CR}_{N^s}$ is a cyclic group of order $\phi(N)/2$, $\mathbb{RU}_{N^s}$ is a cyclic group of order N^{s-1}, and $\mathbb{J}_{N^s} = \mathbb{CR}_{N^s} \otimes \mathbb{RU}_{N^s}$, where $\otimes$ denotes internal direct product.

We also define signed subgroups of $\mathbb{Z}^*_{N^s}$ following the approach of [HK09, Hof16]. For $a \in \mathbb{Z}_{N^s}$, we define the "absolute modular value" notation

$$|a|_{N^s} := \begin{cases} \quad a, & \text{if } 0 \le a \le (N^s-1)/2, \\ N^s - a, & \text{if } (N^s-1)/2 < a \le N^s - 1, \end{cases} \tag{7}$$

so that $|a|_{N^s} \in \{0, \cdots, (N^s-1)/2\}$ in any case. Then we define $\mathbb{J}^+_{N^s} := \big\{\ |a|_{N^s} \ \big|\ a \in \mathbb{Z}^*_{N^s}, (\frac{a}{N}) = 1\big\}$, $\mathbb{CR}^+_{N^s} := \big\{\ |a^{N^{s-1}}|_{N^s} \ \big|\ a \in \mathbb{Z}^*_{N^s}, (\frac{a^{N^{s-1}}}{N}) = 1\big\}$, and $\mathbb{RU}^+_{N^s} := \big\{\ |(1+N)^r|_{N^s} \ \big|\ r \in \mathbb{Z}_{N^{s-1}}\big\}$ as the corresponding subsets of $\mathbb{Z}^+_{N^s} := \big\{\ |a|_{N^s} \ \big|\ a \in \mathbb{Z}_{N^s}\big\} = \{0, \cdots, (N^s-1)/2\}$. These subsets are also groups, but the group operation is defined as $|a|_{N^s} \cdot |b|_{N^s} := |a \cdot b|_{N^s}$. In particular, $\mathbb{CR}^+_{N^s}$ is a cyclic group of order $\phi(N)/4$, $\mathbb{RU}^+_{N^s}$ is a cyclic group of order N^{s-1}, and $\mathbb{J}^+_{N^s} = \mathbb{CR}^+_{N^s} \otimes \mathbb{RU}^+_{N^s}$.

7.2 The Map χ and Its Actions on Cosets of $\mathbb{RU}^+_{N^s}$, $\mathbb{J}^+_{N^s}$ and $\mathbb{CR}^+_{N^s}$

Before presenting the DCR-based construction of THPS, we first define a useful map χ:

$$\begin{array}{cccc} \chi: & \mathbb{Z}_{N^s} & \longrightarrow & \mathbb{Z}_{N^{s-1}} \\ & (a + bN \bmod N^s) & \longmapsto & (b \bmod N^{s-1}), \end{array} \tag{8}$$

where $0 \le a < N$ and $0 \le b < N^{s-1}$.

χ was originally introduced by Cramer and Shoup in [CS02], but our χ is a generalization of theirs, since their χ can be viewed as a special case of $s = 2$. The map χ does not preserve any algebraic structure. However, it enjoys the following nice property which again is a generalized property of that in [CS02].

Lemma 6 (Action of χ on Cosets of $\mathbb{RU}_{N^s}$). *For any* $g \in \mathbb{J}_{N^s}$*, define* $g \cdot \mathbb{RU}_{N^s} := \big\{g \cdot (1+N)^r \ \big|\ r \in \mathbb{Z}_{N^{s-1}}\big\}$ *as the coset of* $\mathbb{RU}_{N^s}$ *with coset leader* g*. Then the restriction of* χ *to* $g \cdot \mathbb{RU}_{N^s}$ *is a one-to-one map from* $g \cdot \mathbb{RU}_{N^s}$ *to* $\mathbb{Z}_{N^{s-1}}$*.*

Proof. Since both the size of $g \cdot \mathbb{RU}_{N^s}$ and $\mathbb{Z}_{N^{s-1}}$ are N^{s-1}, it is sufficient to show that the restriction of χ to $g \cdot \mathbb{RU}_{N^s}$ is injective. That is, for any $g \cdot (1+N)^r, g \cdot (1+N)^{r'} \in g \cdot \mathbb{RU}_{N^s}$, suppose that $\chi\big(g \cdot (1+N)^r\big) = \chi\big(g \cdot (1+N)^{r'}\big)$, we want to show $g \cdot (1+N)^r = g \cdot (1+N)^{r'}$.

Denote $g = a + bN \bmod N^s \in \mathbb{J}_{N^s}$ with $0 \leq a < N$ and $0 \leq b < N^{s-1}$. Then

$$g \cdot (1+N)^r = (a+bN) \cdot \Big(1 + \sum_{j=1}^{r} \tbinom{r}{j} \cdot N^j\Big) = a + \underbrace{\Big(b + (a+bN) \cdot \sum_{j=1}^{r} \tbinom{r}{j} \cdot N^{j-1}\Big)}_{(*)} \cdot N \bmod N^s,$$

thus $\chi\big(g \cdot (1+N)^r\big) = (*) \bmod N^{s-1}$.

Similarly,

$$g \cdot (1+N)^{r'} = a + \underbrace{\Big(b + (a+bN) \cdot \sum_{j=1}^{r'} \tbinom{r'}{j} \cdot N^{j-1}\Big)}_{(**)} \cdot N \bmod N^s,$$

and $\chi\big(g \cdot (1+N)^{r'}\big) = (**) \bmod N^{s-1}$.

Thus, $\chi\big(g \cdot (1+N)^r\big) = \chi\big(g \cdot (1+N)^{r'}\big)$ implies that $(*) = (**) \bmod N^{s-1}$. This in turn implies that

$$g \cdot (1+N)^r = a + (*) \cdot N = a + (**) \cdot N = g \cdot (1+N)^{r'} \bmod N^s,$$

as we desired. So the lemma follows. ▌

Since the elements in $\mathbb{Z}^+_{N^s}$ are integers in the set $\{0, \cdots, (N^s-1)/2\}$, they can be naturally viewed as elements in $\mathbb{Z}_{N^s}$. Therefore, we can also consider the action of the map χ on the signed set $\mathbb{Z}^+_{N^s}$. In particular, we develop the following lemmas and corollaries, which will play important roles in our DCR-based THPS construction later, in order to achieve the average-case strongly-universal$_1$, universal$_2$, and extracting properties.

Lemma 7 (Action of χ on Cosets of $\mathbb{RU}^+_{N^s}$ and on $\mathbb{J}^+_{N^s}$). *For any $|g|_{N^s} \in \mathbb{J}^+_{N^s}$, define $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s} := \big\{|g \cdot (1+N)^r|_{N^s} \;\big|\; r \in \mathbb{Z}_{N^{s-1}}\big\}$ as the coset of $\mathbb{RU}^+_{N^s}$ with coset leader $|g|_{N^s}$. Then (1) the restriction of χ to $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s}$ is a two-to-one map from $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s}$ to $\mathbb{Z}^+_{N^{s-1}} = \{0, \cdots, (N^{s-1}-1)/2\}$ except that it maps only one element in $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s}$ to $(N^{s-1}-1)/2$; (2) the restriction of χ to $\mathbb{J}^+_{N^s}$ has image set $\mathbb{Z}^+_{N^{s-1}}$.*

Proof. It is easy to see that $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s} = \big\{|h|_{N^s} \;\big|\; h \in g \cdot \mathbb{RU}_{N^s}\big\}$ from the definition. By Lemma 6, χ is a bijection from the coset $g \cdot \mathbb{RU}_{N^s}$ to $\mathbb{Z}_{N^{s-1}}$, thus we can represent $g \cdot \mathbb{RU}_{N^s}$ as $\big\{h = \chi^{-1}(b) \;\big|\; b \in \mathbb{Z}_{N^{s-1}}\big\}$ where $\chi^{-1}(b)$ denotes the unique inverse of $b \in \mathbb{Z}_{N^{s-1}}$ under χ in $g \cdot \mathbb{RU}_{N^s}$. By combining the above two relations, we get that

$$|g|_{N^s} \cdot \mathbb{RU}^+_{N^s} = \big\{|\chi^{-1}(b)|_{N^s} \;\big|\; b \in \mathbb{Z}_{N^{s-1}}\big\}.$$

Next we analyze the action of χ on $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s}$. More precisely, for $b \in \mathbb{Z}_{N^{s-1}}$, it holds that $\chi^{-1}(b) = a + bN \bmod N^s$ for some $0 < a < N$. Here $a \neq 0$ because $\chi^{-1}(b) \in g \cdot \mathbb{RU}_{N^s} \subseteq \mathbb{Z}^*_{N^s}$. We compute $\chi(|\chi^{-1}(b)|_{N^s})$ as follows.

- If $0 \leq b < (N^{s-1}-1)/2$, then $|a+bN| \leq (N-1) + ((N^{s-1}-1)/2 - 1) \cdot N < (N^s-1)/2$. According to our notation (7), $|\chi^{-1}(b)|_{N^s} = |a+bN|_{N^s} = a+bN$, where $0 < a < N$, thus $\chi(|\chi^{-1}(b)|_{N^s}) = b$.
- If $(N^{s-1}-1)/2 < b \leq N^{s-1}-1$, then $|a+bN| \geq 1 + ((N^{s-1}-1)/2 + 1) \cdot N > (N^s-1)/2$. According to (7), $|\chi^{-1}(b)|_{N^s} = |a+bN|_{N^s} = N^s - (a+bN) = (N-a) + (N^{s-1}-1-b) \cdot N$, where $0 < N-a < N$, thus $\chi(|\chi^{-1}(b)|_{N^s}) = N^{s-1} - 1 - b$.

– If $b = (N^{s-1}-1)/2$, no matter $|\chi^{-1}(b)|_{N^s} = a + bN$ or $|\chi^{-1}(b)|_{N^s} = N^s - (a+bN)$, we both have that $\chi(|\chi^{-1}(b)|_{N^s}) = (N^{s-1}-1)/2$.

In summary, for $0 \le b < (N^{s-1}-1)/2$, there are exactly two pre-images of b in $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s}$ under χ, i.e., $|\chi^{-1}(b)|_{N^s}$ and $|\chi^{-1}(N^{s-1}-1-b)|_{N^s}$; for $b = (N^{s-1}-1)/2$, there is exactly one pre-image of b in $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s}$ under χ, i.e., $|\chi^{-1}((N^{s-1}-1)/2)|_{N^s}$. Therefore (1) follows.

Since $\mathbb{J}^+_{N^s} = \mathbb{CR}^+_{N^s} \otimes \mathbb{RU}^+_{N^s}$, $\mathbb{J}^+_{N^s}$ can be viewed as unions of cosets of $\mathbb{RU}^+_{N^s}$ with coset leaders in $\mathbb{CR}^+_{N^s} \subseteq \mathbb{J}^+_{N^s}$. Then by (1), χ maps elements in $\mathbb{J}^+_{N^s}$ to $\mathbb{Z}^+_{N^{s-1}}$, thus (2) follows. ▌

Corollary 3 (Action of χ on Cosets of $\mathbb{RU}^+_{N^s}$ and on $\mathbb{J}^+_{N^s}$). *For any $|g|_{N^s} \in \mathbb{J}^+_{N^s}$, both $\chi\big(\mathsf{U}_{|g|_{N^s}\cdot\mathbb{RU}^+_{N^s}}\big)$ and $\chi\big(\mathsf{U}_{\mathbb{J}^+_{N^s}}\big)$ are statistically close to $\mathsf{U}_{\mathbb{Z}^+_{N^{s-1}}}$ with statistical distance $1/N^{s-1}$.*

Proof. By Lemma 7, for $0 \le b < (N^{s-1}-1)/2$, $\Pr\big[\chi\big(\mathsf{U}_{|g|_{N^s}\cdot\mathbb{RU}^+_{N^s}}\big) = b\big] = 2/N^{s-1}$; for $b = (N^{s-1}-1)/2$, $\Pr\big[\chi\big(\mathsf{U}_{|g|_{N^s}\cdot\mathbb{RU}^+_{N^s}}\big) = b\big] = 1/N^{s-1}$. Thus

$$\begin{aligned}\mathit{\Delta}\Big(\ \chi\big(\mathsf{U}_{|g|_{N^s}\cdot\mathbb{RU}^+_{N^s}}\big),\ \mathsf{U}_{\mathbb{Z}^+_{N^{s-1}}}\ \Big) &= \tfrac{1}{2}\cdot\sum_{b=0}^{(N^{s-1}-1)/2}\Big|\Pr\big[\chi\big(\mathsf{U}_{|g|_{N^s}\cdot\mathbb{RU}^+_{N^s}}\big)=b\big]-\Pr[\mathsf{U}_{\mathbb{Z}^+_{N^{s-1}}}=b]\Big|\\ &= \tfrac{1}{2}\cdot\sum_{b=0}^{(N^{s-1}-1)/2-1}\Big|\tfrac{2}{N^{s-1}}-\tfrac{1}{(N^{s-1}+1)/2}\Big| + \tfrac{1}{2}\cdot\Big|\tfrac{1}{N^{s-1}}-\tfrac{1}{(N^{s-1}+1)/2}\Big|\\ &= \tfrac{N^{s-1}-1}{N^{s-1}\cdot(N^{s-1}+1)} \le \tfrac{1}{N^{s-1}}.\end{aligned}$$

Since $\mathbb{J}^+_{N^s} = \mathbb{CR}^+_{N^s} \otimes \mathbb{RU}^+_{N^s}$, $\mathbb{J}^+_{N^s}$ can be viewed as disjoint unions of cosets of $\mathbb{RU}^+_{N^s}$ with coset leaders in $\mathbb{CR}^+_{N^s}$, i.e.,

$$\mathbb{J}^+_{N^s} = \bigcup_{|g|_{N^s}\in\mathbb{CR}^+_{N^s}} |g|_{N^s}\cdot\mathbb{RU}^+_{N^s}.$$

By Lemma 7, for $0 \le b < (N^{s-1}-1)/2$, there are exactly two pre-images in each coset $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s}$, thus $\Pr\big[\chi\big(\mathsf{U}_{\mathbb{J}^+_{N^s}}\big) = b\big] = 2|\mathbb{CR}^+_{N^s}|/|\mathbb{J}^+_{N^s}| = 2/N^{s-1}$; for $b = (N^{s-1}-1)/2$, there is exactly one pre-image in each coset $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s}$, thus $\Pr\big[\chi\big(\mathsf{U}_{\mathbb{J}^+_{N^s}}\big) = b\big] = |\mathbb{CR}^+_{N^s}|/|\mathbb{J}^+_{N^s}| = 1/N^{s-1}$. Similarly, we can get that $\mathit{\Delta}\big(\chi\big(\mathsf{U}_{\mathbb{J}^+_{N^s}}\big),\ \mathsf{U}_{\mathbb{Z}^+_{N^{s-1}}}\big) \le 1/N^{s-1}$. ▌

Corollary 4 (Action of χ on Subsets of Cosets of $\mathbb{RU}^+_{N^s}$). *For any $|g|_{N^s} \in \mathbb{J}^+_{N^s}$ and any subset $\mathcal{S}$ of $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s}$, the guessing probability of $\chi\big(\mathsf{U}_{\mathcal{S}}\big)$ is at most $2/|\mathcal{S}|$.*

Proof. By Lemma 7, for any $b \in \mathbb{Z}^+_{N^{s-1}}$, there are at most two pre-images in the coset $|g|_{N^s} \cdot \mathbb{RU}^+_{N^s}$, so is in $\mathcal{S}$. Then $\max\limits_{b\in\mathbb{Z}^+_{N^{s-1}}} \Pr\big[\chi\big(\mathsf{U}_{\mathcal{S}}\big) = b\big] \le 2/|\mathcal{S}|$, and the corollary follows. ▌

Lemma 8 (Action of χ on $\mathbb{CR}^+_{N^s}$). *The guessing probability of $\chi\big(\mathsf{U}_{\mathbb{CR}^+_{N^s}}\big)$ is at most $(\mathsf{Adv}^{dcr}_{\mathsf{GenN}}(\ell) + 3/N^{s-1})^{1/2}$, which is negligible in ℓ under the DCR assumption w.r.t.* GenN.

Proof. We construct a PPT adversary $\mathcal{A}$ against the DCR assumption. On input (N, v), $\mathcal{A}$ aims to tell whether $v = u$ or $v = u^{N^{s-1}} \bmod N^s$ for $u \leftarrow_{\$} \mathbb{Z}^*_{N^s}$. $\mathcal{A}$ samples $|g|_{N^s} \leftarrow_{\$} \mathbb{CR}^+_{N^s}$ and outputs 1 if and only if $\chi(|g|_{N^s}) = \chi(|v^2|_{N^s})$.

In the case of $v = u$, $|v^2|_{N^s}$ is randomly distributed over $\mathbb{J}^+_{N^s}$, thus

$$\begin{aligned}&\Pr\left[\chi(|g|_{N^s}) = \chi(|v^2|_{N^s})\right] = \Pr\left[\chi\big(\mathsf{U}_{\mathbb{CR}^+_{N^s}}\big) = \chi\big(\mathsf{U}_{\mathbb{J}^+_{N^s}}\big)\right]\\ \leq\ &\Pr\left[\chi\big(\mathsf{U}_{\mathbb{CR}^+_{N^s}}\big) = \mathsf{U}_{\mathbb{Z}^+_{N^{s-1}}}\right] + \Delta\big(\mathsf{U}_{\mathbb{Z}^+_{N^{s-1}}}\ ,\ \chi\big(\mathsf{U}_{\mathbb{J}^+_{N^s}}\big)\big) \leq \tfrac{1}{|\mathbb{Z}^+_{N^{s-1}}|} + \tfrac{1}{N^{s-1}} \leq \tfrac{3}{N^{s-1}},\end{aligned}$$

where the second inequality follows from Corollary 3.

In the case of $v = u^{N^{s-1}} \bmod N^s$, $|v^2|_{N^s}$ is randomly distributed over $\mathbb{CR}^+_{N^s}$, thus

$$\begin{aligned}&\Pr\left[\chi(|g|_{N^s}) = \chi(|v^2|_{N^s})\right] = \Pr\left[\chi\big(\mathsf{U}_{\mathbb{CR}^+_{N^s}}\big) = \chi\big(\mathsf{U}'_{\mathbb{CR}^+_{N^s}}\big)\right]\\ =&\sum_{b\in\mathbb{Z}^+_{N^{s-1}}} \Pr\left[\chi\big(\mathsf{U}_{\mathbb{CR}^+_{N^s}}\big) = b\right]^2 \geq \max_{b\in\mathbb{Z}^+_{N^{s-1}}} \Pr\left[\chi\big(\mathsf{U}_{\mathbb{CR}^+_{N^s}}\big) = b\right]^2,\end{aligned}$$

where $\mathsf{U}_{\mathbb{CR}^+_{N^s}}, \mathsf{U}'_{\mathbb{CR}^+_{N^s}}$ are both randomly distributed over $\mathbb{CR}^+_{N^s}$.

Thus we have that

$$\mathsf{Adv}^{dcr}_{\mathsf{GenN},\mathcal{A}}(\ell) \geq \max_{b\in\mathbb{Z}^+_{N^{s-1}}} \Pr\left[\chi\big(\mathsf{U}_{\mathbb{CR}^+_{N^s}}\big) = b\right]^2 - \tfrac{3}{N^{s-1}},$$

and it follows $\max_{b\in\mathbb{Z}^+_{N^{s-1}}} \Pr\left[\chi\big(\mathsf{U}_{\mathbb{CR}^+_{N^s}}\big) = b\right] \leq \big(\mathsf{Adv}^{dcr}_{\mathsf{GenN},\mathcal{A}}(\ell) + 3/N^{s-1}\big)^{1/2}$. ▌

7.3 $\mathsf{THPS}_{\mathsf{DCR}}$ from the DCR Assumption

Let χ be the map defined in (8). Here we give a DCR-based construction $\mathsf{THPS}_{\mathsf{DCR}}$ in Fig. 11, whose subset membership and public-key collision problems are hard under the DCR assumption.

```
$\mathsf{prm}_{\mathsf{THPS}} \leftarrow\!\$\ \mathsf{THPS.Setup}(1^\ell)$:
$(N, p, q) \leftarrow\!\$\ \mathsf{GenN}(1^\ell)$.   $|g|_{N^s} \leftarrow\!\$\ \mathbb{CR}^+_{N^s}$ s.t. $|g|_{N^s}$ is a generator.
Return $\mathsf{prm}_{\mathsf{THPS}} := (N, |g|_{N^s})$, which implicitly defines $(\mathcal{K}, \mathcal{C}, \mathcal{V}, \mathcal{T}, \mathcal{SK}, \mathcal{PK}, \Lambda_{(\cdot)}, \mu)$:
$\mathcal{K} := \mathbb{Z}^+_{N^{s-1}}$.      $\mathcal{C} := \mathbb{J}^+_{N^s}\backslash\{1\}$.      $\mathcal{V} := \mathbb{CR}^+_{N^s}\backslash\{1\} = \big\{|g|^w_{N^s} \bigm| w \in \mathbb{Z}_{\phi(N)/4}\big\}\backslash\{1\}$.
$\mathcal{T} := \mathbb{Z}_N$.      $\mathcal{SK} := \mathbb{Z}_{N^s} \times \mathbb{Z}_{N^s}$.      $\mathcal{PK} := \mathbb{J}^+_{N^s} \times \mathbb{J}^+_{N^s}$.
For $\mathsf{sk} = (k_1, k_2) \in \mathcal{SK}$,  $C = |c|_{N^s} \in \mathcal{C}$ and $t \in \mathcal{T}$,   $\Lambda_{\mathsf{sk}}(C, t) := \chi\big(|c|^{k_1+k_2t}_{N^s}\big) \in \mathcal{K}$.
For $\mathsf{sk} = (k_1, k_2) \in \mathcal{SK}$,  $\mathsf{pk} = \mu(\mathsf{sk}) := (|g|^{k_1}_{N^s}, |g|^{k_2}_{N^s}) \in \mathcal{PK}$.

$K \leftarrow \mathsf{THPS.Pub}(\mathsf{pk}, C, w, t)$:
Parse $\mathsf{pk} = (|h_1|_{N^s}, |h_2|_{N^s}) \in \mathcal{PK}$.
Return $K := \chi\big(|h_1|^w_{N^s} \cdot |h_2|^{wt}_{N^s}\big)$.

$K \leftarrow \mathsf{THPS.Priv}(\mathsf{sk}, C, t)$:
Parse $\mathsf{sk} = (k_1, k_2) \in \mathcal{SK}$ and $C = |c|_{N^s} \in \mathcal{C}$.
Return $K := \chi\big(|c|^{k_1+k_2t}_{N^s}\big)$.
```

Fig. 11. Construction of $\mathsf{THPS}_{\mathsf{DCR}}$.

We stress that given N, a generator of $\mathbb{CR}^+_{N^s}$ can be sampled as $|a^{2N^{s-1}}|_{N^s}$ for a uniform $a \in \mathbb{Z}^*_{N^s}$; given $\mathsf{prm}_{\mathsf{THPS}} = (N, |g|_{N^s})$, the membership of $\mathcal{C} = \mathbb{J}^+_{N^s}\backslash\{1\}$ can be efficiently checked, an element in $\mathcal{V}$ can be sampled as $|g|^w_{N^s}$ for a uniform $w \in \mathbb{Z}_{\lfloor N/4 \rfloor}$ which is statistically close to the uniform distribution with a negligible statistical distance $1 - \phi(N)/N \leq 1/p + 1/q$, and an element in $\mathcal{C}$ can be sampled as $|a^2|_{N^s}$ for a uniform $a \in \mathbb{Z}^*_{N^s}$ until $|a^2|_{N^s} \neq 1$ [HK09, Hof16].

Theorem 5. *The* $\mathsf{THPS}_{\mathsf{DCR}}$ *in Fig. 11 is an* $\mathcal{F}_{\mathit{raff}}$*-tailored THPS under the DCR assumption w.r.t.* GenN*, where* $\mathcal{F}_{\mathit{raff}} = \big\{ f_{(a,\mathsf{b})} : (k_1, k_2) \in \mathcal{SK} \longmapsto (ak_1 + b_1, ak_2 + b_2) \in \mathcal{SK} \;\big|\; a \in \mathbb{Z}_N^*, \gcd(a, \phi(N)/4) = 1,\ \mathsf{b} = (b_1, b_2) \in \mathcal{SK} \big\}$ *is the class of restricted affine functions. More precisely, it is average-case* $\mathcal{F}_{\mathit{raff}}$*-strongly-universal*$_1$*,* $\mathcal{F}_{\mathit{raff}}$*-universal*$_2$*,* $\mathcal{F}_{\mathit{raff}}$*-public-key-homomorphic and has* $\mathcal{F}_{\mathit{raff}}$*-poly-bounded collisions. Furthermore, it is* $\mathcal{F}_{\mathit{raff}}$*-extracting under the DCR assumption w.r.t.* GenN *.*

Proof of Theorem 5.

[Projectiveness.] For all $\mathsf{sk} = (k_1, k_2) \in \mathcal{SK}$, all $C = |g|_{N^s}^{w} \in \mathcal{V}$ with witness w and all $t \in \mathcal{T}$, it follows that

$$\begin{aligned} \mathsf{THPS.Pub}(\mu(\mathsf{sk}), C, w, t) &= \chi\big(\ (|g|_{N^s}^{k_1})^{w} \cdot (|g|_{N^s}^{k_2})^{wt}\ \big) \\ &= \chi\big(\ (|g|_{N^s}^{w})^{k_1 + k_2 t}\ \big) = \mathsf{THPS.Priv}(\mathsf{sk}, C, t). \end{aligned}$$

[Average-Case $\mathcal{F}_{\mathrm{raff}}$-Strongly-Universal$_1$.] Suppose that $f_{(a,\mathsf{b})} \in \mathcal{F}_{\mathrm{raff}}$ with $\mathsf{b} = (b_1, b_2)$ and $t \in \mathcal{T}$. For $\mathsf{sk} = (k_1, k_2) \leftarrow_{\$} \mathcal{SK}$ and $C \leftarrow_{\$} \mathcal{C} \setminus \mathcal{V}$, we consider the distribution of $\Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$ conditioned on $\mathsf{pk} = \mu(\mathsf{sk})$ and C.

Note that the distribution of $(k_1, k_2) \leftarrow_{\$} \mathcal{SK} = \mathbb{Z}_{N^s} \times \mathbb{Z}_{N^s}$ is statistically close to $(k_1, k_2) \leftarrow_{\$} \mathcal{SK}' = \mathbb{Z}_{\phi(N) \cdot N^{s-1}} \times \mathbb{Z}_{\phi(N) \cdot N^{s-1}}$, with a negligible statistical distance $2 \cdot (1 - \phi(N)/N) \leq 2/p + 2/q$. For the latter distribution, we have that $(k_1, k_2) \bmod \phi(N)/4$ is randomly distributed over $\mathbb{Z}_{\phi(N)/4} \times \mathbb{Z}_{\phi(N)/4}$, $(k_1, k_2) \bmod N^{s-1}$ is randomly distributed over $\mathbb{Z}_{N^{s-1}} \times \mathbb{Z}_{N^{s-1}}$, and they are independent of each other.

By the fact that $\mathbb{J}_{N^s}^{+} = \mathbb{CR}_{N^s}^{+} \otimes \mathbb{RU}_{N^s}^{+}$, we can represent $C \leftarrow_{\$} \mathcal{C} \setminus \mathcal{V}$ as $C = |g|_{N^s}^{r_1} \cdot |1 + N|_{N^s}^{r_2}$ for $r_1 \leftarrow_{\$} \mathbb{Z}_{\phi(N)/4}$ and $r_2 \leftarrow_{\$} \mathbb{Z}_{N^{s-1}} \setminus \{0\}$. Except with a negligible probability $(1 - \phi(N)/N) \leq 1/p + 1/q$, we have $r_2 \in \mathbb{Z}_{N^{s-1}}^*$.

In the following analysis, we let $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}'$ and assume that $r_2 \in \mathbb{Z}_{N^{s-1}}^*$. Firstly $\mathsf{pk} = \mu(\mathsf{sk}) = (|g|_{N^s}^{k_1}, |g|_{N^s}^{k_2})$, which leaks $(k_1, k_2) \bmod \phi(N)/4$, but the values of $(k_1, k_2) \bmod N^{s-1}$ are totally hidden. Then

$$\begin{aligned} \Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t) &= \Lambda_{(ak_1 + b_1, ak_2 + b_2)}(C, t) = \chi\big((|g|_{N^s}^{r_1} \cdot |1 + N|_{N^s}^{r_2})^{(ak_1 + b_1) + (ak_2 + b_2)t} \big) \\ &= \chi\big(\underbrace{|g|_{N^s}^{r_1 a(k_1 + k_2 t)} \cdot \boxed{|1 + N|_{N^s}^{r_2 a(k_1 + k_2 t)}} \cdot (|g|_{N^s}^{r_1} \cdot |1 + N|_{N^s}^{r_2})^{b_1 + b_2 t}}_{(*)} \big). \end{aligned} \tag{9}$$

Conditioned on pk and C, $(k_1 + k_2 t \bmod N^{s-1})$ is randomly distributed over $\mathbb{Z}_{N^{s-1}}$. Since $r_2 \in \mathbb{Z}_{N^{s-1}}^*$ and $a \in \mathbb{Z}_N^*$, the term $|1 + N|_{N^s}^{r_2 a(k_1 + k_2 t)}$ is randomly distributed over $\mathbb{RU}_{N^s}^{+}$. So $(*)$ is randomly distributed over the coset of $\mathbb{RU}_{N^s}^{+}$ with coset leader $|g|_{N^s}^{r_1 a(k_1 + k_2 t)} \cdot (|g|_{N^s}^{r_1} \cdot |1 + N|_{N^s}^{r_2})^{b_1 + b_2 t} \in \mathbb{J}_{N^s}^{+}$. By Corollary 3, $\Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t) = \chi(*)$ is statistically close to the uniform distribution over $\mathcal{K} = \mathbb{Z}_{N^{s-1}}^{+}$ conditioned on pk and C, with statistical distance $1/N^{s-1}$.

Therefore, let $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$, $\mathsf{pk} = \mu(\mathsf{sk})$ and $C \leftarrow_{\$} \mathcal{C} \setminus \mathcal{V}$,

$$\Delta\big(\ (\mathsf{pk}, C, \Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t))\ ,\ (\mathsf{pk}, C, \mathsf{U}_{\mathcal{K}})\ \big) \leq \tfrac{3}{p} + \tfrac{3}{q} + \tfrac{1}{N^{s-1}}.$$

That is, $\mathsf{THPS}_{\mathsf{DCR}}$ is average-case $\mathcal{F}_{\mathrm{raff}}$-strongly-universal$_1$ with $\epsilon_{\mathsf{THPS}, \mathcal{F}_{\mathrm{raff}}}^{\mathit{ac\text{-}str\text{-}u_1}}(\ell) = 3/p + 3/q + 1/N^{s-1}$, which is negligible in ℓ.

[$\mathcal{F}_{\mathbf{raff}}$**-Universal**$_2$**.**] Suppose that $f_{(a,\mathsf{b})}, f_{(a',\mathsf{b}')} \in \mathcal{F}_{\mathrm{raff}}$ with $\mathsf{b} = (b_1, b_2)$ and $\mathsf{b}' = (b_1', b_2')$, $C \in \mathcal{C}$, $C' \in \mathcal{C} \setminus \mathcal{V}$ and $t, t' \in \mathcal{T}$ with $t \neq t'$. For $\mathsf{sk} = (k_1, k_2) \leftarrow_{\$} \mathcal{SK}$, we consider the distribution of $\mathit{\Lambda}_{f_{(a',\mathsf{b}')}(\mathsf{sk})}(C', t')$ conditioned on $\mathsf{pk} = \mu(\mathsf{sk})$ and $\mathit{\Lambda}_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$.

Similar as above, in the following analysis, we let $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}'$, which has a negligible statistical distance $2/p + 2/q$ with $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$, and we represent C, C' as $C = |g|_{N^s}^{r_1} \cdot |1+N|_{N^s}^{r_2}$ and $C' = |g|_{N^s}^{r_1'} \cdot |1+N|_{N^s}^{r_2'}$ for some $r_1, r_1' \in \mathbb{Z}_{\phi(N)/4}$ and $r_2, r_2' \in \mathbb{Z}_{N^{s-1}}$ with $r_2' \neq 0$ (because $C' \notin \mathcal{V}$).

Firstly $\mathsf{pk} = \mu(\mathsf{sk}) = (|g|_{N^s}^{k_1}, |g|_{N^s}^{k_2})$, which leaks $(k_1, k_2) \bmod \phi(N)/4$, but the values of $(k_1, k_2) \bmod N^{s-1}$ are totally hidden. Next, by Eq. (9),

$$\mathit{\Lambda}_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t) = \chi\big(|g|_{N^s}^{r_1 a(k_1+k_2 t)} \cdot |1+N|_{N^s}^{r_2 a(k_1+k_2 t)} \cdot (|g|_{N^s}^{r_1} \cdot |1+N|_{N^s}^{r_2})^{b_1+b_2 t}\big),$$

which may further leak the value of $(k_1 + k_2 t \bmod N^{s-1})$. Similarly,

$$\mathit{\Lambda}_{f_{(a',\mathsf{b}')}(\mathsf{sk})}(C', t') = \chi\big(\underbrace{|g|_{N^s}^{r_1' a'(k_1+k_2 t')} \cdot \boxed{|1+N|_{N^s}^{r_2' a'(k_1+k_2 t')}} \cdot (|g|_{N^s}^{r_1'} \cdot |1+N|_{N^s}^{r_2'})^{b_1'+b_2' t'}}_{(**)}\big).$$

Since $t \neq t' \in \mathbb{Z}_N$, it follows that $(k_1 + k_2 t' \bmod N^{s-1})$ is independent of $(k_1 + k_2 t \bmod N^{s-1})$,[5] and randomly distributed over $\mathbb{Z}_{N^{s-1}}$ conditioned on pk and $\mathit{\Lambda}_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$. Together with $r_2' \neq 0 \bmod N^{s-1}$ and $a' \in \mathbb{Z}_N^*$, the term $|1+N|_{N^s}^{r_2' a'(k_1+k_2 t')}$ is randomly distributed over a subgroup of $\mathbb{RU}_{N^s}^+$ of size at least $\min\{p, q\}$. So $(**)$ is randomly distributed over a subset $\mathcal{S}$ of the coset of $\mathbb{RU}_{N^s}^+$ with coset leader $|g|_{N^s}^{r_1' a'(k_1+k_2 t')} \cdot (|g|_{N^s}^{r_1'} \cdot |1+N|_{N^s}^{r_2'})^{b_1'+b_2' t'} \in \mathbb{J}_{N^s}^+$, where the size of $\mathcal{S}$ is at least $\min\{p, q\}$. By Corollary 4, the guessing probability of $\mathit{\Lambda}_{f_{(a',\mathsf{b}')}(\mathsf{sk})}(C', t') = \chi(**) = \chi(\mathsf{U}_{\mathcal{S}})$ is at most $2/|\mathcal{S}| \leq 2/p + 2/q$ conditioned on pk and $\mathit{\Lambda}_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$.

Therefore, for $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$, the guessing probability of $\mathit{\Lambda}_{f_{(a',\mathsf{b}')}(\mathsf{sk})}(C', t')$ is at most $4/p + 4/q$ conditioned on pk and $\mathit{\Lambda}_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$. This implies that $\mathsf{THPS}_{\mathsf{DCR}}$ is $\mathcal{F}_{\mathrm{raff}}$-universal$_2$ with $\epsilon^{u_2}_{\mathsf{THPS}, \mathcal{F}_{\mathrm{raff}}}(\ell) = 4/p + 4/q$, which is negligible in ℓ.

[$\mathcal{F}_{\mathbf{raff}}$**-Extracting.**] For all $f_{(a,\mathsf{b})} \in \mathcal{F}_{\mathrm{raff}}$ with $\mathsf{b} = (b_1, b_2)$, all $C \in \mathcal{C} = \mathbb{J}_{N^s}^+ \setminus \{1\}$ and all $t \in \mathcal{T}$, we can represent C as $C = |g|_{N^s}^{r_1} \cdot |1+N|_{N^s}^{r_2}$ for some $r_1 \in \mathbb{Z}_{\phi(N)/4}$ and $r_2 \in \mathbb{Z}_{N^{s-1}}$ with $(r_1, r_2) \neq (0, 0)$. For $\mathsf{sk} = (k_1, k_2) \leftarrow_{\$} \mathcal{SK}$, we consider the guessing probability of $\mathit{\Lambda}_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$.

- If $r_2 \neq 0$, i.e., $C \in \mathcal{C} \setminus \mathcal{V}$, then by the $\mathcal{F}_{\mathrm{raff}}$-universal$_2$ property, the guessing probability of $\mathit{\Lambda}_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t)$ is at most $4/p + 4/q$.
- If $r_2 = 0$ but $r_1 \neq 0$, i.e., $C \in \mathcal{V}$, then according to Eq. (9),

$$\mathit{\Lambda}_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t) = \chi\big(\underbrace{|g|_{N^s}^{r_1 a(k_1+k_2 t)+r_1(b_1+b_2 t)}}_{(***)}\big).$$

We let $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}'$, which has a negligible statistical distance $2/p + 2/q$ with $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$. Then $(k_1 + k_2 t \bmod \phi(N)/4)$ is randomly distributed over $\mathbb{Z}_{\phi(N)/4}$. Since $r_1 \neq 0$ and $\gcd(a, \phi(N)/4) = 1$, $(***)$ is randomly distributed over $\mathbb{CR}_{N^s}^+$. By Lemma 8, the guessing probability of $\mathit{\Lambda}_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C, t) = \chi(***) = \chi(\mathsf{U}_{\mathbb{CR}_{N^s}^+})$ is at most $(\mathsf{Adv}^{dcr}_{\mathsf{GenN}}(\ell) + 3/N^{s-1})^{1/2}$.

[5] Strictly speaking, this holds only if $\gcd(t - t', N) = 1$. However, in our applications, if $t \neq t' \in \mathbb{Z}_N$ but $\gcd(t - t', N) \neq 1$, i.e., $\gcd(t - t', N) \in \{p, q\}$, the adversary can factorize N thus break the DCR assumption w.r.t. GenN. Therefore, except with a negligible probability, we can always assume that $\gcd(t - t', N) = 1$.

Therefore, for $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$, the guessing probability of $\Lambda_{f_{(a,\mathsf{b})}(\mathsf{sk})}(C,t)$ is at most $2/p + 2/q + (\mathsf{Adv}^{dcr}_{\mathsf{GenN}}(\ell) + 3/N^{s-1})^{1/2}$.

Overall, $\mathsf{THPS}_{\mathsf{DCR}}$ is $\mathcal{F}_{\rm raff}$-extracting with $\epsilon^{ext}_{\mathsf{THPS},\mathcal{F}_{\rm raff}}(\ell) = \max\{4/p{+}4/q,\, 2/p{+}2/q{+}(\mathsf{Adv}^{dcr}_{\mathsf{GenN}}(\ell){+}3/N^{s-1})^{1/2}\}$, which is negligible in ℓ under the DCR assumption w.r.t. GenN.

[**$\mathcal{F}_{\rm raff}$-Public-Key-Homomorphism.**] For all $f_{(a,\mathsf{b})} \in \mathcal{F}_{\rm raff}$ with $\mathsf{b} = (b_1, b_2)$, and all $\mathsf{sk} = (k_1, k_2) \in \mathcal{SK}$, observe that

$$\begin{aligned} \mu\big(f_{(a,\mathsf{b})}(\mathsf{sk})\big) &= \mu(ak_1 + b_1, ak_2 + b_2) = \big(\ |g|_{N^s}^{ak_1+b_1}\ ,\ |g|_{N^s}^{ak_2+b_2}\ \big) \\ &= \big(\ (|g|_{N^s}^{k_1})^a \cdot |g|_{N^s}^{b_1}\ ,\ (|g|_{N^s}^{k_2})^a \cdot |g|_{N^s}^{b_2}\ \big). \end{aligned} \tag{10}$$

We define the $\mathcal{F}_{\rm raff}$-public-key transformer $\mathsf{THPS.PKTran} : \mathcal{PK} \times \mathcal{F}_{\rm raff} \longrightarrow \mathcal{PK}$ as follows: for any $\mathsf{pk} = (|h_1|_{N^s}, |h_2|_{N^s}) \in \mathcal{PK}$,

$$\mathsf{THPS.PKTran}(\mathsf{pk}, f_{(a,\mathsf{b})}) := \big(\ |h_1|_{N^s}^a \cdot |g|_{N^s}^{b_1}\ ,\ |h_2|_{N^s}^a \cdot |g|_{N^s}^{b_2}\ \big).$$

Then according to Eq. (10), $\mu\big(f_{(a,\mathsf{b})}(\mathsf{sk})\big) = \mathsf{THPS.PKTran}(\mu(\mathsf{sk}), f_{(a,\mathsf{b})})$.

[**$\mathcal{F}_{\rm raff}$-Poly-Bounded Collisions.**] For any pair of distinct $f_{(a,\mathsf{b})}, f_{(a',\mathsf{b}')} \in \mathcal{F}_{\rm raff}$ with $\mathsf{b} = (b_1, b_2)$ and $\mathsf{b}' = (b_1', b_2')$, we count the number of $\mathsf{sk} = (k_1, k_2) \in \mathcal{SK}$, such that $f_{(a,\mathsf{b})}(\mathsf{sk}) = f_{(a',\mathsf{b}')}(\mathsf{sk})$, i.e., $(ak_1 + b_1, ak_2 + b_2) = (a'k_1 + b_1', a'k_2 + b_2')$.

If $a = a'$ but $\mathsf{b} \neq \mathsf{b}'$, the equation can never be satisfied. If $a \neq a'$, there is exactly one sk satisfying the equation, i.e., $\mathsf{sk} = (k_i)_{i=1}^2 = \big((b_i' - b_i)/(a - a')\big)_{i=1}^2$.[6]

Therefore, $\max\limits_{f_{(a,\mathsf{b})} \neq f_{(a',\mathsf{b}')} \in \mathcal{F}_{\rm raff}} \big|\{\mathsf{sk} \in \mathcal{SK} \mid f_{(a,\mathsf{b})}(\mathsf{sk}) = f_{(a',\mathsf{b}')}(\mathsf{sk})\}\big| \leq 1.$ ▮

Theorem 6. *For the* $\mathsf{THPS}_{\mathsf{DCR}}$ *in Fig. 11, the SMP and PKCP are both hard under the DCR assumption w.r.t.* GenN.

Proof of Theorem 6.

[**Subset Membership Problem.**] Suppose that $\mathcal{A}$ is a PPT adversary against the SMP related to $\mathsf{THPS}_{\mathsf{DCR}}$, we construct a PPT adversary $\mathcal{B}$ against the DCR assumption w.r.t. GenN by invoking $\mathcal{A}$.

On input (N, v), $\mathcal{B}$ aims to tell whether $v = u$ or $v = u^{N^{s-1}} \bmod N^s$ for $u \leftarrow_{\$} \mathbb{Z}^*_{N^s}$. $\mathcal{B}$ samples a generator $|g|_{N^s} \leftarrow_{\$} \mathbb{CR}^+_{N^s}$, sets $\mathsf{prm}_{\mathsf{THPS}} := (N, |g|_{N^s})$ and $C := |v^2|_{N^s}$. Then $\mathcal{B}$ invokes $\mathcal{A}(\mathsf{prm}_{\mathsf{THPS}}, C)$ and outputs whatever $\mathcal{A}$ outputs.

In the case of $v = u$, C is uniformly distributed over $\mathbb{J}^+_{N^s}$, thus $C = 1$ with probability of $1/(\frac{1}{4}\phi(N)N^{s-1})$, C is randomly distributed over $\mathcal{V}$ with probability of $(\frac{1}{4}\phi(N){-}1)/(\frac{1}{4}\phi(N)N^{s-1})$, and C is randomly distributed over $\mathcal{C}\backslash\mathcal{V}$ with probability of $(\frac{1}{4}\phi(N)N^{s-1}{-}\frac{1}{4}\phi(N))/(\frac{1}{4}\phi(N)N^{s-1})$; in the case of $v = u^{N^{s-1}} \bmod N^s$, C is uniformly distributed over $\mathbb{CR}^+_{N^s}$, thus $C = 1$ with probability of $1/(\frac{1}{4}\phi(N))$ and C is randomly distributed over $\mathcal{V}$ with probability of $(\frac{1}{4}\phi(N) - 1)/(\frac{1}{4}\phi(N))$. In conclusion, we have that

$$\mathsf{Adv}^{dcr}_{\mathsf{GenN},\mathcal{B}}(\ell) \geq (1 - \tfrac{1}{N^{s-1}}) \cdot \mathsf{Adv}^{smp}_{\mathsf{THPS},\mathcal{A}}(\ell) - \tfrac{2}{\frac{1}{4}\phi(N)} \geq \tfrac{1}{2} \cdot \mathsf{Adv}^{smp}_{\mathsf{THPS},\mathcal{A}}(\ell) - \tfrac{8}{\phi(N)},$$

and the SMP related to $\mathsf{THPS}_{\mathsf{DCR}}$ is hard under the DCR assumption.

[6] Strictly speaking, $a - a'$ has inverse only if $\gcd(a - a', N) = 1$. By a similar argument as Footnote 5, we can always assume that $\gcd(a - a', N) = 1$, otherwise the adversary in our applications can break the DCR assumption w.r.t. GenN.

[Public-Key Collision problem.] Suppose that $\mathcal{A}'$ is a PPT adversary against the PKCP related to $\mathsf{THPS}_{\mathsf{DCR}}$, we construct a PPT adversary $\mathcal{B}'$ against the DCR assumption w.r.t. GenN by invoking $\mathcal{A}'$.

On input (N, v), $\mathcal{B}'$ aims to tell whether $v = u$ or $v = u^{N^{s-1}} \bmod N^s$ for $u \leftarrow_{\$} \mathbb{Z}^*_{N^s}$. $\mathcal{B}'$ samples $|g|_{N^s} \leftarrow_{\$} \mathbb{CR}^+_{N^s}$, and sets $\mathsf{prm}_{\mathsf{THPS}} := (N, |g|_{N^s})$. Then $\mathcal{B}'$ feeds $\mathcal{A}'$ with $\mathsf{prm}_{\mathsf{THPS}}$ and gets back a pair of $\mathsf{sk} = (k_1, k_2)$ and $\mathsf{sk}' = (k'_1, k'_2)$.

Suppose that $\mathcal{A}'$ succeeds, i.e., $\mathsf{sk} \neq \mathsf{sk}'$ but $\mu(\mathsf{sk}) = \mu(\mathsf{sk}')$, then we have that $(\,|g|^{k_1}_{N^s}, |g|^{k_2}_{N^s}\,) = (\,|g|^{k'_1}_{N^s}, |g|^{k'_2}_{N^s}\,)$, that is, $(\,|g|^{k_1-k'_1}_{N^s}, |g|^{k_2-k'_2}_{N^s}\,) = (1, 1)$. It must holds that $\phi(N)/4$ divides both $k_1 - k'_1$ and $k_2 - k'_2$. Without loss of generality, suppose that $k_1 \neq k'_1$, then $k_1 - k'_1$ must be a non-zero multiple of $\phi(N)/4$. In this case, it will be quite easy for $\mathcal{B}'$ to solve its own problem: $\mathcal{B}'$ simply checks whether or not $v^{k_1 - k'_1} = 1 \bmod N^s$ holds, and returns 1 if it is. Obviously, the equation holds if and only if $v = u'^{N^{s-1}} \bmod N^s$ for some $u' \in \mathbb{Z}^*_{N^s}$. In the case of $v = u$, $\mathcal{B}'$ outputs 1 with probability at most $1/N^{s-1}$; in the case of $v = u^{N^{s-1}} \bmod N^s$, $\mathcal{B}'$ will always output 1. Therefore

$$\mathsf{Adv}^{dcr}_{\mathsf{GenN},\mathcal{B}'}(\ell) \geq \mathsf{Adv}^{pkcp}_{\mathsf{THPS},\mathcal{A}'}(\ell) \cdot (1 - \tfrac{1}{N^{s-1}}) \geq \tfrac{1}{2} \cdot \mathsf{Adv}^{pkcp}_{\mathsf{THPS},\mathcal{A}'}(\ell),$$

and the PKCP related to $\mathsf{THPS}_{\mathsf{DCR}}$ is hard under the DCR assumption. ▌

Remark 4. For our applications, we can relax the function class $\mathcal{F}_{\mathrm{raff}}$ specified in Theorem 5 to $\widetilde{\mathcal{F}_{\mathrm{raff}}} = \big\{ f_{(a,\mathsf{b})} : (k_1, k_2) \in \mathcal{SK} \longmapsto (ak_1 + b_1, ak_2 + b_2) \in \mathcal{SK} \;\big|\; a \in \mathbb{Z}_N \backslash \{0\}, \gcd(a, \phi(N)/4) = 1, \mathsf{b} = (b_1, b_2) \in \mathcal{SK} \big\}$. The reason is that, if the adversary submits a function $f_{(a,\mathsf{b})} \in \widetilde{\mathcal{F}_{\mathrm{raff}}} \setminus \mathcal{F}_{\mathrm{raff}}$, i.e., $a \in \mathbb{Z}_N \backslash \{0\}$ but $a \notin \mathbb{Z}^*_N$, then $\gcd(a, N) \in \{p, q\}$, thus one can factorize N and break the DCR assumption w.r.t. GenN.

When plugging the $\mathsf{THPS}_{\mathsf{DCR}}$ into the paradigms in Fig. 4, Fig. 8 and Fig. 16, we obtain a MAC $\mathsf{MAC}[\mathsf{THPS}_{\mathsf{DCR}}]$, a PKE scheme $\mathsf{PKE}[\mathsf{THPS}_{\mathsf{DCR}}, \mathsf{AE}]$ and a SE scheme $\mathsf{SE}[\mathsf{THPS}_{\mathsf{DCR}}, \mathsf{AE}]$ respectively. The super-strong RKA securities of the resulting MAC, PKE and SE schemes are stated as follows.

Corollary 5. *If $\mathcal{H}$ is collision-resistant and the DCR assumption holds w.r.t.* GenN, *then the* $\mathsf{MAC}[\mathsf{THPS}_{\mathsf{DCR}}]$ *is super-strong EU-$\widetilde{\mathcal{F}_{raff}}$-RK-CMVA secure, where $\widetilde{\mathcal{F}_{raff}}$ is specified in Remark 4.*

If $\mathcal{H}_1$ is collision-resistant, $\mathcal{H}_2$ is universal, AE *is OT-secure with key space $\mathcal{K}_{\mathsf{AE}} = \{0,1\}^\ell$, and the DCR assumption holds w.r.t.* GenN, *then the* $\mathsf{PKE}[\mathsf{THPS}_{\mathsf{DCR}}, \mathsf{AE}]$ *and* $\mathsf{SE}[\mathsf{THPS}_{\mathsf{DCR}}, \mathsf{AE}]$ *are super-strong IND-$\widetilde{\mathcal{F}_{raff}}$-RK-CCA2 secure, where $\widetilde{\mathcal{F}_{raff}}$ is specified in Remark 4.*

The above corollary follows from Theorems 1, 2, 5, 6, Corollary 1 and Remark 4, as well as the fact that both $|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}_{\mathrm{raff}}}(\ell) = 2^\ell \cdot (4/p + 4/q)$ and $|\mathcal{K}_{\mathsf{AE}}|/|\mathcal{K}| = 2^\ell \cdot 2/(N^{s-1} + 1)$ are negligible in ℓ since p, q are of 2ℓ-bit.

Acknowledgments. The authors are supported by the National Natural Science Foundation of China Grant (Nos. 61672346 and 61373153).

References

[ABPP14] Abdalla, M., Benhamouda, F., Passelègue, A., Paterson, K.G.: Related-key security for pseudorandom functions beyond the linear barrier. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I, pp. 77–94 (2014)

[BC10] Bellare, M., Cash, D.: Pseudorandom functions and permutations provably secure against related-key attacks. In: Rabin, T. (ed.) CRYPTO 2010, pp. 666–684 (2010)

[BCM11] Bellare, M., Cash, D., Miller, R.: Cryptography secure against related-key attacks and tampering. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011, pp. 486–503 (2011)

[BDL97] Boneh, D., DeMillo, R.A., Lipton, R.J.: On the importance of checking cryptographic protocols for faults (extended abstract). In: Fumy, W. (ed.) EUROCRYPT 1997, pp. 37–51 (1997)

[Bih93] Biham, E.: New types of cryptanalytic attacks using related keys. In: Helleseth, T. (ed.) EUROCRYPT 1993, pp. 398–409 (1993)

[BK03] Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: Rka-prps, rka-prfs, and applications. In: Biham, E. (ed.) EUROCRYPT 2003, pp. 491–506 (2003)

[BPT12] Bellare, M., Paterson, K.G., Thomson, S.: RKA security beyond the linear barrier: IBE, encryption and signatures. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012, pp. 331–348 (2012)

[BR13] Bhattacharyya, R., Roy, A.: Secure message authentication against related-key attack. In: Moriai, S. (ed.) FSE 2013, pp. 305–324 (2013)

[BS97] Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Jr., B.S.K. (ed.) CRYPTO 1997, pp. 513–525 (1997)

[CHK04] Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004, pp. 207–222 (2004)

[CS02] Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002, LNCS, vol. 2332, pp. 45–64 (2002)

[CS04] Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. vol. 33(1), pp. 167–226 (2004)

[DFMV13] Damgård, I., Faust, S., Mukherjee, P., Venturi, D.: Bounded tamper resilience: How to go beyond the algebraic barrier. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II, pp. 140–160 (2013)

[DJ01] Damgård, I., Jurik, M.: A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. In: Kim, K. (ed.) PKC 2001, LNCS, vol. 1992, pp. 119–136. Springer (2001)

[DKPW12] Dodis, Y., Kiltz, E., Pietrzak, K., Wichs, D.: Message authentication, revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012, pp. 355–374 (2012)

[EHK$^+$13] Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.L.: An algebraic framework for diffie-hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II, pp. 129–147 (2013)

[GLM$^+$04] Gennaro, R., Lysyanskaya, A., Malkin, T., Micali, S., Rabin, T.: Algorithmic tamper-proof (ATP) security: Theoretical foundations for security against hardware tampering. In: Naor, M. (ed.) TCC 2004, pp. 258–277 (2004)

[HILL99] Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. SIAM J. Comput. vol. 28(4), pp. 1364–1396 (1999)

[HK09] Hofheinz, D., Kiltz, E.: The group of signed quadratic residues and applications. In: Halevi, S. (ed.) CRYPTO 2009, pp. 637–653 (2009)

[Hof16] Hofheinz, D.: Adaptive partitioning. IACR Cryptology ePrint Archive 2016/373 (2016)

[JLLM13] Jia, D., Lu, X., Li, B., Mei, Q.: RKA secure PKE based on the DDH and HR assumptions. In: Susilo, W., Reyhanitabar, R. (eds.) ProvSec 2013, pp. 271–287 (2013)

[JLLM14] Jia, D., Li, B., Lu, X., Mei, Q.: Related key secure PKE from hash proof systems. In: Yoshida, M., Mouri, K. (eds.) IWSEC 2014, pp. 250–265 (2014)

[KD04] Kurosawa, K., Desmedt, Y.: A new paradigm of hybrid encryption scheme. In: Franklin, M.K. (ed.) CRYPTO 2004, LNCS, vol. 3152, pp. 426–442. Springer (2004)

[KMO10] Kiltz, E., Mohassel, P., O'Neill, A.: Adaptive trapdoor functions and chosen-ciphertext security. In: Gilbert, H. (ed.) EUROCRYPT 2010, pp. 673–692 (2010)

[Knu92] Knudsen, L.R.: Cryptanalysis of LOKI91. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992, pp. 196–208 (1992)

[KPSY09] Kiltz, E., Pietrzak, K., Stam, M., Yung, M.: A new randomness extraction paradigm for hybrid encryption. In: Joux, A. (ed.) EUROCRYPT 2009, pp. 590–609 (2009)

[LLJ14] Lu, X., Li, B., Jia, D.: Related-key security for hybrid encryption. In: Chow, S.S.M., Camenisch, J., Hui, L.C.K., Yiu, S. (eds.) ISC 2014, pp. 19–32 (2014)

[MRV15] Morillo, P., Ràfols, C., Villar, J.L.: Matrix computational assumptions in multilinear groups. IACR Cryptology ePrint Archive 2015/353 (2015)

[QLC15] Qin, B., Liu, S., Chen, K.: Efficient chosen-ciphertext secure public-key encryption scheme with high leakage-resilience. IET Information Security vol. 9(1), pp. 32–42 (2015)

[WC81] Wegman, M.N., Carter, L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. vol. 22(3), pp. 265–279 (1981)

[Wee12] Wee, H.: Public key encryption against related key attacks. In: Fischlin, M., Buchmann, J.A., Manulis, M. (eds.) PKC 2012, pp. 262–279 (2012)

[Xag13] Xagawa, K.: Message authentication codes secure against additively related-key attacks. In: Symposium on Cryptography and Information Security (SCIS) (2013)

A Authenticated Encryption and Symmetric Encryption

A.1 Authenticated Encryption

An authenticated encryption (AE) scheme is associated with a message space $\mathcal{M}$ and a key space $\mathcal{K}_{\mathsf{AE}}$, and consists of a pair of PPT algorithms $\mathsf{AE} = (\mathsf{AE.Enc}, \mathsf{AE.Dec})$: $\mathsf{AE.Enc}(\kappa, m)$ takes as input a key $\kappa \in \mathcal{K}_{\mathsf{AE}}$ and a message $m \in \mathcal{M}$, and outputs a ciphertext χ; $\mathsf{AE.Dec}(\kappa, \chi)$ takes as input a key $\kappa \in \mathcal{K}_{\mathsf{AE}}$ and a ciphertext χ, and outputs a message $m \in \mathcal{M}$ or a rejection symbol $\perp$. Correctness of AE requires that, for all $\kappa \in \mathcal{K}_{\mathsf{AE}}$, all $m \in \mathcal{M}$ and all possible $\chi \leftarrow_{\$} \mathsf{AE.Enc}(\kappa, m)$, it holds that $\mathsf{AE.Dec}(\kappa, \chi) = m$.

The security notions for AE include One-time ciphertext-indistinguishability (IND-OT) and One-time ciphertext-integrity (INT-OT). The IND-OT and INT-OT securities of AE are formalized via the security games in Fig. 12.

```
Procedure INITIALIZE:
$\kappa \leftarrow_{\$} \mathcal{K}_{\mathsf{AE}}$.
$b \leftarrow_{\$} \{0, 1\}$.        // challenge bit
Return $\varepsilon$.

Procedure LR$(m_0, m_1)$: // one query
$\chi \leftarrow_{\$} \mathsf{AE.Enc}(\kappa, m_b)$.
Return $\chi$.

Procedure FINALIZE$(b')$:
Return $(b' = b)$.
```

```
Procedure INITIALIZE:
$\kappa \leftarrow_{\$} \mathcal{K}_{\mathsf{AE}}$.
Return $\varepsilon$.

Procedure LR$(m)$: // one query
$\chi \leftarrow_{\$} \mathsf{AE.Enc}(\kappa, m)$.
Return $\chi$.

Procedure FINALIZE$(\chi^*)$:
If $\chi^* = \chi$, Return 0.
Return $(\mathsf{AE.Dec}(\kappa, \chi^*) \neq \perp)$.
```

Fig. 12. Security games for AE. Left: $\mathsf{IND\text{-}OT}$; Right: $\mathsf{INT\text{-}OT}$.

Definition 23 (One-Time Security for AE). AE *is one-time secure (OT-secure), if it is IND-OT secure and INT-OT secure, i.e., for any PPT adversary* $\mathcal{A}$, *both* $\mathsf{Adv}^{\text{ind-ot}}_{\mathsf{AE},\mathcal{A}}(\ell) := |\Pr[\mathsf{IND\text{-}OT}^{\mathcal{A}} \Rightarrow 1] - 1/2|$ *and* $\mathsf{Adv}^{\text{int-ot}}_{\mathsf{AE},\mathcal{A}}(\ell) := \Pr[\mathsf{INT\text{-}OT}^{\mathcal{A}} \Rightarrow 1]$ *are negligible in* ℓ, *where games* $\mathsf{IND\text{-}OT}$ *and* $\mathsf{INT\text{-}OT}$ *are specified in Fig. 12.*

A.2 Symmetric Encryption

A symmetric encryption (SE) scheme consists of four PPT algorithms $\mathsf{SE} = (\mathsf{SE.Setup}, \mathsf{SE.Gen}, \mathsf{SE.Enc}, \mathsf{SE.Dec})$: $\mathsf{SE.Setup}(1^{\ell})$ outputs a system parameter prm, which implicitly defines a key space $\mathcal{K}_{\mathsf{SE}}$ and a message space $\mathcal{M}$; $\mathsf{SE.Gen}(\mathsf{prm})$ generates a key $\mathsf{k} \in \mathcal{K}_{\mathsf{SE}}$; $\mathsf{SE.Enc}(\mathsf{k}, m)$ takes as input a key $\mathsf{k} \in \mathcal{K}_{\mathsf{SE}}$ and a message $m \in \mathcal{M}$, and outputs a ciphertext c; $\mathsf{SE.Dec}(\mathsf{k}, c)$ takes as input a key $\mathsf{k} \in \mathcal{K}_{\mathsf{SE}}$ and a ciphertext c, and outputs a message $m \in \mathcal{M}$ or a rejection symbol $\perp$. Correctness of SE requires that, for all possible $\mathsf{prm} \leftarrow_{\$} \mathsf{SE.Setup}(1^{\ell})$, $\mathsf{k} \leftarrow_{\$} \mathsf{SE.Gen}(\mathsf{prm})$ and $m \in \mathcal{M}$, we have that $\mathsf{SE.Dec}(\mathsf{k}, \mathsf{SE.Enc}(\mathsf{k}, m)) = m$.

Procedure INITIALIZE:	**Proc.** LR($f^* \in \mathcal{F}, m_0, m_1$):	**Procedure** ENC($f \in \mathcal{F}, m$):	**Procedure** DEC($f \in \mathcal{F}, c$):
$\mathsf{prm} \leftarrow_{\$} \mathsf{SE.Setup}(1^{\ell})$. $\mathsf{k} \leftarrow_{\$} \mathsf{SE.Gen}(\mathsf{prm})$. $b \leftarrow_{\$} \{0, 1\}$. Return prm.	// one query $\mathsf{k}'^* := f^*(\mathsf{k}) \in \mathcal{K}_{\mathsf{SE}}$. $c^* \leftarrow_{\$} \mathsf{SE.Enc}(\mathsf{k}'^*, m_b)$. $\mathcal{Q}_{\mathcal{ENC}} := \{(\mathsf{k}'^*, c^*)\}$. Return c^*.	$\mathsf{k}' := f(\mathsf{k}) \in \mathcal{K}_{\mathsf{SE}}$. $c \leftarrow_{\$} \mathsf{SE.Enc}(\mathsf{k}', m)$. Return c.	$\mathsf{k}' := f(\mathsf{k}) \in \mathcal{K}_{\mathsf{SE}}$. If $(\mathsf{k}', c) \in \mathcal{Q}_{\mathcal{ENC}}$, Return $\perp$. Return $\mathsf{SE.Dec}(\mathsf{k}', c)$. **Procedure** FINALIZE(b'): Return $(b' = b)$.

Fig. 13. IND-$\mathcal{F}$-RK-CCA2 security game for SE.

Let $\mathcal{F}$ be a class of functions from $\mathcal{K}_{\mathsf{SE}}$ to $\mathcal{K}_{\mathsf{SE}}$. We define the indistinguishability under $\mathcal{F}$-related-key chosen-plaintext and chosen-ciphertext attacks (IND-$\mathcal{F}$-RK-CCA2) according to [BCM11], where the adversary can obtain a challenge ciphertext, and make encryption and decryption queries under any $\mathcal{F}$-related key.

Definition 24 (IND-$\mathcal{F}$-RK-CCA2 Security for SE). *SE is IND-$\mathcal{F}$-RK-CCA2 secure, if for any PPT adversary $\mathcal{A}$, the advantage $\mathsf{Adv}^{\text{ind-rk-cca2}}_{\mathsf{SE},\mathcal{F},\mathcal{A}}(\ell) := \left|\Pr[\mathsf{IND}\text{-}\mathcal{F}\text{-}\mathsf{RK}\text{-}\mathsf{CCA2}^{\mathcal{A}} \Rightarrow 1] - \frac{1}{2}\right|$ is negligible in ℓ, where game IND-$\mathcal{F}$-RK-CCA2 is specified in Fig. 13.*

B Proof of Lemma 2

The $\mathcal{F}$-universal$_2$ property implies that, for all $\mathsf{prm}_{\mathsf{THPS}} \leftarrow_{\$} \mathsf{THPS.Setup}(1^{\ell})$,

$$\max_{f', \mathsf{pk}, C', t', K'} \Pr\left[\Lambda_{f'(\mathsf{sk})}(C', t') = K' \mid \mu(\mathsf{sk}) = \mathsf{pk}\right] \leq \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell),$$

where the maximum is over all $f' \in \mathcal{F}$, all $\mathsf{pk} \in \mathcal{PK}$, all $C' \in \mathcal{C} \setminus \mathcal{V}$, all $t' \in \mathcal{T}$ and all $K' \in \mathcal{K}$, and the probability is over $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$.

By a simple fact about guessing probability (i.e., for any random variable X over $\mathcal{X}$ and any function f from $\mathcal{X}$ to $\mathcal{Y}$, $\max\limits_{x \in \mathcal{X}} \Pr[X = x] \leq \max\limits_{y \in \mathcal{Y}} \Pr[f(X) = y]$), we get that

$$\max_{\mathsf{sk}' \in \mathcal{SK}} \Pr[\mathsf{sk} = \mathsf{sk}' \mid \mu(\mathsf{sk}) = \mathsf{pk}] \leq \max_{f', \mathsf{pk}, C', t', K'} \Pr\left[\Lambda_{f'(\mathsf{sk})}(C', t') = K' \mid \mu(\mathsf{sk}) = \mathsf{pk}\right],$$

and the lemma follows from the above two in-equations.

C Description of Games G_1–G_6 in the Proof of Theorem 2

- Game G_1: This game is the same as game G_0, except that, the challenger changes the way it computes pk'^*, K^* in LR and pk' in ENC and DEC.

  In game G_0, the challenger computes $\mathsf{pk}'^* := \mu(\mathsf{sk}'^*)$ with $\mathsf{sk}'^* := f^*(\mathsf{sk})$ in LR(f^*, m_0, m_1) and $\mathsf{pk}' := \mu(\mathsf{sk}')$ with $\mathsf{sk}' := f(\mathsf{sk})$ in ENC(f, m) and DEC$\big(f, \langle C, \chi\rangle\big)$. Now in game G_1, it simply invokes the $\mathcal{F}$-public-key transformer $\mathsf{THPS.PKTran}$ to compute $\mathsf{pk}'^* := \mathsf{THPS.PKTran}(\mathsf{pk}, f^*)$ in LR and $\mathsf{pk}' := \mathsf{THPS.PKTran}(\mathsf{pk}, f)$ in Enc and Dec.

Since THPS is $\mathcal{F}$-public-key-homomorphic, this change is conceptual.

In addition, in game G_0, the challenger computes $K^* := \mathsf{THPS.Pub}(\mathsf{pk}'^*,\ C^*, w^*, t^*)$ in LR. Now in game G_1, it computes $K^* := \Lambda_{\mathsf{sk}'^*}(C^*, t^*)$.

By the fact that THPS is projective, it holds that

$$\begin{aligned} K^* &\overset{\mathsf{G}_0}{=} \mathsf{THPS.Pub}(\mathsf{pk}'^*, C^*, w^*, t^*) && : \ C^* \leftarrow_\$ \mathcal{V} \text{ with witness } w^* \\ &\overset{\mathsf{G}_1}{=} \Lambda_{\mathsf{sk}'^*}(C^*, t^*) && : \ \text{via projective property.} \end{aligned}$$

Therefore G_1 is identical to G_0, and $\Pr_0[\mathsf{Win}] = \Pr_1[\mathsf{Win}]$.

Next, through the following games G_2–G_5, the challenger will answer Dec queries $\big(f, \langle C, \chi\rangle\big)$ in different ways (and finally avoid using the secret key sk), as long as $t = t^*$, where $t = \mathsf{H}_1(\mathsf{pk}', C)$ and $t^* = \mathsf{H}_1(\mathsf{pk}'^*, C^*)$.

More precisely, we divide the event that $t = t^*$ into four cases:

- Case 1: $t = t^* \wedge (f, C) = (f^*, C^*)$
- Case 2: $t = t^* \wedge \big(C \neq C^* \vee (C = C^* \wedge \mathsf{pk}' \neq \mathsf{pk}'^*)\big)$
- Case 3: $t = t^* \wedge C = C^* \wedge \mathsf{pk}' = \mathsf{pk}'^* \wedge \mathsf{sk}' \neq \mathsf{sk}'^*$
- Case 4: $t = t^* \wedge C = C^* \wedge \mathsf{sk}' = \mathsf{sk}'^* \wedge f \neq f^*$

In the next four games, the challenger will handle these cases one by one.

– Game G_2: This game is the same as game G_1, except that, when answering $\mathrm{Dec}\big(f, \langle C, \chi\rangle\big)$, if Case 1 occurs, i.e., $t = t^* \wedge (f, C) = (f^*, C^*)$, the challenger directly sets $\kappa := \kappa^*$ instead of computing $\kappa := \mathsf{H}_2(K)$.

Suppose that Case 1 holds. Clearly, $f = f^*$ leads to $\mathsf{sk}' = \mathsf{sk}'^*$. Thus in game G_1,

$$K = \Lambda_{\mathsf{sk}'}(C, t) = \Lambda_{\mathsf{sk}'^*}(C^*, t^*) = K^*, \qquad \kappa = \mathsf{H}_2(K) = \mathsf{H}_2(K^*) = \kappa^*.$$

Therefore in Case 1, $\kappa = \kappa^*$ holds both in G_1 and G_2. Then G_2 is identical to G_1, and $\Pr_1[\mathsf{Win}] = \Pr_2[\mathsf{Win}]$.

– Game G_3: This game is the same as game G_2, except that, when answering $\mathrm{Dec}\big(f, \langle C, \chi\rangle\big)$, if Case 2 occurs, i.e., $t = t^* \wedge \big(C \neq C^* \vee (C = C^* \wedge \mathsf{pk}' \neq \mathsf{pk}'^*)\big)$, the challenger returns $\perp$ directly.

Since $t = \mathsf{H}_1(\mathsf{pk}', C)$ and $t^* = \mathsf{H}_1(\mathsf{pk}'^*, C^*)$, any difference between G_2 and G_3 will imply a collision of $\mathcal{H}_1$. Thus $\big|\Pr_2[\mathsf{Win}] - \Pr_3[\mathsf{Win}]\,\big| \leq \mathsf{Adv}^{cr}_{\mathcal{H}_1}(\ell)$.

– Game G_4: This game is the same as game G_3, except that, when answering $\mathrm{Dec}\big(f, \langle C, \chi\rangle\big)$, if Case 3 occurs, i.e., $t = t^* \wedge C = C^* \wedge \mathsf{pk}' = \mathsf{pk}'^* \wedge \mathsf{sk}' \neq \mathsf{sk}'^*$, the challenger simply returns $\perp$.

Let PKColl denote the event that $\mathcal{A}$ ever queries $\mathrm{Dec}\big(f, \langle C, \chi\rangle\big)$, such that $\mathsf{pk}' = \mathsf{pk}'^*$ but $\mathsf{sk}' \neq \mathsf{sk}'^*$. Clearly G_3 and G_4 are the same unless PKColl occurs. We have that $\big|\Pr_3[\mathsf{Win}] - \Pr_4[\mathsf{Win}]\,\big| \leq \Pr_4[\mathsf{PKColl}]$.

Since $\mathsf{pk}' = \mu(\mathsf{sk}')$ and $\mathsf{pk}'^* = \mu(\mathsf{sk}'^*)$, it is straightforward to construct a PPT adversary to solve the PKCP related to THPS, such that $\Pr_4[\mathsf{PKColl}] \leq \mathsf{Adv}^{pkcp}_{\mathsf{THPS}}(\ell)$. Therefore $\big|\Pr_3[\mathsf{Win}] - \Pr_4[\mathsf{Win}]\,\big| \leq \mathsf{Adv}^{pkcp}_{\mathsf{THPS}}(\ell)$.

- Game G_5: This game is the same as game G_4, except that, when answering $\textsc{Dec}\big(f, \langle C, \chi\rangle\big)$, if Case 4 occurs, i.e., $t = t^* \wedge C = C^* \wedge \mathsf{sk}' = \mathsf{sk}'^* \wedge f \neq f^*$, the challenger directly returns $\perp$.

  Let Guess denote the event that $\mathcal{A}$ ever queries $\textsc{Dec}(f, \langle C, \chi\rangle)$, such that $\mathsf{sk}' = \mathsf{sk}'^*$ but $f \neq f^*$. Clearly G_4 and G_5 are the same unless Guess occurs. Therefore we have that

$$\big|\Pr_4[\mathsf{Win}] - \Pr_5[\mathsf{Win}]\big| \le \Pr_5[\mathsf{Guess}]. \tag{11}$$

We will give an upper bound on $\Pr_5[\mathsf{Guess}]$. However, the analysis of $\Pr_5[\mathsf{Guess}]$ is not an easy task, and we will defer it to the following game G_5'.

– Game G_5': It is the same as game G_5, except that, when answering $\textsc{Dec}\big(f, \langle C, \chi\rangle\big)$, if $t \neq t^*$ and $C \in \mathcal{C} \setminus \mathcal{V}$, the challenger returns $\perp$ directly instead of outputting $\mathsf{AE.Dec}(\kappa, \chi)$.

Let Bad denote the event that $\mathcal{A}$ ever queries $\textsc{Dec}(f, \langle C, \chi\rangle)$, such that $C \in \mathcal{C} \setminus \mathcal{V}$ but $\mathsf{AE.Dec}(\kappa, \chi) \neq \perp$. Clearly games G_5 and G_5' are the same until Bad happens, thus

$$\big|\Pr_5[\mathsf{Guess}] - \Pr_5'[\mathsf{Guess}]\big| \le \Pr_5'[\mathsf{Bad}]. \tag{12}$$

We give an upper bound on $\Pr_5'[\mathsf{Bad}]$ via the following lemma.

Lemma 9. $\Pr_5'[\mathsf{Bad}] \le Q_d \cdot \Big(\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)\Big)$.

Proof. The proof follows the high-level strategy of that for Lemma 3, however, they differ in the low-level analysis. We consider the information about sk that $\mathcal{A}$ may obtain in game G_5'.

- For $\textsc{Initialize}$, the value of $\mathsf{pk} = \mu(\mathsf{sk})$ is leaked to $\mathcal{A}$.
- For $\mathrm{LR}(f^*, m_0, m_1)$, the challenger can use pk to compute pk'^* and K^*. More precisely, $\mathsf{pk}'^* = \mathsf{THPS.PKTran}(\mathsf{pk}, f^*)$ and

$$\begin{aligned} K^* &= \Lambda_{\mathsf{sk}'^*}(C^*, t^*) && : \ C^* \leftarrow_\$ \mathcal{V} \text{ with witness } w^* \\ &= \mathsf{THPS.Pub}(\mathsf{pk}'^*, C^*, w^*, t^*) && : \ \text{via projective property.} \end{aligned}$$

- For $\textsc{Enc}(f, m)$, the challenger uses pk to compute pk' and K by $\mathsf{pk}' = \mathsf{THPS.PKTran}(\mathsf{pk}, f)$ and $K = \mathsf{THPS.Pub}(\mathsf{pk}', C, w, t)$.
- For $\textsc{Dec}\big(f, \langle C, \chi\rangle\big)$, the challenger uses pk to compute pk' by $\mathsf{pk}' = \mathsf{THPS.PKTran}(\mathsf{pk}, f)$.
  - If $t = t^* \wedge (f, C) = (f^*, C^*)$, i.e., Case 1 occurs, the challenger does not use sk at all but simply sets $\kappa = \kappa^*$.
  - If $t = t^* \wedge (f, C) \neq (f^*, C^*)$, i.e., Case 2 or Case 3 or Case 4 occurs, the challenger does not use sk and returns $\perp$ directly.
  - If $t \neq t^*$ and $C \in \mathcal{C} \setminus \mathcal{V}$, the challenger returns $\perp$ directly.
  - If $t \neq t^*$ and $C \in \mathcal{V}$, the challenger computes $K = \Lambda_{\mathsf{sk}'}(C, t)$, which leaks at most pk' to $\mathcal{A}$ since THPS is projective.

Thus the only information about sk that $\mathcal{A}$ may get in G_5' is $\mathsf{pk} = \mu(\mathsf{sk})$.

The event Bad occurs in game G_5' means that $\mathcal{A}$ ever queries $\textsc{Dec}(f, \langle C, \chi\rangle)$ such that $C \in \mathcal{C} \setminus \mathcal{V}$ but $\mathsf{AE.Dec}(\kappa, \chi) \neq \perp$, where $\kappa := \mathsf{H}_2(K)$ with $K := \Lambda_{\mathsf{sk}'}(C, t) = \Lambda_{f(\mathsf{sk})}(C, t)$.

Since $C \in \mathcal{C} \setminus \mathcal{V}$, by the $\mathcal{F}$-universal$_2$ property of THPS, the guessing probability of $K = \Lambda_{f(\mathsf{sk})}(C, t)$ is at most $\epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)$ conditioned on $\mathsf{pk} = \mu(\mathsf{sk})$. Then by the Leftover Hash Lemma (i.e., Lemma 1), since H_2 is universal, $\kappa := \mathsf{H}_2(K)$ is statistically close to the uniform distribution over $\mathcal{K}_{\mathsf{AE}}$, with statistical distance $\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)}$. For $\kappa \leftarrow_{\$} \mathcal{K}_{\mathsf{AE}}$, $\mathsf{AE.Dec}(\kappa, \chi) \neq \perp$ will hold with probability at most $\mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)$. Thus in one DEC query, Bad occurs with probability at most $\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)$.

By a union bound, $\Pr'_5[\mathsf{Bad}] \leq Q_d \cdot \big(\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)\big)$ and the lemma follows. ▌

Finally, we analyze $\Pr'_5[\mathsf{Guess}]$. Recall that in the proof of Lemma 9, we observe that the only information about sk that $\mathcal{A}$ may get in game G'_5 is $\mathsf{pk} = \mu(\mathsf{sk})$. Since THPS is $\mathcal{F}$-universal$_2$, by Lemma 2, given pk, the conditional guessing probability of sk is at most $\epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

Since THPS has $\mathcal{F}$-poly-bounded collisions, i.e.,

$$\max_{f \neq f^* \in \mathcal{F}} \big|\{\mathsf{sk} \in \mathcal{SK} \mid f(\mathsf{sk}) = f^*(\mathsf{sk})\}\big| \leq p(\ell),$$

for some polynomial $p(\ell)$, in one DEC query $\big(f, \langle C, \chi\rangle\big)$, the event $\mathsf{sk}' = f(\mathsf{sk}) = f^*(\mathsf{sk}) = \mathsf{sk}'^*$ but $f \neq f^*$ can hold with probability at most $p(\ell) \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)$. By a union bound over Q_d times of DEC queries,

$$\Pr'_5[\mathsf{Guess}] \leq Q_d \cdot p(\ell) \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell). \tag{13}$$

By combining Eqs. (11)-(13) and Lemma 9, we get that $\big|\Pr_4[\mathsf{Win}] - \Pr_5[\mathsf{Win}]\ \big| \leq Q_d \cdot \big(\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)\big) + Q_d \cdot p(\ell) \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

Next, we consider a sequence of games $\mathsf{G}_{5,1}$–$\mathsf{G}_{5,4}$, as shown in Fig. 14, which are defined analogous to $\{\mathsf{G}_{5,i,0}$–$\mathsf{G}_{5,i,4}\}_{i \in [Q_t]}$ in the proof of Theorem 1.

- Game $\mathsf{G}_{5,1}$: This game is the same as game G_5, except that, in $\mathrm{LR}(f^*, m_0, m_1)$, the challenger samples C^* uniformly from $\mathcal{C} \setminus \mathcal{V}$ instead of $\mathcal{V}$.

  It is straightforward to bound the difference between G_5 and $\mathsf{G}_{5,1}$ by constructing a PPT adversary to solve the SMP related to THPS, such that $\big|\Pr_5[\mathsf{Win}] - \Pr_{5,1}[\mathsf{Win}]\ \big| \leq \mathsf{Adv}^{smp}_{\mathsf{THPS}}(\ell)$.

- Game $\mathsf{G}_{5,2}$: This game is the same as game $\mathsf{G}_{5,1}$, except that, when answering $\mathrm{DEC}\big(f, \langle C,\ \chi\rangle\big)$, if $t \neq t^*$ and $C \in \mathcal{C} \setminus \mathcal{V}$, the challenger directly returns $\perp$ instead of outputting $\mathsf{AE.Dec}(\kappa, \chi)$.

  Let $\widetilde{\mathsf{Bad}}$ denote the event that $\mathcal{A}$ ever queries $\mathrm{DEC}(f, \langle C, \chi\rangle)$ such that $t \neq t^*$ and $C \in \mathcal{C} \setminus \mathcal{V}$ but $\mathsf{AE.Dec}(\kappa, \chi) \neq \perp$. Clearly $\mathsf{G}_{5,1}$ and $\mathsf{G}_{5,2}$ are the same until $\widetilde{\mathsf{Bad}}$ happens, therefore $\big|\Pr_{5,1}[\mathsf{Win}] - \Pr_{5,2}[\mathsf{Win}]\ \big| \leq \Pr_{5,2}[\widetilde{\mathsf{Bad}}]$.

  We give an upper bound on $\Pr_{5,2}[\widetilde{\mathsf{Bad}}]$ via the following lemma.

Lemma 10. $\Pr_{5,2}[\widetilde{\mathsf{Bad}}] \leq Q_d \cdot \big(\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)\big)$.

Proof. The proof is essentially a combination of that for Lemma 4 and 9. We consider the information about sk that $\mathcal{A}$ may get in game $\mathsf{G}_{5,2}$.

- For INITIALIZE, the value of $\mathsf{pk} = \mu(\mathsf{sk})$ is leaked to $\mathcal{A}$.
- For $\mathrm{LR}(f^*, m_0, m_1)$, the challenger can use pk to compute pk'^* by $\mathsf{pk}'^* = \mathsf{THPS.PKTran}(\mathsf{pk}, f^*)$. However, the challenger may leak the value of $K^* = \Lambda_{\mathsf{sk}'^*}(C^*, t^*) = \Lambda_{f^*(\mathsf{sk})}(C^*, t^*)$ to $\mathcal{A}$, where $C^* \leftarrow_{\$} \mathcal{C} \setminus \mathcal{V}$.
- For $\mathrm{ENC}(f, m)$, the challenger uses pk to compute pk' and K by $\mathsf{pk}' = \mathsf{THPS.PKTran}(\mathsf{pk}, f)$ and $K = \mathsf{THPS.Pub}(\mathsf{pk}', C, w, t)$.

```
$\textsc{Dec}\big(f \in \mathcal{F}, \langle C, \chi\rangle\big)$:
  // $\mathsf{G}_5$, $\mathsf{G}_{5,1}$, $\mathsf{G}_{5,2}$, $\mathsf{G}_{5,3}$, $\mathsf{G}_{5,4}$, $\mathsf{G}_6$
  If $(f, \langle C, \chi\rangle) \in \mathcal{Q}_{\mathcal{ENC}}$, Return $\perp$.
  $\mathsf{pk}' := \mathsf{THPS.PKTran}(\mathsf{pk}, f) \in \mathcal{PK}$.
  If $C \notin \mathcal{C}$, Return $\perp$.
  $t := \mathsf{H}_1(\mathsf{pk}', C) \in \mathcal{T}$.
  If $t = t^*$,
      If $(f, C) = (f^*, C^*)$,
          $\kappa := \kappa^*$.
      If $(f, C) \neq (f^*, C^*)$,
          Return $\perp$.
  Else $t \neq t^*$,
      If $C \in \mathcal{C} \setminus \mathcal{V}$, Return $\perp$.
      If $C \in \mathcal{V}$,
          $K := \Lambda_{\mathsf{sk}'}(C, t) \in \mathcal{K}$.
          $\kappa := \mathsf{H}_2(K) \in \mathcal{K}_{\mathsf{AE}}$.
  Return $\mathsf{AE.Dec}(\kappa, \chi)$.

$\textsc{Initialize}$ & $\textsc{Finalize}(b')$.
      // same as in Fig. 9
```

```
$\mathrm{LR}(f^* \in \mathcal{F}, m_0, m_1)$:   // one query
  // $\mathsf{G}_5$, $\boxed{\mathsf{G}_{5,1},\ \mathsf{G}_{5,2},\ \boxed{\mathsf{G}_{5,3},\ \mathsf{G}_{5,4}}}$, $\boxed{\mathsf{G}_6}$
  $\mathsf{pk}'^* := \mathsf{THPS.PKTran}(\mathsf{pk}, f^*) \in \mathcal{PK}$.
  $C^* \leftarrow_{\$} \mathcal{V}$ with witness $w^*$.
  $\boxed{C^* \leftarrow_{\$} \mathcal{C} \setminus \mathcal{V}.}$
  $t^* := \mathsf{H}_1(\mathsf{pk}'^*, C^*) \in \mathcal{T}$.
  $K^* := \Lambda_{\mathsf{sk}'^*}(C^*, t^*) \in \mathcal{K}$.
  $\boxed{K^* \leftarrow_{\$} \mathcal{K}.}$
  $\kappa^* := \mathsf{H}_2(K^*) \in \mathcal{K}_{\mathsf{AE}}$.
  $\chi^* \leftarrow_{\$} \mathsf{AE.Enc}(\kappa^*, m_b)$.
  $\mathcal{Q}_{\mathcal{ENC}} := \big\{(f^*, \langle C^*, \chi^*\rangle)\big\}$.
  Return $\langle C^*, \chi^*\rangle$.

$\textsc{Enc}(f \in \mathcal{F}, m)$:        // $\mathsf{G}_5$–$\mathsf{G}_6$
  $\mathsf{pk}' := \mathsf{THPS.PKTran}(\mathsf{pk}, f) \in \mathcal{PK}$.
  $C \leftarrow_{\$} \mathcal{V}$ together with witness $w$.
  $t := \mathsf{H}_1(\mathsf{pk}', C) \in \mathcal{T}$.
  $K := \mathsf{THPS.Pub}(\mathsf{pk}', C, w, t) \in \mathcal{K}$.
  $\kappa := \mathsf{H}_2(K) \in \mathcal{K}_{\mathsf{AE}}$.
  $\chi \leftarrow_{\$} \mathsf{AE.Enc}(\kappa, m)$.
  Return $\langle C, \chi\rangle$.
```

Fig. 14. Games G_5, $\{\mathsf{G}_{5,1}\text{–}\mathsf{G}_{5,4}\}$, G_6 for super-strong IND-$\mathcal{F}$-RK-CCA2 security of $\mathsf{PKE}[\mathsf{THPS}, \mathsf{AE}]$.

- For $\textsc{Dec}\big(f, \langle C, \chi\rangle\big)$, the challenger uses pk to compute pk' by $\mathsf{pk}' = \mathsf{THPS.PKTran}(\mathsf{pk}, f)$.
  - If $t = t^* \wedge (f, C) = (f^*, C^*)$, the challenger does not use sk at all but simply sets $\kappa = \kappa^*$.
  - If $t = t^* \wedge (f, C) \neq (f^*, C^*)$, the challenger returns $\perp$.
  - If $t \neq t^*$ and $C \in \mathcal{C} \setminus \mathcal{V}$, the challenger returns $\perp$.
  - If $t \neq t^*$ and $C \in \mathcal{V}$, the challenger computes $K = \Lambda_{\mathsf{sk}'}(C, t)$, which leaks at most pk' to $\mathcal{A}$ since THPS is projective.

Thus the only information about sk that $\mathcal{A}$ may get in game $\mathsf{G}_{5,2}$ is $\mathsf{pk} = \mu(\mathsf{sk})$ and $K^* = \Lambda_{f^*(\mathsf{sk})}(C^*, t^*)$, where $C^* \leftarrow_{\$} \mathcal{C} \setminus \mathcal{V}$.

The event $\widetilde{\mathsf{Bad}}$ occurs in game $\mathsf{G}_{5,2}$ means that $\mathcal{A}$ ever queries $\textsc{Dec}(f, \langle C, \chi\rangle)$ such that $t \neq t^*$ and $C \in \mathcal{C} \setminus \mathcal{V}$ but $\mathsf{AE.Dec}(\kappa, \chi) \neq \perp$, where $\kappa := \mathsf{H}_2(K)$ with $K := \Lambda_{\mathsf{sk}'}(C, t) = \Lambda_{f(\mathsf{sk})}(C, t)$.

Since $C \in \mathcal{C} \setminus \mathcal{V}$ and $t \neq t^*$, by the $\mathcal{F}$-universal$_2$ property of THPS, the guessing probability of $K = \Lambda_{f(\mathsf{sk})}(C, t)$ is at most $\epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)$ conditioned on $\mathsf{pk} = \mu(\mathsf{sk})$ and $K^* = \Lambda_{f^*(\mathsf{sk})}(C^*, t^*)$. Then by the Leftover Hash Lemma, since H_2 is universal, $\kappa := \mathsf{H}_2(K)$ is statistically close to the uniform distribution over $\mathcal{K}_{\mathsf{AE}}$, with statistical distance $\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)}$. For $\kappa \leftarrow_{\$} \mathcal{K}_{\mathsf{AE}}$, $\mathsf{AE.Dec}(\kappa, \chi) \neq \perp$ will hold with probability at most $\mathsf{Adv}^{\textit{int-ot}}_{\mathsf{AE}}(\ell)$. Thus in one $\textsc{Dec}$ query, $\widetilde{\mathsf{Bad}}$ occurs with probability at most $\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{\textit{int-ot}}_{\mathsf{AE}}(\ell)$.

By a union bound, $\Pr_{5,2}[\widetilde{\mathsf{Bad}}] \leq Q_d \cdot \Big(\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{\textit{int-ot}}_{\mathsf{AE}}(\ell)\Big)$. The lemma follows. ▌

Thus $\big|\Pr_{5,1}[\mathsf{Win}] - \Pr_{5,2}[\mathsf{Win}]\big| \leq Q_d \cdot \Big(\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{\textit{int-ot}}_{\mathsf{AE}}(\ell)\Big)$.

- Game $\mathsf{G}_{5,3}$: This game is the same as game $\mathsf{G}_{5,2}$, except that, in $\mathrm{LR}(f^*, m_0, m_1)$, the challenger samples K^* uniformly from $\mathcal{K}$ instead of computing $K^* := \Lambda_{\mathsf{sk}'^*}(C^*, t^*) = \Lambda_{f^*(\mathsf{sk})}(C^*, t^*)$.

  Recall that in the proof of Lemma 10, we observe that the only information about sk that $\mathcal{A}$ may get in game $\mathsf{G}_{5,2}$ is $\mathsf{pk} = \mu(\mathsf{sk})$ and $K^* = \Lambda_{f^*(\mathsf{sk})}(C^*, t^*)$, where $C^* \leftarrow_\$ \mathcal{C} \setminus \mathcal{V}$. By the average-case $\mathcal{F}$-strongly-universal$_1$ property of THPS, the joint distribution of $(\mathsf{pk}, C^*, K^* = \Lambda_{f^*(\mathsf{sk})}(C^*, t^*))$ in game $\mathsf{G}_{5,2}$ is statistically close to $(\mathsf{pk}, C^*, K^* = \mathsf{U}_{\mathcal{K}})$, with statistical distance $\epsilon^{ac\text{-}str\text{-}u_1}_{\mathsf{THPS},\mathcal{F}}(\ell)$. The latter distribution is exactly the one used in game $\mathsf{G}_{5,3}$.

  Therefore, games $\mathsf{G}_{5,2}$ and $\mathsf{G}_{5,3}$ are statistically close with statistical distance $\epsilon^{ac\text{-}str\text{-}u_1}_{\mathsf{THPS},\mathcal{F}}(\ell)$, i.e., $\big|\Pr_{5,2}[\mathsf{Win}] - \Pr_{5,3}[\mathsf{Win}]\big| \le \epsilon^{ac\text{-}str\text{-}u_1}_{\mathsf{THPS},\mathcal{F}}(\ell)$.

- Game $\mathsf{G}_{5,4}$: This game is the same as game $\mathsf{G}_{5,3}$, except that, when answering $\textsc{Dec}\big(f, \langle C, \chi\rangle\big)$, if $t \neq t^*$ and $C \in \mathcal{C} \setminus \mathcal{V}$, the challenger outputs $\mathsf{AE.Dec}(\kappa, \chi)$ again, instead of returning $\perp$ directly. That is, the challenger will output $\mathsf{AE.Dec}(\kappa, \chi)$ no matter $C \in \mathcal{V}$ or $C \in \mathcal{C} \setminus \mathcal{V}$.

  The analysis of the difference between games $\mathsf{G}_{5,3}$ and $\mathsf{G}_{5,4}$ is analogous to that between $\mathsf{G}_{5,1}$ and $\mathsf{G}_{5,2}$. Similarly, we have that $\big|\Pr_{5,3}[\mathsf{Win}] - \Pr_{5,4}[\mathsf{Win}]\big| \le Q_d \cdot \big(\sqrt{|\mathcal{K}_{\mathsf{AE}}| \cdot \epsilon^{u_2}_{\mathsf{THPS},\mathcal{F}}(\ell)} + \mathsf{Adv}^{int\text{-}ot}_{\mathsf{AE}}(\ell)\big)$.

- Game G_6: This game is the same as game $\mathsf{G}_{5,4}$, except that, in $\mathrm{LR}(f^*, m_0, m_1)$, the challenger samples C^* uniformly from $\mathcal{V}$ instead of $\mathcal{C} \setminus \mathcal{V}$.

  It is easy to construct a PPT adversary to solve the SMP related to THPS, such that $\big|\Pr_{5,4}[\mathsf{Win}] - \Pr_6[\mathsf{Win}]\big| \le \mathsf{Adv}^{smp}_{\mathsf{THPS}}(\ell)$.

D Super-Strong RKA secure SE from THPS

D.1 Super-Strong IND-$\mathcal{F}$-RK-CCA2 Security for SE

Let $\mathcal{F}$ be a class of functions from $\mathcal{K}_{\mathsf{SE}}$ to $\mathcal{K}_{\mathsf{SE}}$. The IND-$\mathcal{F}$-RK-CCA2 security notion for SE (cf. Definition 24) defined in [BPT12] allows the adversary to get a challenge ciphertext c^* through $\mathrm{LR}(f^*, m_0, m_1)$, which encrypts m_b under $\mathcal{F}$-related key $\mathsf{k}'^* = f^*(\mathsf{k})$. However, the decryption oracle $\textsc{Dec}(f, c)$ is a bit restricted: it prohibits decryption of the challenger ciphertext c^* under the corresponding $\mathcal{F}$-related key k'^*. In other words, if the adversary queries $\textsc{Dec}(f, c)$ such that $(f(\mathsf{k}), c) = (\mathsf{k}'^*, c^*)$, the decryption oracle does not work. Similar to the discussion of that for the strong IND-$\mathcal{F}$-RK-CCA2 security of PKE in Subsection 5.1, this restriction is by no means reasonable. The adversary does not own the key k, thus it might not even realize $(f(\mathsf{k}), c) = (\mathsf{k}'^*, c^*)$.

Here we relax the decryption restriction, and define an enhanced security notion for SE, namely *super-strong IND-$\mathcal{F}$-RK-CCA2 security*. That is, we allow the adversary to query $\textsc{Dec}(f, c)$ even if it has queried $\mathrm{LR}(f^*, m_0, m_1)$ such that $(f(\mathsf{k}), c) = (f^*(\mathsf{k}), c^*)$, as long as $(f, c) \neq (f^*, c^*)$.

Definition 25 (Super-Strong IND-$\mathcal{F}$-RK-CCA2 Security for SE). SE *is super-strong IND-$\mathcal{F}$-RK-CCA2 secure, if for any PPT adversary $\mathcal{A}$, the advantage* $\mathsf{Adv}^{sup\text{-}str\text{-}ind\text{-}rk\text{-}cca2}_{\mathsf{SE},\mathcal{F},\mathcal{A}}(\ell) := \big|\Pr[\mathsf{super\text{-}strong\text{-}IND\text{-}}\mathcal{F}\mathsf{\text{-}RK\text{-}CCA2}^{\mathcal{A}} \Rightarrow 1] - \frac{1}{2}\big|$ *is negligible in ℓ, where game* $\mathsf{super\text{-}strong\text{-}IND\text{-}}\mathcal{F}\mathsf{\text{-}RK\text{-}CCA2}$ *is specified in Fig. 15.*

D.2 The Construction

Let $\mathsf{PKE}[\mathsf{THPS}, \mathsf{AE}] = (\mathsf{PKE.Setup}, \mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ be the canonical PKE scheme in Fig. 8, with secret key space $\mathcal{SK}$, public key space $\mathcal{PK}$ and message space $\mathcal{M}$. It also associates with algorithms $\mathsf{PKE.SK}$ and $\mathsf{PKE.PK}$. The proposed SE scheme $\mathsf{SE}[\mathsf{THPS}, \mathsf{AE}] = (\mathsf{SE.Setup}, \mathsf{SE.Gen}, \mathsf{SE.Enc},$

Procedure INITIALIZE:	**Proc.** LR$(f^* \in \mathcal{F}, m_0, m_1)$:	**Procedure** ENC$(f \in \mathcal{F}, m)$:	**Procedure** DEC$(f \in \mathcal{F}, c)$:
$\mathsf{prm} \leftarrow_{\$} \mathsf{SE.Setup}(1^\ell)$. $\mathsf{k} \leftarrow_{\$} \mathsf{SE.Gen}(\mathsf{prm})$. $b \leftarrow_{\$} \{0,1\}$. Return prm.	// one query $\mathsf{k}'^* := f^*(\mathsf{k}) \in \mathcal{K}_{\mathsf{SE}}$. $c^* \leftarrow_{\$} \mathsf{SE.Enc}(\mathsf{k}'^*, m_b)$. $\mathcal{Q}_{\mathcal{ENC}} := \{(f^*, c^*)\}$. Return c^*.	$\mathsf{k}' := f(\mathsf{k}) \in \mathcal{K}_{\mathsf{SE}}$. $c \leftarrow_{\$} \mathsf{SE.Enc}(\mathsf{k}', m)$. Return c.	If $(f, c) \in \mathcal{Q}_{\mathcal{ENC}}$, Return $\perp$. $\mathsf{k}' := f(\mathsf{k}) \in \mathcal{K}_{\mathsf{SE}}$. Return $\mathsf{SE.Dec}(\mathsf{k}', c)$. **Procedure** FINALIZE$(b')$: Return $(b' = b)$.

Fig. 15. super-strong-IND-$\mathcal{F}$-RK-CCA2 security game for SE.

SE.Dec) with key space $\mathcal{K}_{\mathsf{SE}} := \mathcal{SK}$ and message space $\mathcal{M}$ is defined in a black-box manner by invoking the algorithms of PKE[THPS, AE], as shown in Fig. 16. The correctness of SE[THPS, AE] follows from the canonical property and the correctness of PKE[THPS, AE] directly.

$\mathsf{prm} \leftarrow_{\$} \mathsf{SE.Setup}(1^\ell)$:	$\mathsf{sk} \leftarrow_{\$} \mathsf{SE.Gen}(\mathsf{prm})$:	$\langle C, \chi \rangle \leftarrow_{\$} \mathsf{SE.Enc}(\mathsf{sk}, m)$:	$m/\perp \leftarrow \mathsf{SE.Dec}\big(\mathsf{sk}, \langle C, \chi \rangle\big)$:
$\mathsf{prm} \leftarrow_{\$} \mathsf{PKE.Setup}(1^\ell)$. Return prm.	$\mathsf{sk} \leftarrow_{\$} \mathsf{PKE.SK}(\mathsf{prm})$. Return sk.	$\mathsf{pk} := \mathsf{PKE.PK}(\mathsf{sk}) \in \mathcal{PK}$. $\langle C, \chi \rangle \leftarrow_{\$} \mathsf{PKE.Enc}(\mathsf{pk}, m)$. Return $\langle C, \chi \rangle$.	$m/\perp \leftarrow \mathsf{PKE.Dec}\big(\mathsf{sk}, \langle C, \chi \rangle\big)$. Return $m/\perp$.

Fig. 16. Construction of SE[THPS, AE]. Here PKE denotes the PKE[THPS, AE] in Fig. 8.

Theorem 7. *If the* PKE[THPS, AE] *in Fig. 8 is super-strong IND-$\mathcal{F}$-RK-CCA2 secure, then the* SE[THPS, AE] *in Fig. 16 is super-strong IND-$\mathcal{F}$-RK-CCA2 secure.*

Proof of Theorem 7. Suppose that $\mathcal{A}$ is a PPT adversary against the super-strong IND-$\mathcal{F}$-RK-CCA2 security of SE[THPS, AE]. We want to construct a PPT adversary $\mathcal{B}$ against the super-strong IND-$\mathcal{F}$-RK-CCA2 security of PKE[THPS, AE]. The security reduction is quite straightforward. $\mathcal{B}$ has access to oracles INITIALIZE$_{\mathsf{PKE}}$, LR$_{\mathsf{PKE}}$, ENC$_{\mathsf{PKE}}$ and DEC$_{\mathsf{PKE}}$ in the super-strong-IND-$\mathcal{F}$-RK-CCA2 game of PKE[THPS, AE] (cf. Fig. 7), and $\mathcal{B}$ wants to simulate the oracles INITIALIZE, LR, ENC and DEC in the super-strong-IND-$\mathcal{F}$-RK-CCA2 game of SE[THPS, AE] (cf. Fig. 15) for $\mathcal{A}$.

For INITIALIZE, $\mathcal{B}$ invokes its own INITIALIZE$_{\mathsf{PKE}}$ oracle and gets $(\mathsf{prm}, \mathsf{pk})$. $\mathcal{B}$ discards pk and returns prm to $\mathcal{A}$. Note that $\mathcal{B}$ does not have the secret key sk. To simulate LR(f^*, m_0, m_1), $\mathcal{B}$ queries its own LR$_{\mathsf{PKE}}$ oracle with (f^*, m_0, m_1), gets $\langle C^*, \chi^* \rangle$ and simply returns $\langle C^*, \chi^* \rangle$ to $\mathcal{A}$. To simulate ENC(f, m), $\mathcal{B}$ queries its own ENC$_{\mathsf{PKE}}$ oracle with (f, m), gets $\langle C, \chi \rangle$ and replies $\mathcal{A}$ with $\langle C, \chi \rangle$. To simulate DEC$\big(f, \langle C, \chi \rangle\big)$, $\mathcal{B}$ queries its own DEC$_{\mathsf{PKE}}$ oracle with $\big(f, \langle C, \chi \rangle\big)$, gets $m/\perp$ and replies $\mathcal{A}$ with $m/\perp$. Finally, $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs.

It is easy to check that $\mathcal{B}$ simulates the super-strong-IND-$\mathcal{F}$-RK-CCA2 game perfectly with $\mathcal{A}$, and $\mathcal{B}$ succeeds as long as $\mathcal{A}$ succeeds. Therefore, we have that

$$\mathsf{Adv}^{sup\text{-}str\text{-}ind\text{-}rk\text{-}cca2}_{\mathsf{SE[THPS,AE]},\mathcal{F},\mathcal{A}}(\ell) = \mathsf{Adv}^{sup\text{-}str\text{-}ind\text{-}rk\text{-}cca2}_{\mathsf{PKE[THPS,AE]},\mathcal{F},\mathcal{B}}(\ell),$$

and the super-strong IND-$\mathcal{F}$-RK-CCA2 security of SE[THPS, AE] follows. ▌

By combining Theorem 2 in Subsection 5.2 with Theroem 7, we immediately obtain Corollary 1 shown in Subsection 5.3.

Contents