Published in *Designs, Codes and Cryptography* **60**(1):15–35, 2011.

Notions and Relations for RKA-Secure Permutation and Function Families

Jongsung Kim · Jaechul Sung · Ermaliza Razali · Raphael C.-W. Phan · Marc Joye

Abstract The theory of designing block ciphers is mature, having seen significant progress since the early 1990s for over two decades, especially during the AES development effort. Nevertheless, interesting directions exist, in particular in the study of the provable security of block ciphers along similar veins as public-key primitives, i.e. the notion of pseudorandomness (PRP) and indistinguishability (IND). Furthermore, recent cryptanalytic progress has shown that block ciphers well designed against known cryptanalysis techniques including related-key attacks (RKA) may turn out to be less secure against related-key attacks than expected. The notion of provable security of block ciphers against related-key attacks was initiated by Bellare and Kohno, and subsequently treated by Lucks. Concrete block cipher constructions were proposed therein with provable security guarantees. In this paper, we are interested in the security notions for RKA-secure block ciphers.

This work was supported by Kyungnam University Foundation Grant, 2010.

Work done while the fourth author was with the Laboratoire de sécurité et de cryptographie (LASEC), EPFL, Switzerland.

Jongsung Kim
Division of e-Business, Kyungnam University, 449 Wolyoung-dong, Masan, Kyungnam, Korea
E-mail: jongsung.k@gmail.com

Jaechul Sung (Corresponding Author)
Department of Mathematics, University of Seoul, Cheonnong-Dong, Dongdaemun-Gu, Seoul, Korea
E-mail: jcsung@uos.ac.kr

Ermaliza Razali
Information Security Research (iSECURES) Lab, Swinburne University of Technology, Sarawak campus, Malaysia
E-mail: erazali@swinburne.edu.my

Raphael C.-W. Phan
Electronic & Electrical Engineering, Loughborough University, United Kingdom
E-mail: r.phan@lboro.ac.uk

Marc Joye
Technicolor, Security & Content Protection Labs, 1 avenue de Belle Fontaine, 35576 Cesson-Sévigné Cedex, France
E-mail: marc.joye@technicolor.com

In the first part of the paper, we show that secure tweakable permutation families in the sense of strong pseudorandom permutation (SPRP) can be transformed into secure permutation families in the sense of SPRP against some classes of related-key attacks (SPRP-RKA). This fact allows us to construct a secure SPRP-RKA cipher which is faster than the Bellare-Kohno PRP-RKA cipher. We also show that function families of a certain form secure in the sense of a pseudorandom function (PRF) can be transformed into secure permutation families in the sense of PRP against some classes of related-key attacks (PRP-RKA). We can exploit it to get various constructions secure against some classes of related-key attacks from known MAC algorithms. Furthermore, we discuss how the key recovery (KR) security of the Bellare-Kohno PRP-RKA, the Lucks PRP-RKA and our SPRP-RKA ciphers relates to existing types of attacks on block ciphers like meet-in-the-middle and slide attacks.

In the second part of the paper, we define other security notions for RKA-secure block ciphers, namely in the sense of *indistinguishability* and *non-malleability*, and show the relations between these security notions. In particular, we show that secure tweakable permutation families in the sense of indistinguishability (resp. non-malleability) can be transformed into RKA-secure permutation families in the sense of indistinguishability (resp. non-malleability).

Keywords Pseudorandom · Related-Key Attacks · PRP · SPRP-RKA
Mathematics Subject Classification (2000) 94A60

1 Introduction

The design and analysis of block ciphers is an established field of study which has seen significant progress especially for the past 2 decades. While numerous cryptanalytic results and techniques have been discovered, what remains on an interesting direction to explore is the theoretical study of provable security for block ciphers. Some work in this direction includes those initiated by Luby and Rackoff [28] which treated the pseudorandomness of Feistel cipher constructions, and by Vaudenay [36] which considered some form of provable security against known types of block cipher attacks like differential and linear cryptanalysis.

In 1992 and 1993, Knudsen [25] and Biham [4] independently introduced a cryptanalytic technique which exploits related keys in a differential attack. This so-called *related-key attack* (RKA) has widely been used to evaluate the security of block ciphers [4, 18–20, 26]. The related-key differential attack has also been extended into various cryptanalytic techniques such as a related-key differential-linear attack [15], a related-key impossible differential attack [18], a related-key boomerang and rectangle attacks [5, 22]. Related-key attacks are well-known to be powerful tools to analyze block ciphers: up to now, the best known attacks (in terms of the number of attacked rounds) against AES [24], KASUMI [6], IDEA [7], SHACAL-1 [8] and GOST [26] are all related-key attacks. Furthermore, related-key attacks can be used to evaluate the security of message authentication codes and block cipher based enciphering modes (refer to [3] for an example).

Related-key attacks allow an adversary to obtain plaintext and ciphertext pairs by using different but related keys which are unknown to the adversary. Such attacks are commonly exploited to mount a key-recovery attack on the block cipher, i.e. retrieve some or all portions of the related keys by using collected plaintext and ciphertext pairs;

the success or failure of these attacks is determined by whether or not the adversary can distinguish the underlying cipher from a random permutation family with the same key space and plaintext/ciphertext space as those of the underlying cipher (sometimes we refer to a permutation family as *a cipher*). Hence, from a theoretical point of view, the distinguishing ability of the most powerful related-key adversary determines the security of the underlying cipher against related-key attacks. More precisely, if a cipher E (resp. E, E^{-1}) and a randomly chosen permutation family G (resp. G, G^{-1}) are indistinguishable under related-key attack models, we then say that E is secure in the sense of a pseudorandom permutation (PRP) (resp. a strong pseudorandom permutation (SPRP)) against related-key attacks (RKA); simply, we say that E is a secure PRP-RKA (resp. SPRP-RKA) cipher.

Compared to cryptanalytic results on related-key attacks there are few theoretical results on them. In 2003, Bellare and Kohno [3] first initiated a theoretical investigation of security against related-key attacks. They defined a general model of related-key attacks, i.e., classes of related-key attacks which are specified by an associated set of key transformations, together with some security notions for these attacks including PRP-RKA, SPRP-RKA and PRF-RKA. They also clarified what classes of these attacks do or do not allow to achieve security against them (note that for any normal ciphers there exist classes of related-key attacks against which they are always insecure: for instance, if a ciphertext generated from a plaintext P and a key K is equal to that generated from the same plaintext and its related key $K' = K|a$ where a is a bit-string whose bits are all 0 except for the i-th position and $|$ is the bitwise-or, then the i-th bit of the key should be 1 with a high probability [3] – if the i-th bit of the key K is 0, then $K \neq K'$). They also gave a construction of secure PRP-RKA cipher. In [29] Lucks proposed another construction of secure PRP-RKA cipher that has a better security bound than that of [3].

The first goal of this paper is to construct various provably secure ciphers against some classes of related-key attacks from constructions which are already known to be provably secure. The second goal of this paper is to study how existing block-cipher cryptanalysis techniques relate to the key recovery (KR) security of these concrete PRP-RKA secure ciphers. The third goal of the paper is to define various security notions of RKA-secure block ciphers and to show the relationships among these security notions.

In this paper, more precisely, we show that secure tweakable permutation families in the sense of SPRP can be transformed into secure permutation families in the sense of SPRP-RKA (with respect to some classes of related-key attacks); and furthermore that secure function families of a certain form in the sense of PRF can be transformed into secure permutation families in the sense of PRP-RKA (with respect to some classes of related-key attacks). This enables us to construct various SPRP-RKA or PRP-RKA ciphers from known design methods. We then discuss how[1] the KR security of the Bellare-Kohno PRP-RKA, the Lucks PRP-RKA and our SPRP-RKA ciphers relates to existing types of attacks on block ciphers, e.g., meet-in-the-middles and slide attacks. Furthermore, we define other security notions for related-key attacks, *indistinguishability* and *non-malleability*, and look into the relations between these RKA security notions. At the end of this paper, we show that secure tweakable permutation families in the sense of indistinguishability (resp. non-malleability) can be transformed to secure permutation families in the sense of indistinguishability (resp. non-malleability) against some classes of related-key attacks.

[1] An extended abstract of this latter work appeared in [35].

This paper is organized as follows: Section 2 provides some notation and security notions for related-key attacks and key recovery attacks. In Section 3 and Section 4, we observe that various secure permutation families against some classes of related-key attacks can be constructed from schemes which are already known to be secure in the sense of PRF. Section 5 describes several key recovery attacks on existing PRP-RKA secure ciphers and relates the corresponding success probability with the security bound derived from a generic attacker. Section 6 defines various security notions for related-key attacks and shows the relationships among these security notions and Section 7 concludes the paper.

2 Preliminaries

In this section, we present some notation and definitions of security notions which are used throughout the paper. We adopt the notation of [3].

2.1 Notation

- $s \xleftarrow{\$} \mathcal{S}$: the operation of selecting s uniformly at random from the set $\mathcal{S}$
- $F : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$: a family of functions from $\mathcal{D}$ to $\mathcal{R}$ indexed by keys $\mathcal{K}$, i.e., $F_K(\cdot)$ is a function from $\mathcal{D}$ to $\mathcal{R}$ for each key $K \in \mathcal{K}$
- $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$: a family of permutations on $\mathcal{D}$ indexed by $\mathcal{K}$, i.e., $E_K(\cdot)$ is a permutation on $\mathcal{D}$ for each key $K \in \mathcal{K}$
- $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{D} \to \mathcal{D}$: a family of permutations on $\mathcal{D}$ indexed by $\mathcal{K} \times \mathcal{T}$, i.e., $\tilde{E}_K(T, \cdot)$ is a permutation on $\mathcal{D}$ for each key $K \in \mathcal{K}$ and tweak $T \in \mathcal{T}$ (note that T is an independent second input which is public information rather than a nonce or initialization vector, but the intent is similar [27].)
- $\mathrm{Perm}(\mathcal{D})$: the set of all permutations on $\mathcal{D}$
- $\mathrm{Perm}(\mathcal{K}, \mathcal{D})$: the set of all families of permutations with domain $\mathcal{D}$ and keys $\mathcal{K}$
- $\mathrm{Rand}(\mathcal{D}, \mathcal{R})$: the set of all functions from $\mathcal{D}$ to $\mathcal{R}$
- $\mathrm{Rand}(\mathcal{K}, \mathcal{D}, \mathcal{R})$: the set of all families of functions with domain $\mathcal{D}$, range $\mathcal{R}$ and keys $\mathcal{K}$

In this paper, we call F a function family. We also call E and $\tilde{E}$ a permutation family and a tweakable permutation family, respectively. According to the above notation, $G \xleftarrow{\$} \mathrm{Perm}(\mathcal{K}, \mathcal{D})$ represents the selection of a random permutation family, i.e., for each key $K \in \mathcal{K}$, $G_K(\cdot)$ is a permutation randomly chosen from $\mathrm{Perm}(\mathcal{D})$. Furthermore, $G \xleftarrow{\$} \mathrm{Rand}(\mathcal{K}, \mathcal{D}, \mathcal{R})$ represents the selection of a random function family, i.e., for each key $K \in \mathcal{K}$, $G_K(\cdot)$ is a function randomly chosen from $\mathrm{Rand}(\mathcal{D}, \mathcal{R})$.

2.2 Definitions of Security Notions

Many security notions have been introduced for function and permutation families; in these notions, an adversary $\mathcal{A}$ can black-box access to one or more oracle(s). While the computational power of $\mathcal{A}$ is unlimited, the total number of oracle calls is limited to a certain number. For each query of $\mathcal{A}$ the oracle gives an answer to $\mathcal{A}$. After making a limited number of queries to the oracle(s) adaptively, $\mathcal{A}$ outputs a bit. Sections 3,

4 and 5 consider the following security notions in the sense of pseudorandomness and key-recovery. Some other security notions will be introduced in Section 6 in the sense of indistinguishability and non-malleability. In this paper, for any adversary $\mathcal{A}$, we say the advantage is negligible if it vanishes faster than the inverse of any polynomial [2].

Definition 1 (PRF) [2] Let $F : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ be a function family and $\mathcal{A}$ be an adversary. Then the prf-advantage of $\mathcal{A}$ is defined by

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) = \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{F_K(\cdot)} = 1] - \Pr[g \xleftarrow{\$} \mathrm{Rand}(\mathcal{D}, \mathcal{R}) : \mathcal{A}^{g(\cdot)} = 1].$$

$\mathcal{A}^{\mathcal{O}(\cdot)}$ means $\mathcal{A}$ with an oracle $\mathcal{O}(\cdot)$, which returns $\mathcal{O}(M)$ for the adversary's query M. Thus F is a secure PRF if $\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{A})$ is negligible for any $\mathcal{A}$.

Definition 2 (SPRP) [31] Let $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ be a permutation family and $\mathcal{A}$ be an adversary. Then the sprp-advantage of A is defined by

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) = \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_K(\cdot), E_K^{-1}(\cdot)} = 1] - \Pr[g \xleftarrow{\$} \mathrm{Perm}(\mathcal{D}) : \mathcal{A}^{g(\cdot), g^{-1}(\cdot)} = 1].$$

$\mathcal{A}^{\mathcal{O}(\cdot), \mathcal{O}^{-1}(\cdot)}$ means $\mathcal{A}$ with two oracles $\mathcal{O}(\cdot), \mathcal{O}^{-1}(\cdot)$; for an adversary's query of M (resp. C) to the first (resp. second) oracle it returns $\mathcal{O}(M)$ (resp. $\mathcal{O}^{-1}(C)$). Thus E is a secure SPRP if $\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A})$ is negligible for any $\mathcal{A}$.

Definition 3 (TWEAK-SPRP) [13] Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{D} \to \mathcal{D}$ be a tweakable permutation family and $\mathcal{A}$ be an adversary. Then the tweak-sprp-advantage of $\mathcal{A}$ is defined by

$$\begin{aligned}\mathbf{Adv}_{\tilde{E}}^{\text{tweak-sprp}}(\mathcal{A}) = \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\tilde{E}_K(\cdot,\cdot), \tilde{E}_K^{-1}(\cdot,\cdot)} = 1] \\ - \Pr[\tilde{G} \xleftarrow{\$} \mathrm{Perm}(\mathcal{T}, \mathcal{D}) : \mathcal{A}^{\tilde{G}(\cdot,\cdot), \tilde{G}^{-1}(\cdot,\cdot)} = 1].\end{aligned}$$

$\mathcal{A}^{\tilde{\mathcal{O}}(\cdot,\cdot), \tilde{\mathcal{O}}^{-1}(\cdot,\cdot)}$ means $\mathcal{A}$ with two oracles $\tilde{\mathcal{O}}(\cdot,\cdot), \tilde{\mathcal{O}}^{-1}(\cdot,\cdot)$; for an adversary's query of (T, M) (resp. (T, C)) to the first (resp. second) oracle it returns $\tilde{\mathcal{O}}(T, M)$ (resp. $\tilde{\mathcal{O}}^{-1}(T, C)$). Thus $\tilde{E}$ is a secure TWEAK-SPRP if $\mathbf{Adv}_{\tilde{E}}^{\mathrm{tweak-sprp}}(\mathcal{A})$ is negligible for any $\mathcal{A}$.

Definition 4 (SPRP-RKA) [3] Let $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ be a permutation family and Φ be a set of functions over $\mathcal{K}$. Let $\mathcal{A}$ be an adversary that is restricted to queries of the form (ϕ, x) in which $\phi \in \Phi$ and $x \in \mathcal{D}$. Then the sprp-rka advantage of $\mathcal{A}$ is defined by

$$\begin{aligned}\mathbf{Adv}_{\Phi,E}^{\text{sprp-rka}}(\mathcal{A}) = \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_{RK(\cdot,K)}(\cdot), E_{RK(\cdot,K)}^{-1}(\cdot)} = 1] \\ -\Pr[K \xleftarrow{\$} \mathcal{K}; G \xleftarrow{\$} \mathrm{Perm}(\mathcal{K}, \mathcal{D}) : \mathcal{A}^{G_{RK(\cdot,K)}(\cdot), G_{RK(\cdot,K)}^{-1}(\cdot)} = 1].\end{aligned}$$

$\mathcal{A}^{\mathcal{O}_{RK(\cdot)}(\cdot), \mathcal{O}_{RK(\cdot)}^{-1}(\cdot)}$ means $\mathcal{A}$ with two oracles $\mathcal{O}_{RK(\cdot)}(\cdot), \mathcal{O}_{RK(\cdot)}^{-1}(\cdot)$; for an adversary's query of (ϕ, M) (resp. (ϕ, C)) to the first (resp. second) oracle it returns $\mathcal{O}_{\phi(K)}(M)$ (resp. $\mathcal{O}_{\phi(K)}^{-1}(C)$).[2] Thus E is a secure SPRP-RKA if $\mathbf{Adv}_{\Phi,E}^{\text{sprp-rka}}(\mathcal{A})$ is negligible for any $\mathcal{A}$.

[2] Note that $RK(\cdot, K)$ has a single parameter which is for the query ϕ where $\phi \in \Phi$ (it follows that a related key $\phi(K)$ is applied in $E_{RK(\cdot,K)}(\cdot)$, i.e., $E_{\phi(K)}(\cdot)$).

The PRP, TWEAK-PRP and PRP-RKA security notions are defined by removing the decryption oracle in Definitions 2, 3 and 4, respectively.

For security against key recovery, a KR adversary $\mathcal{A}$ is given a list $\mathcal{L}$ of p pairs of plaintext/ciphertext

$$\mathcal{L} = \{\langle P_1, C_1\rangle, \ldots, \langle P_p, C_p\rangle\}$$

where $C_i = E_K(P_i)$ for $1 \leq i \leq p$. Depending on the assumed adversarial ability, the list $\mathcal{L}$ could be known plaintext/ciphertext or chosen plaintext/ciphertext pairs, where in the latter kind, the plaintexts in $\mathcal{L}$ are chosen to have specific differences between them [9]. $\mathcal{L}$ is typically formed by an oracle implementing $E_K(\cdot)$ taking plaintexts as input and outputting the corresponding ciphertexts.

The goal of $\mathcal{A}$ is to find a key $\hat{K}$ that is *consistent* with $\mathcal{L}$, that is, a key such that, for all $\langle P_i, C_i\rangle \in \mathcal{L}$, $E_{\hat{K}}(P_i) = C_i$.

Definition 5 (KR) [16] Let $\mathrm{Cons}_E(\mathcal{L})$ denote the set of all keys consistent with $\mathcal{L}$, where $\mathcal{L}$ as previously defined above is a list of p pairs of plaintext/ciphertext accessible to the adversary. The advantage of KR adversary $\mathcal{A}$ is then given by:

$$\mathbf{Adv}^{\mathrm{kr}}_E(\mathcal{A}) = \Pr\left[K \xleftarrow{\$} \mathcal{K}; \mathcal{L} \leftarrow \{\langle P_i, E_K(P_i)\rangle\} : \mathcal{A}^{\mathcal{L}} = \hat{K} \in \mathrm{Cons}_E(\mathcal{L})\right] .$$

E is KR-secure if $\mathbf{Adv}^{\mathrm{kr}}_E(\mathcal{A})$ is negligible for any $\mathcal{A}$.

This can be extended to include RKA [38]:

$$\mathbf{Adv}^{\text{kr-rka}}_{\Phi,E}(\mathcal{A}) = \Pr\Big[K \xleftarrow{\$} \mathcal{K}; \mathcal{L} \leftarrow \{\langle P_i, E_K(P_i)\rangle\} : \mathcal{A}^{\mathcal{L}, E_{RK(\cdot,K)}(\cdot)} = \hat{K} \in \mathrm{Cons}_E(\mathcal{L})\Big] .$$

3 Construction of Secure SPRP-RKA Families from Secure Tweakable SPRP Families

Bellare and Kohno propose a construction method of secure PRP-RKA family (Proposition 9.1 of [3]). In their security proof there are two ways to complete it: one is a direct proof which was concretely described in [3], and the other one is an indirect proof, i.e., it is based on the relationship between tweakable PRP families and PRP-RKA families (the second proof was sketched in [3]). In a formal statement, we can naturally extend this proof sketch into the SPRP security notion.

Theorem 1 (TWEAK-SPRP→SPRP-RKA) *Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{D} \to \mathcal{D}$ be a tweakable permutation family and let $E : \mathcal{K} \times \mathcal{T} \times \mathcal{D} \to \mathcal{D}$ be a permutation family defined as $E_{K||T}(M) = \tilde{E}_K(T, M)$ where K is a secret key in $\mathcal{K}$, T is either a tweak value in $\mathcal{T}$ of $\tilde{E}$ or a secret key in $\mathcal{T}$ of E, and M is a message in $\mathcal{D}$. If $\tilde{E}$ is a secure tweakable SPRP, then E is a secure SPRP with respect to Φ-restricted RKAs[3] if each function ϕ in Φ is a partial transformation[4] for which there exists a function $\phi' : \mathcal{T} \to \mathcal{T}$ such*

[3] Φ-restricted RKAs are defined as related-key attacks which perform under the restriction Φ when choosing a related key.

[4] A partial transformation is to transform some part of instances while the rest part remains unchanged.

that $\phi(K,T) = (K, \phi'(T))$. Formally, given an SPRP-RKA adversary $\mathcal{A}$ attacking E, we can construct a TWEAK-SPRP adversary $\mathcal{B}_\mathcal{A}$ attacking $\tilde{E}$ such that

$$\mathbf{Adv}^{\text{sprp-rka}}_{\Phi,E}(\mathcal{A}) \leq \mathbf{Adv}^{\text{tweak-sprp}}_{\tilde{E}}(\mathcal{B}_\mathcal{A})$$

and $\mathcal{B}_\mathcal{A}$ takes the same amount of time and makes the same number of oracle queries as $\mathcal{A}$.

Using the above Theorem 1 and Theorem 2 of [27] (an excerpt of this is given in Appendix A), we can construct a secure SPRP-RKA family. See Proposition 1 for the details, where a set $\mathcal{H}$ of functions with domain $\mathcal{T}$ and range $\mathcal{D}$ is said to be ϵ-almost 2-xor universal (ϵ-AXU_2) if $Pr_h[h(x) \oplus h(y) = z] \leq \epsilon$ for all x, y, z [27].

Proposition 1 (An SPRP-RKA Construction) *Let $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ be a permutation family, let $\mathcal{H} : \mathcal{T} \to \mathcal{D}$ be an ϵ-AXU_2 family with $\epsilon \geq 1/|\mathcal{D}|$ and let $E' : (\mathcal{K} \times \mathcal{T} \times \mathcal{H}) \times \mathcal{D} \to \mathcal{D}$ be another permutation family defined as $E'_{K,T,h}(M) = E_K(M \oplus h(T)) \oplus h(T)$ where (K,T,h) is a secret key in $\mathcal{K} \times \mathcal{T} \times \mathcal{H}$, and M is a message in $\mathcal{D}$. If E is a secure SPRP and $\mathcal{H}$ is ϵ-AXU_2 where ϵ is negligible, then E' is a secure SPRP with respect to Φ-restricted RKAs when each function ϕ in Φ is a partial transformation for which there exists a function $\phi' : \mathcal{T} \to \mathcal{T}$ such that $\phi(K,T,h) = (K, \phi'(T), h)$. Formally, given an SPRP-RKA adversary $\mathcal{A}$ attacking E' that queries its oracles with at most q queries, we can construct an SPRP adversary $\mathcal{B}_\mathcal{A}$ attacking E such that*

$$\mathbf{Adv}^{\text{sprp-rka}}_{\Phi,E'}(\mathcal{A}) \leq \mathbf{Adv}^{\text{sprp}}_{E}(\mathcal{B}_\mathcal{A}) + 3\epsilon q^2$$

and $\mathcal{B}_\mathcal{A}$ takes the same amount of time and makes the same number of oracle queries as $\mathcal{A}$.

Note that the ϵ-AXU_2 family $\mathcal{H}$ and its domain $\mathcal{T}$ are parts of the key space of E'. A practical impact of Proposition 1 is that if one does not want to lose much time for rekeying, then the rekeying process can apply T to generate its related key T' without a loss of security for the cipher. Figure 1 compares the construction of Proposition 1 (which we denote here as Construction C) with the previous ones. Constructions A (the Bellare-Kohno cipher) and B (the Lucks cipher) call the underlying ciphers twice, while Construction C requires a single call to the underlying cipher and another single call to the h function which is normally faster than the underlying cipher. Note that Constructions B and C can store the key generation parts $E_{K_1}(K_2)$ and $h(T)$ respectively before the message M is applied, and thus until these key generation parts are refreshed with other keys, they both require a single call to the underlying cipher. As the h function is normally faster than the E cipher, Construction C is expected to be not slower than the both of Constructions B and C. See Sect. 5 for the concrete RKA security bounds of Constructions A and B.

Theorem 1 can be also exploited to construct various RKA-secure permutation families from tweakable enciphering modes which are already known to be secure. The security of tweakable enciphering modes CMC [13], EME [14], EME* [12] is based on the security of the underlying block ciphers. In CMC, EME, EME*, if the tweaks of CMC, EME, EME* are modified into parts of keys, then the modified enciphering modes with fixed-length messages, i.e., the modified permutation families are secure against any Φ-restricted related-key attack under the assumption that the underlying block ciphers are secure and the functions of Φ only transform the modified key portions.

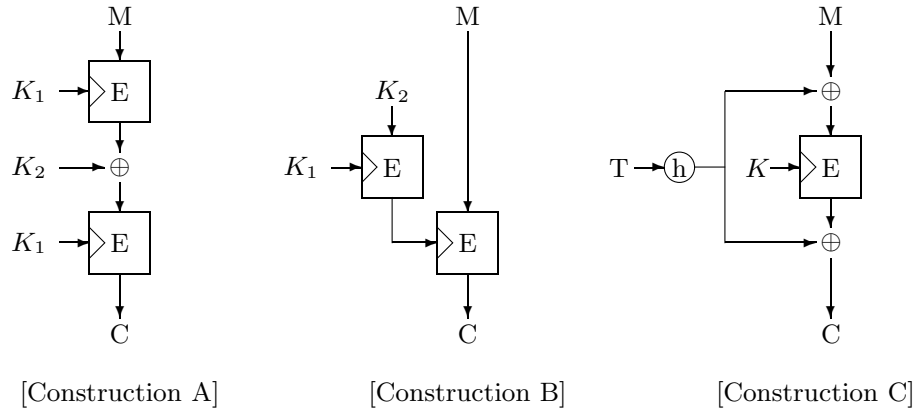

Fig. 1 Comparison of the construction (C) of Proposition 1 and the previous ones (A, B)

In Section 5, we will discuss how known types of attacks can apply and relate to the key-recovery security bounds for Constructions A, B and C.

4 Construction of Secure PRP-RKA Families from Secure PRF Families of a Certain Form

This section shows that secure PRF families of a certain form can be transformed into secure PRP-RKA families. Before showing it, we give a more rigorous bound of the PRF-RKA/PRP-RKA switching Proposition 8.9 in [3].

Lemma 1 (PRF-RKA/PRP-RKA Switching) *Let $\mathcal{A}$ be a related-key adversary that queries its oracle with at most r different key transformations from fixed Φ and at most q times per transformation. Then*

$$|\Pr[\ K \xleftarrow{\$} \mathcal{K}, G \xleftarrow{\$} \mathit{Rand}(\mathcal{K},\mathcal{D},\mathcal{D}) : \mathcal{A}^{G_{RK(\cdot,K)}(\cdot)} = 1] - \Pr[K \xleftarrow{\$} \mathcal{K}, G' \xleftarrow{\$} \mathit{Perm}(\mathcal{K},\mathcal{D}) : \mathcal{A}^{G'_{RK(\cdot,K)}(\cdot)} = 1]| \leq \frac{r \cdot q \cdot (q \cdot \mathit{min}\{r, NM_\Phi\} - 1)}{2 \cdot |D|}$$

where $NM_\Phi = max_{K,K' \in \mathcal{K}}\{|\{\phi \in \Phi : \phi(K) = K'\}|\}$.

Proof From Proposition 8.9 in [3] we know that

$$|\Pr[\ K \xleftarrow{\$} \mathcal{K}, G \xleftarrow{\$} \mathrm{Rand}(\mathcal{K},\mathcal{D},\mathcal{D}) : \mathcal{A}^{G_{RK(\cdot,K)}(\cdot)} = 1] - \Pr[K \xleftarrow{\$} \mathcal{K}, G' \xleftarrow{\$} \mathrm{Perm}(\mathcal{K},\mathcal{D}) : \mathcal{A}^{G'_{RK(\cdot,K)}(\cdot)} = 1]| \leq \Pr_g[\overline{D}]\,,$$

where $\Pr_g[\cdot]$ represents the probability in the experiment $K \xleftarrow{\$} \mathcal{K}, G \xleftarrow{\$} \mathrm{Rand}(\mathcal{K}, \mathcal{D}, \mathcal{D}), \mathcal{A}^{G_{RK(\cdot,K)}(\cdot)}$, where $g \xleftarrow{\$} G$, and g is the probability variable. Let D represent the event that, for each related-key that $\mathcal{A}$ accesses to its oracle (i.e., $\phi(K)$ where $\mathcal{A}$ queries (ϕ, M) to its oracle), there are no collisions in the responses of the oracle for different messages. In [3], Bellare and Kohno showed that $\Pr_g[\overline{D}] \leq \frac{r \cdot q \cdot NM_\Phi \cdot (q \cdot NM_\Phi - 1)}{2 \cdot |D|}$. However, we can give a more rigorous bound for $\Pr_g[\overline{D}]$.

Let $\phi_1, \phi_2, \cdots, \phi_{r'}$, $(r' \leq r)$ be transformations in Φ that $\mathcal{A}$ queries. Without loss of generality, we assume that $\phi_1(K) = \cdots = \phi_{a_1}(K) = K_1$, $\phi_{a_1+1}(K) = \cdots = \phi_{a_1+a_2}(K) = K_2, \cdots, \phi_{a_1+\cdots+a_{m-1}+1}(K) = \cdots = \phi_{a_1+\cdots+a_{m-1}+a_m}(K) = K_m$ where $a_1 + \cdots + a_{m-1} + a_m = r'$ and $K_j \neq K_{j'}$ for $1 \leq j < j' \leq m$. Since $\mathcal{A}$ queries at most q times per key transformation, for each K_i the probability of a collision in the output of the oracle on distinct inputs is at most $\frac{a_i \cdot q \cdot (a_i \cdot q - 1)}{2 \cdot |\mathcal{D}|}$ (this bound follows from Proposition A.1 in [2]). Furthermore, each a_i is at most $min\{r', NM_\Phi\}$. Thus $\Pr_g[\overline{D}]$ is bounded as follows.

$$\begin{aligned}\Pr_g[\overline{D}] &\leq \sum_{i=1}^{m} \frac{a_i \cdot q \cdot (a_i \cdot q - 1)}{2 \cdot |\mathcal{D}|} \leq \sum_{i=1}^{m} \frac{a_i \cdot q \cdot (q \cdot min\{r', NM_\Phi\} - 1)}{2 \cdot |\mathcal{D}|} \\ &\leq \frac{r \cdot q \cdot (q \cdot min\{r, NM_\Phi\} - 1)}{2 \cdot |\mathcal{D}|}. \qquad \square\end{aligned}$$

Note that Lemma 1 improves the bound of Bellare and Kohno's PRF-RKA/PRP-RKA switching proposition by a factor of approximately NM_Φ. Using Lemma 1 we can easily show Theorem 2.

Theorem 2 (PRF→PRP-RKA) *let $E : \mathcal{K}_1 \times \mathcal{K}_2 \times \mathcal{D} \to \mathcal{D}$ be a permutation family on $\mathcal{D}$ and let $F : \mathcal{K}_1 \times \mathcal{K}_2 \times \mathcal{D} \to \mathcal{D}$ be a function family defined as $F_{K_1}(K_2||M) = E_{K_1||K_2}(M)$ where K_1 is a secret key in $\mathcal{K}_1$, K_2 is either a secret key in $\mathcal{K}_2$ of E or a message in $\mathcal{K}_2$ of F, and M is a message in $\mathcal{D}$. If F is a secure PRF, then E is a secure PRP with respect to $\Phi-$restricted RKAs if each function ϕ in Φ is a partial transformation for which there exists a function $\phi' : \mathcal{K}_2 \to \mathcal{K}_2$ such that $\phi(K_1, K_2) = (K_1, \phi'(K_2))$. Formally, given a PRP-RKA adversary $\mathcal{A}$ attacking E that queries its oracle with at most r different key transformations and at most q queries per transformation, we can construct a PRF adversary $\mathcal{B}_\mathcal{A}$ attacking F such that*

$$\mathbf{Adv}^{\text{prp-rka}}_{\Phi,E}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prf}}_{F}(\mathcal{B}_\mathcal{A}) + \frac{r \cdot q \cdot (q \cdot min\{r, NM_\Phi\} - 1)}{2 \cdot |\mathcal{D}|}$$

and $\mathcal{B}_\mathcal{A}$ takes the same amount of time and makes the same number of oracle queries as $\mathcal{A}$.

Proof Let $\mathcal{B}_\mathcal{A}$ be the F adversary that works as follows.

<Adversary $\mathcal{B}_\mathcal{A}^{\mathcal{O}(\cdot)}$>

1. Select K_2 at random from $\mathcal{K}_2$.
2. Obtain $\mathcal{A}$'s request $(\phi(= (id, \phi')), M)$ by running $\mathcal{A}$.
3. Return $\mathcal{O}(\phi'(K_2)||M)$ to $\mathcal{A}$.
4. If $\mathcal{A}$ outputs b, then output b. Otherwise, go to Step 2.

When $\mathcal{B}_\mathcal{A}$ is given access to F, $\mathcal{A}$ computes E with related keys. So the following equality holds:

$$\begin{aligned}&\Pr\left[K_1 \xleftarrow{\$} \mathcal{K}_1 : \mathcal{B}_\mathcal{A}^{F_{K_1}(\cdot)} = 1\right] = \\ &\Pr\left[(K_1, K_2) \xleftarrow{\$} \mathcal{K}_1 \times \mathcal{K}_2 : \mathcal{A}^{E_{RK(\cdot,(K_1,K_2))}(\cdot)} = 1\right].\end{aligned}$$

When $\mathcal{B}_{\mathcal{A}}$ is given access to G where G is randomly chosen from $\mathrm{Rand}(\mathcal{K}_2 \times \mathcal{D}, \mathcal{D})$, $\mathcal{B}_{\mathcal{A}}$ replies to $\mathcal{A}$ using an independently selected random function on $\mathcal{D}$ for each $\phi'(K_2)$. So the equation

$$\Pr\left[G \xleftarrow{\$} \mathrm{Rand}(\mathcal{K}_2 \times \mathcal{D}, \mathcal{D}) : \mathcal{B}_{\mathcal{A}}^{G(\cdot)} = 1\right] =$$
$$\Pr\left[(K_1, K_2) \xleftarrow{\$} \mathcal{K}_1 \times \mathcal{K}_2, G \xleftarrow{\$} \mathrm{Rand}(\mathcal{K}_1 \times \mathcal{K}_2, \mathcal{D}, \mathcal{D}) : \mathcal{A}^{G_{RK(\cdot,(K_1,K_2))}(\cdot)} = 1\right]$$

holds. Therefore, by using the above two equations and Lemma 1,

$$\begin{aligned}
\mathbf{Adv}^{\text{prp-rka}}_{\Phi,E}(\mathcal{A}) &= \Pr[(K_1, K_2) \xleftarrow{\$} \mathcal{K}_1 \times \mathcal{K}_2 : \mathcal{A}^{E_{RK(\cdot,(K_1,K_2))}(\cdot)} = 1] \\
&- \Pr[(K_1, K_2) \xleftarrow{\$} \mathcal{K}_1 \times \mathcal{K}_2, G \xleftarrow{\$} \mathrm{Rand}(\mathcal{K}_1 \times \mathcal{K}_2, \mathcal{D}, \mathcal{D}) : \mathcal{A}^{G_{RK(\cdot,(K_1,K_2))}(\cdot)} = 1] \\
&+ \Pr[(K_1, K_2) \xleftarrow{\$} \mathcal{K}_1 \times \mathcal{K}_2, G \xleftarrow{\$} \mathrm{Rand}(\mathcal{K}_1 \times \mathcal{K}_2, \mathcal{D}, \mathcal{D}) : \mathcal{A}^{G_{RK(\cdot,(K_1,K_2))}(\cdot)} = 1] \\
&- \Pr[(K_1, K_2) \xleftarrow{\$} \mathcal{K}_1 \times \mathcal{K}_2, G \xleftarrow{\$} \mathrm{Perm}(\mathcal{K}_1 \times \mathcal{K}_2, \mathcal{D}) : \mathcal{A}^{G_{RK(\cdot,(K_1,K_2))}(\cdot)} = 1] \\
&\leq \mathbf{Adv}^{\text{prf}}_{F}(\mathcal{B}_{\mathcal{A}}) + \frac{r \cdot q \cdot (q \cdot min\{r, NM_{\Phi}\} - 1)}{2 \cdot |\mathcal{D}|} . \qquad \square
\end{aligned}$$

Theorem 2 can be exploited to construct various RKA-secure permutation families from MAC algorithms which are already known to be secure in the sense of PRF. Consider for example OMAC [17] with fixed-length inputs, if all message blocks except for the first one are modified into parts of keys, then the modified permutation family is secure against any Φ-restricted related-key attack under the assumption that the underlying block cipher is secure in the sense of PRP and functions in Φ only transform the modified key portions.

Note. A function family $F : \mathcal{K}_1 \times \mathcal{K}_2 \times \mathcal{D} \to \mathcal{D}$ may not be a permutation on $\mathcal{D}$ with respect to each element of $\mathcal{K}_1 \times \mathcal{K}_2$. In this case, Theorem 2 is not applicable. However, notice that most existing block-cipher based MAC algorithms (function families) can be converted to permutation function families, because they are constructed based on permutation families, i.e., block ciphers.

5 Security of Three PRP-RKA Ciphers against Key Recovery

A preliminary extended abstract version of this section appeared in [35]. In [16], it was shown that the advantage $\mathbf{Adv}^{\text{kr}}_{E}(\mathcal{A})$ of any KR adversary $\mathcal{A}$ mounting a *generic* attack depends on the number t of verifications made to the block cipher E (i.e., evaluations of the form $E_{K_i}(M_i)$ for any text M_i and any key K_i of the adversary's choice), and on the key bit-length k. More specifically, it was shown that:

$$\mathbf{Adv}^{\text{kr}}_{E}(\mathcal{A}) \leq \frac{t}{2^k} + \frac{1}{2^k - t} \ .$$

This bounds the advantage of a generic adversary. We see that both terms on the right side of the inequality remain small as long as $t \ll 2^k$. As t relates to an exhaustive key search, this means that a generic adversary must exhaust a significant fraction of key candidates to have a reasonable chance to recover the actual key. This also means that having an advantage significantly better than by exhaustive search requires exploiting the specific structure of the block cipher under attack.

Similarly, in [38], it was shown that the advantage $\mathbf{Adv}^{\text{kr-rka}}_{\Phi,E}(\mathcal{A})$ of any KR-RKA adversary $\mathcal{A}$ mounting a generic related-key attack is bounded by:

$$\mathbf{Adv}^{\text{kr-rka}}_{\Phi,E}(\mathcal{A}) \leq \frac{mt}{2^k} + \frac{1}{2^k} \ ,$$

where m is the number of related-key oracle queries to block cipher E. Analogously, we see that the advantage of a generic adversary remains small as long as $mt \ll 2^k$.

5.1 Construction A

In [3], Bellare and Kohno analyzed a PRP-RKA secure block-cipher based construct that is essentially a generalization of the 2-key variant of DES-EXE [32] structure (see Fig. 1-Construction A). In particular, they proved:

Theorem 3 (Bellare-Kohno) *Let $E : \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^l$ be a block cipher. Let $E' : \{0,1\}^{k+l} \times \{0,1\}^l \rightarrow \{0,1\}^l$ be the block cipher defined as*

$$E'_{K_1\|K_2}(M) = E_{K_1}\big(E_{K_1}(M) \oplus K_2\big)$$

where K_1 is k bits long and K_2 is l bits long. Let Φ be any set of RKD functions over $\{0,1\}^{k+l}$ that modify only K_2 and that are independent of K_1. Then, for any adversary $\mathcal{A}$ against E' that queries its related-key oracle with at most r different RKD transformations and at most q times per transformation, we can construct an adversary $\mathcal{B}_\mathcal{A}$ against E such that

$$\mathbf{Adv}^{\text{prp-rka}}_{\Phi,E'}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prp}}_{E}(\mathcal{B}_\mathcal{A}) + \frac{16r^2q^2 + rq'(q'-1)}{2^{l+1}}$$

and $\mathcal{B}_\mathcal{A}$ makes $2rq$ oracle queries and runs in the same time as $\mathcal{A}$ and q' is q times the maximum over all $K, K' \in \{0,1\}^{k+l}$, of the number of $\phi \in \Phi$ mapping K to K'. □

The result above shows the existence of block ciphers secure against certain classes of Φ-restricted related-key attacks. PRP-RKA security of the resulting cipher comes with a restriction that the set of RKD functions Φ defining an RKA adversary *only modifies the second part of the key* (i.e., K_2). This is a weaker notion of RKA security compared to previous works [19,20,34] where no such restriction is made.

With DES-EXE like structures, one may wonder if existing attacks [32,11] on DES-EXE apply to this variant. We answer this in the affirmative. First, we describe a meet-in-the-middle (MITM) attack that does not require related-key queries. Next, we present a differential RKA that requires slightly less effort.

MITM Attack.

1. Let $\langle M, C\rangle$ and $\langle M', C'\rangle$ be any two pairs of plaintext/ciphertext in $\mathcal{L}$ with $C = E'_{K_1\|K_2}(M)$ and $C' = E'_{K_1\|K_2}(M')$.
2. For each key guess, $\hat{K}_1 \in \{0,1\}^k$, do the following.
   (a) Evaluate

$$S_1 = E_{\hat{K}_1}(M) \oplus E_{\hat{K}_1}(M') \quad \text{and} \quad S_2 = E^{-1}_{\hat{K}_1}(C) \oplus E^{-1}_{\hat{K}_1}(C')$$

   and check whether $S_1 = S_2$.

(b) If so, let $\hat{K}_2 = E^{-1}_{\hat{K}_1}(C) \oplus E_{\hat{K}_1}(M)$ and validate the guessed key $\hat{K}_1 \| \hat{K}_2$ on all pairs of $\mathcal{L}$.

3. If the guessed key is validated, return (the consistent key) $\hat{K}_1 \| \hat{K}_2$.

If the above MITM adversary tries all possible keys $\hat{K}_1 \in \{0,1\}^k$ at Step 2, it will win the key recovery game with probability 1. As a result, the success probability of this adversary is ρ, the proportion of guessed keys.

Recalling the results in [16], when considering a generic adversary, any block cipher E' of key length $k+l$ bits is expected to provide the following security bound:

$$\mathbf{Adv}^{\mathrm{kr}}_{E'}(A) \leq \frac{t}{2^{k+l}} + \frac{1}{2^{k+l}-t} ,$$

where t denotes the number of verifications. A closer look at the proof offered in [16] shows that if the generic adversary makes verifications with distinct key candidates then the bound can be sharpened as:

$$\mathbf{Adv}^{\mathrm{kr}}_{E'}(\mathcal{A}) \leq \frac{t}{2^{k+l}} + \frac{1-\frac{t}{2^{k+l}}}{2^{k+l}-t} = \frac{t}{2^{k+l}} + \frac{1}{2^{k+l}} \ .$$

If we let t denote the number of times Step 2 in the MITM attack is performed (i.e., the number of times distinct key candidates are being manipulated), then the success probability is given by:

$$\mathbf{Adv}^{\mathrm{kr}}_{E'}(\mathrm{MITM}) = \rho = \frac{t}{2^k} \ .$$

Interestingly, we observe that

$$\mathbf{Adv}^{\mathrm{kr}}_{E'}(\mathrm{MITM}) = \frac{t}{2^k} > \frac{t}{2^{k+l}} + \frac{1}{2^{k+l}} ,$$

and so the block-cipher based construct of Fig. 1-A does not give the best possible security against key recovery. In fact, the effective keyspace is essentially reduced by l bits.

Differential RKA Attack (DRKA).

1. Let $\langle M, C \rangle$ be any pairs of plaintext/ciphertext in $\mathcal{L}$ with $C = E'_{K_1 \| K_2}(M)$.
2. Query the related-key oracle with (M, Δ) and obtain the pair (M, C') with $C' = E'_{K_1 \| K_2 + \Delta}(M)$.
3. For each key guess, $\hat{K}_1 \in \{0,1\}^k$, do the following.
   (a) Check whether
   $$E^{-1}_{\hat{K}_1}(C) \oplus E^{-1}_{\hat{K}_1}(C') = \Delta \ .$$
   (b) If so, let $\hat{K}_2 = E^{-1}_{\hat{K}_1}(C) \oplus E_{\hat{K}_1}(M)$ and validate the guessed key $\hat{K}_1 \| \hat{K}_2$ on all pairs of $\mathcal{L}$.
4. If the guessed key is validated, return (the consistent key) $\hat{K}_1 \| \hat{K}_2$.

According to [38], we know that any block cipher E' of key length $k+l$ bits is expected to provide the following security against generic related-key attacks:

$$\mathbf{Adv}^{\text{kr-rka}}_{\Phi, E'}(\mathcal{A}) \leq \frac{mt}{2^{k+l}} + \frac{1}{2^{k+l}} ,$$

where m denotes the number of calls to the related-key oracle and t the number of verifications. Interestingly, in a way similar to the analysis of the previous attack, we get that, for $m = 1$, the success probability of our differential related-key attack (DRKA) satisfies

$$\mathbf{Adv}^{\text{kr-rka}}_{E'}(\text{DRKA}) = \frac{t}{2^k} > \frac{t}{2^{k+l}} + \frac{1}{2^{k+l}} \ .$$

Again, we conclude that the block-cipher based construct of Fig. 1-A does not offer the best possible security against key recovery, in this case, in the presence of related-key oracles.

5.2 Construction B

Lucks [29] argued that Theorem 3 only applies for large l. For practical values of l, one may have that $\mathbf{Adv}^{\text{prp-rka}}_{\Phi,E'}(\mathcal{A}) - \mathbf{Adv}^{\text{prp}}_{E}(\mathcal{B}_{\mathcal{A}})$ is not negligible. He therefore considered a construction that yields a more meaningful security bound. See Fig. 1-B.

Theorem 4 (Lucks) *Let $E : \{0,1\}^l \times \{0,1\}^l \to \{0,1\}^l$ be a block cipher. Let $E' : \{0,1\}^{2l} \times \{0,1\}^l \to \{0,1\}^l$ be the block cipher defined as*

$$E'_{K_1\|K_2}(M) = E_{E_{K_1}(K_2)}(M)$$

where K_1 and K_2 are l bits long. Let Φ be any set of RKD functions over $\{0,1\}^{k+l}$ that modify only K_2 and that are independent of K_1. Then, for any adversary $\mathcal{A}$ against E' that queries its related-key oracle with at most r different RKD transformations, we can construct an adversary $\mathcal{B}_{\mathcal{A}}$ against E such that

$$\frac{\mathbf{Adv}^{\text{prp-rka}}_{\Phi,E'}(\mathcal{A})}{r+1} \leq \mathbf{Adv}^{\text{prp}}_{E}(\mathcal{B}_{\mathcal{A}}) \ .$$

and $\mathcal{B}_{\mathcal{A}}$ makes no more oracle queries than $\mathcal{A}$ and runs in the same running time as $\mathcal{A}$. □

The encryption of key K_2 under key K_1 is used as the final secret key to encrypt the plaintext M, i.e., $C = E_{E_{K_1}(K_2)}(M)$. Further, note that although a $2l$-bit key $K_1\|K_2$ is used, essentially the adversary just needs to recover the final l-bit secret key $\widetilde{K} := E_{K_1}(K_2)$ that is used to key the encryption of M, which reduces the exhaustive key search space to l bits. For an attacker performing an exhaustive search (XS) on $\widetilde{K}$, we therefore have

$$\mathbf{Adv}^{\text{kr}}_{E'}(\text{XS}) = \frac{t}{2^l} = \frac{t}{2^k} \ ,$$

where t denotes the number of guessed keys (note that in this construction, $k = l$). This has to be compared with the security bound given by a generic KR adversary against a $2l$-bit key cipher E'':

$$\mathbf{Adv}^{\text{kr}}_{E''}(\mathcal{A}) \leq \frac{t}{2^{2l}} + \frac{1}{2^{2l} - t} = \frac{t}{2^{2k}} + \frac{1}{2^{2k} - t} \ .$$

We see that the above XS attacker has a substantially larger success probability, and the effective keyspace is halved.

5.3 Construction C

Recall that DESX [21] is defined as:

$$\mathrm{DESX}(M, K_1 \| K \| K_2) = K_2 \oplus E_K(M \oplus K_1)$$

where K_1 and K_2 are the pre- and post-whitening keys, respectively, and K is the key to the inner E encapsulated by the two outer whitening (XOR) operations. The basic structure of Construction C is like DESX [21] except that the pre- and post-whitening keys equal each other and is the result of applying an ϵ-AXU$_2$ hash function h to the input tweak T, $K_1 = K_2 = h(T)$:

$$E'_{K\|T,h}(M) = h(T) \oplus E_K(M \oplus h(T)).$$

In other words, this construction can be viewed as 2-key DESX where the secret key is equivalently K and $h(T)$, thus the total key length is $|K| + |h(T)|$, i.e. $k + l$.

This construction, by design, and hence its security proof in Proposition 1, restricts that the set of RKD functions Φ defining an RKA adversary only modifies the input T and not the input K to $E_K(\cdot)$; this is similar to the RKD-restricting design approach of Constructions A and B.

An advanced slide attack [10] was applied to DESX. It is basically an MITM attack. We show that a variant also applies here.

MITM Attack. We first make some observations. Consider a pair of plaintexts M and M' such that the corresponding ciphertexts, C and C', satisfy the relation $C \oplus C' = h(T)$. Such a pair is called a *slid pair*. For such a slid pair $\langle M, C\rangle$ and $\langle M', C'\rangle$, we have

$$C = C' \oplus h(T) = E_K\big(M' \oplus h(T)\big) \quad \text{and} \quad C' = C \oplus h(T) = E_K\big(M \oplus h(T)\big)$$

which yields

$$E_K^{-1}(C) \oplus M = E_K^{-1}(C') \oplus M' \ .$$

Based on this, we can mount the following attack.

1. Let $\mathcal{L} = \langle M_i, C_i\rangle_{1\le i\le p}$ be a list of p known pairs of plaintext/ciphertext with, $C_i = E'_{K\|T,h}(M_i)$.
2. For each key guess, $\hat{K} \in \{0,1\}^k$, do the following.
   (a) For each $1 \le i \le p$, evaluate $E_{\hat{K}}^{-1}(C_i) \oplus M_i$ and insert
   $$\langle E_{\hat{K}}^{-1}(C_i) \oplus M_i, i\rangle$$
   into a hash table keyed by the first component, and check whether there is a coincidence (collision) in the table.
   (b) If so, assuming that the collision occurs for indexes i and j, namely, $E_{\hat{K}}^{-1}(C_i) \oplus M_i = E_{\hat{K}}^{-1}(C_j) \oplus M_j$, let $h(\hat{T}) = C_i \oplus C_j$ and validate the guessed key $\hat{K}\|h(\hat{T})$ on all pairs of $\mathcal{L}$.
3. If the guessed key is validated, return (the consistent key) $\hat{K}\|h(\hat{T})$.

The probability to have at least one coincidence (i.e., to find at least one slid pair $\langle M_i, C_i\rangle$ and $\langle M_j, C_j\rangle$ in $\mathcal{L}$) is about

$$1 - \exp(-p^2/2^{l+1}) \quad \text{with } p = |\mathcal{L}|$$

due to the birthday paradox.

As a result, if $t/2^k$ denotes the proportion of keys guessed at Step 2, the success probability of our MITM attacker is

$$\mathbf{Adv}^{\mathsf{kr}}_{E'}(\text{MITM}) \approx \frac{t}{2^k}\left(1 - \exp(-p^2/2^{l+1})\right).$$

More precisely, when the cardinality p of the plaintext/ciphertext list is square-root of the entire plaintext space, i.e. $p = 2^{(l+1)/2}$, then this MITM attack gives the adversarial advantage

$$\mathbf{Adv}^{\mathsf{kr}}_{E'}(\text{MITM}) = O\left(\frac{t}{2^k}\right) > \frac{t}{2^{k+l}} + \frac{1}{2^{k+l}}.$$

Thus, the MITM applies to this construction when the adversary has access to a significantly large plaintext/ciphertext list, of cardinality $p \geq 2^{(l+1)/2}$. Further discussions of this in comparison with other constructions are given in subsection 5.4.

Resistance against RKA. We consider whether allowing the adversary extra access to a related-key oracle would cause an attack better than bruteforce. To do so, we need to exploit the related-key oracle to our advantage. The related-key oracle, by design of the Construction C only allows variation to T, thus related-key differences can only be induced with the T input via the function $h(\cdot)$. If with non-negligible probability an input difference $\Delta T = T \oplus T'$ leads to an output difference $\Delta H = h(T) \oplus h(T')$, then one could choose two plaintexts m and $m' = m \oplus \Delta H$ such that a zero input difference goes into the underlying cipher E_K (a non-zero difference does not propagate to any non-negligibly observable property at the output since E_K is a secure block cipher), and a ciphertext difference $C \oplus C' = \Delta H$ is obtained. This could give a distinguisher for the construction but does not lead to key recovery. However, $h(\cdot)$ by design is ϵ-AXU_2, therefore

$$\Pr[h(T) \oplus h(T') = \Delta H] \leq \epsilon$$

for all $T, T', \Delta H$ so even this would not apply. A potential strategy to extend this to key recovery is to consider message-input dependent differences [9] $\langle \Delta T, \Delta H_i\rangle$ through $h(\cdot)$, where the space of possible output differences is partitioned into classes ΔH_i dependent on the classes of input values T_i, so one can query the related-key oracle with plaintext inputs $m_i = m \oplus \Delta H_i$ and expect that the ciphertext difference be observed as ΔH_i only if the unknown input T falls within the class T_i. Once detected, T can be searched (along with exhaustive guess of K) within the reduced space of T_i. The notion of input (message/key) dependent differences [9,30] has been considered for block ciphers; we leave open the question of whether input dependent differences can be exploitable for ϵ-AXU_2 hash functions. Meanwhile, the idea of exploiting many small biases rather than confining to only one larger bias, was proposed in [37] as the generalized (truncated) differential cryptanalysis technique.

The best known attack therefore remains to be the related-key meet-in-the-middle attack over the keyspace [38]; more precisely the keyspace is reduced by the number m of queries made to the related-key oracle, resulting in the success probability of

$$\mathbf{Adv}^{\text{kr-rka}}_{\Phi,E'}(\mathcal{A}) \leq \frac{mt}{2^{k+l}} + \frac{1}{2^{k+l}}\ .$$

5.4 Discussions

Table 1 summarizes the KR and KR-RKA adversarial advantages for Constructions A, B and C, contrasting between the expected (exp) advantage and the actual derived advantage as a consequence of specific attacks.

Table 1 Comparing the Adversarial Advantages

Cipher	Key Length	exp $\mathbf{Adv}^{\mathsf{kr}}(\cdot)$	$\mathbf{Adv}^{\mathsf{kr}}(\cdot)$	exp $\mathbf{Adv}^{\mathsf{kr\text{-}rka}}(\cdot)$	$\mathbf{Adv}^{\mathsf{kr\text{-}rka}}(\cdot)$
A	$k+l$	$\frac{t}{2^{k+l}} + \frac{1}{2^{k+l}}$	$MITM: \frac{t}{2^k}$	$\frac{mt}{2^{k+l}} + \frac{1}{2^{k+l}}$	$DRKA: \frac{t}{2^k}$
B	$2l = 2k$	$\frac{t}{2^{2l}} + \frac{1}{2^{2l}-t}$	$XS: \frac{t}{2^l}$	$\frac{mt}{2^{2l}} + \frac{1}{2^{2l}}$	–
C	$k+l$	$\frac{t}{2^{k+l}} + \frac{1}{2^{k+l}}$	$MITM: \frac{t}{2^k}(1-\exp(-p^2/2^{l+1}))$	$\frac{mt}{2^{k+l}} + \frac{1}{2^{k+l}}$	–

In the KR case, attacks exist on Constructions A and B that reduce their security effectively to the exhaustive search space over one (instead of both) key part. Construction C thus far fares better where its adversarial advantage is additionally a function of the cardinality p of the plaintext/ciphertext list; whereas the specific attacks on Constructions A and B work with only a pair of plaintext/ciphertexts. Having said that, the attacks on Constructions A, B and C in previous subsections are the best known attacks so far; it is open whether there are better attacks in future that close this gap between the constructions.

In the KR-RKA case, a specific attack exists on Construction A; while it seems similar attacks do not exist on the other constructions. For Construction B, this resistance is derived from the fact that both key parts K_1 and K_2 are input to an underlying cipher E before being input as a key to a subsequent application of the cipher E. This way, assuming that the underlying cipher E is a good PRP, adversarial variations in the key parts are not significantly observable at the output of E. For Construction C, this resistance is similarly derived from the fact that the adversarial variation on key part K enters a good underlying PRP cipher E, and that even if the input T to the key part $h(T)$ is adversarially variable, the fact that h is ϵ-AXU_2 means no significant variation patterns will be observed at the output.

6 Relationships between Security Notions

In this section, we introduce indistinguishability and non-malleability based security notions for the RKA setting that give more information on permutation families. We also show the relations among these notions as well as relations with pseudorandomness and tweakable counterparts.

We first give a definition of *indistinguishability*, which is the same as the left-or-right security notion of Bellare et al. [1].

Definition 6 (TWEAK-IND) [13] Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{D} \to \mathcal{D}$ be a tweakable permutation family and $\mathcal{A}$ be an adversary. Then the tweak-ind advantage of $\mathcal{A}$ is defined by

$$\begin{aligned}\mathbf{Adv}^{\text{tweak-ind}}_{\tilde{E}}(\mathcal{A}) &= \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\tilde{E}_K(\cdot,\cdot)^1, \tilde{E}_K^{-1}(\cdot,\cdot)^1} = 1] \\ &- \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\tilde{E}_K(\cdot,\cdot)^0, \tilde{E}_K^{-1}(\cdot,\cdot)^0} = 1].\end{aligned}$$

$\mathcal{A}^{\tilde{\mathcal{O}}(\cdot,\cdot)^b,\tilde{\mathcal{O}}^{-1}(\cdot,\cdot)^b}$ ($b = 0$ or 1) means $\mathcal{A}$ with two oracles $\tilde{\mathcal{O}}(\cdot,\cdot)^b, \tilde{\mathcal{O}}^{-1}(\cdot,\cdot)^b$; for an adversary's query of $((T_0, M_0), (T_1, M_1))$ (resp. $((T_0, C_0), (T_1, C_1))$) to the first (resp. second) oracle it returns $\tilde{\mathcal{O}}(T_b, M_b)$ (resp. $\tilde{\mathcal{O}}^{-1}(T_b, C_b)$).

Similarly, the IND-RKA security notion can be defined as follows.

Definition 7 (IND-RKA) Let $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ be a permutation family and Φ be a set of functions over $\mathcal{K}$. Let $\mathcal{A}$ be an adversary that is restricted to queries within $\Phi \times \mathcal{D}$. Then the ind-rka advantage of $\mathcal{A}$ is defined by

$$\begin{aligned}\mathbf{Adv}^{\text{ind-rka}}_{\Phi,E}(\mathcal{A}) &= \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_{RK(\cdot,K)}(\cdot)^1, E^{-1}_{RK(\cdot,K)}(\cdot)^1} = 1] \\ &\quad - \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_{RK(\cdot,K)}(\cdot)^0, E^{-1}_{RK(\cdot,K)}(\cdot)^0} = 1].\end{aligned}$$

$\mathcal{A}^{\mathcal{O}_{RK(\cdot)}(\cdot)^b, \mathcal{O}^{-1}_{RK(\cdot)}(\cdot)^b}$ ($b = 0$ or 1) means $\mathcal{A}$ with two oracles $\mathcal{O}_{RK(\cdot)}(\cdot)^b, \mathcal{O}^{-1}_{RK(\cdot)}(\cdot)^b$; for an adversary's query of $((\phi_0, M_0), (\phi_1, M_1))$ (resp. $((\phi_0, C_0), (\phi_1, C_1))$) to the first (resp. second) oracle it returns $\mathcal{O}_{\phi_b(K)}(M_b)$ (resp. $\mathcal{O}^{-1}_{\phi_b(K)}(C_b)$).

Note that the TWEAK-IND adversary and the IND-RKA adversary should be disallowed from asking queries that will allow it to win trivially. In the IND-RKA security notion, when the IND-RKA adversary gets an answer C from the encryption oracle for a query $((\phi_0, M_0), (\phi_1, M_1))$, the adversary should be disallowed from asking queries $((\phi_0, M_0), (\cdot, \cdot))$, or $((\cdot, \cdot), (\phi_1, M_1))$ to the encryption oracle and queries $((\phi_0, C), (\cdot, \cdot))$, or $((\cdot, \cdot), (\phi_1, C))$ to the decryption oracle, where $(\cdot, \cdot)$ represents an arbitrary argument. The similar argument is applied when the IND-RKA adversary gets an answer M from the decryption oracle for a query $((\phi_0, C_0), (\phi_1, C_1))$. See [13] for the disallowed queries of a tweak-ind adversary.

We now consider another security notion, *non-malleability*. In a tweakable permutation family $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{D} \to \mathcal{D}$, a tweak-nm adversary $\mathcal{A}$ is given access to an encrypting oracle $\tilde{E}_K(\cdot, \cdot)$ and a decrypting oracle $\tilde{E}^{-1}_K(\cdot, \cdot)$ where K is chosen uniformly at random from the set of keys $\mathcal{K}$. In order to define the advantage of a tweak-nm adversary $\mathcal{A}$ we need definitions of the following three sets.

- $\mathcal{M}(T)$: a set of all M such that $\mathcal{A}$ asks $\tilde{E}_K(\cdot, \cdot)$ to encrypt (T, M) or $\mathcal{A}$ asks $\tilde{E}^{-1}_K(\cdot, \cdot)$ to decrypt (T, C) and its answer is M.
- $\mathcal{C}(T)$: a set of all C such that $\mathcal{A}$ asks $\tilde{E}^{-1}_K(\cdot, \cdot)$ to decrypt (T, C) or $\mathcal{A}$ asks $\tilde{E}_K(\cdot, \cdot)$ to encrypt (T, M) and its answer is C.
- $\mathcal{M}(T, C)$: a set $\{\tilde{E}^{-1}_K(T, C)\}$ if $C \in \mathcal{C}(T)$, and a set $\mathcal{D} \setminus \mathcal{M}(T)$ otherwise.

Definition 8 (TWEAK-NM) [13] Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{D} \to \mathcal{D}$ be a tweakable permutation family and $\mathcal{A}$ be an adversary. Then the tweak-nm advantage of $\mathcal{A}$ is defined by

$$\begin{aligned}\mathbf{Adv}^{\text{tweak-nm}}_{\tilde{E}}(\mathcal{A}) &= \Pr[K \xleftarrow{\$} \mathcal{K}, (T, C, f) \xleftarrow{\$} \mathcal{A}^{\tilde{E}_K(\cdot,\cdot), \tilde{E}^{-1}_K(\cdot,\cdot)}, M = \tilde{E}^{-1}_K(T, C) : f(M) = 1] \\ &\quad - \Pr[K \xleftarrow{\$} \mathcal{K}, (T, C, f) \xleftarrow{\$} \mathcal{A}^{\tilde{E}_K(\cdot,\cdot), \tilde{E}^{-1}_K(\cdot,\cdot)}, M \xleftarrow{\$} \mathcal{M}(T, C) : f(M) = 1].\end{aligned}$$

The function f is the encoding of a predicate $f : \mathcal{D} \to \{0, 1\}$.

Similarly, we can define non-malleability of a permutation family $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ against related-key attacks. In related-key attack models, an NM-RKA adversary $\mathcal{A}$ is given access to an encrypting oracle $E_{RK(\cdot,K)}(\cdot)$ and a decrypting oracle $E^{-1}_{RK(\cdot,K)}(\cdot)$ where K is chosen uniformly at random from the set of keys $\mathcal{K}$. In these attack models, A is restricted to queries of the form (ϕ, x) in which ϕ is in a certain set of key transformations Φ and x is in $\mathcal{D}$. The three sets are defined as follows.

- $\mathcal{M}(\phi)$: a set of all M such that $\mathcal{A}$ asks $E_{RK(\cdot,K)}(\cdot)$ to encrypt (ϕ, M) or $\mathcal{A}$ asks $E^{-1}_{RK(\cdot,K)}(\cdot)$ to decrypt (ϕ, C) and its answer is M.
- $\mathcal{C}(\phi)$: a set of all C such that $\mathcal{A}$ asks $E^{-1}_{RK(\cdot,K)}(\cdot)$ to decrypt (ϕ, C) or $\mathcal{A}$ asks $E_{RK(\cdot,K)}(\cdot)$ to encrypt (ϕ, M) and its answer is C.
- $\mathcal{M}(\phi, C)$: a set $\{E^{-1}_{\phi(K)}(C)\}$ if $C \in \mathcal{C}(\phi)$, and a set $\mathcal{D} \setminus \mathcal{M}(\phi)$ otherwise.

Definition 9 (NM-RKA) Let $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ be a permutation family and Φ be a set of functions over $\mathcal{K}$. Let $\mathcal{A}$ be an adversary that is restricted to queries within $\Phi \times \mathcal{D}$. Then the nm-rka advantage of $\mathcal{A}$ is defined by

$$\begin{aligned}\mathbf{Adv}^{\text{nm-rka}}_{\Phi,E}(\mathcal{A}) = \Pr[K \xleftarrow{\$} \mathcal{K}, (\phi, C, f) \xleftarrow{\$} \mathcal{A}^{E_{RK(\cdot,K)}(\cdot), E^{-1}_{RK(\cdot,K)}(\cdot)}, M = E^{-1}_{\phi(K)}(C) : f(M) = 1] \\ - \Pr[K \xleftarrow{\$} \mathcal{K}, (\phi, C, f) \xleftarrow{\$} \mathcal{A}^{E_{RK(\cdot,K)}(\cdot), E^{-1}_{RK(\cdot,K)}(\cdot)}, M \xleftarrow{\$} \mathcal{M}(\phi, C) : f(M) = 1].\end{aligned}$$

The function f is the encoding of a predicate $f : \mathcal{D} \to \{0, 1\}$.

The following three theorems clarify the relationships between these newly defined security notions IND-RKA, NM-RKA and the SPRP-RKA security notion. Theorem 5 shows that SPRP-RKA security implies IND-RKA security and Theorem 6 shows the converse. Theorem 7 shows that SPRP-RKA security implies NM-RKA security. The proofs of Theorems 5, 6 and 7 are similar to the proofs of [13], so we omit them.

Theorem 5 (SPRP-RKA→IND-RKA) *Let $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ be a permutation family and Φ be a set of functions over $\mathcal{K}$. If E is secure in the sense of SPRP-RKA restricted to Φ, then E is also secure in the sense of IND-RKA restricted the Φ. Formally, given a Φ-restricted IND-RKA adversary $\mathcal{A}$ that queries its oracles with at most q queries, we can construct a Φ-restricted SPRP-RKA adversary $\mathcal{B}_{\mathcal{A}}$ such that*

$$\mathbf{Adv}^{\text{ind-rka}}_{\Phi,E}(\mathcal{A}) \leq 2 \cdot \mathbf{Adv}^{\text{sprp-rka}}_{\Phi,E}(\mathcal{B}_{\mathcal{A}}) + \frac{2 \cdot q^2}{|\mathcal{D}| - q}$$

and $\mathcal{B}_{\mathcal{A}}$ takes almost same amount of time and makes the same number of oracle queries as $\mathcal{A}$.[5]

Theorem 6 (IND-RKA→SPRP-RKA) *Let $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ be a permutation family and Φ be a set of functions over $\mathcal{K}$. If E is secure in the sense of IND-RKA restricted to Φ, then E is also secure in the sense of SPRP-RKA restricted the Φ. Formally, given a Φ-restricted SPRP-RKA adversary $\mathcal{A}$ that queries its oracles with at most q queries, we can construct a Φ-restricted IND-RKA adversary $\mathcal{B}_{\mathcal{A}}$ such that*

$$\mathbf{Adv}^{\text{sprp-rka}}_{\Phi,E}(\mathcal{A}) \leq \mathbf{Adv}^{\text{ind-rka}}_{\Phi,E}(\mathcal{B}_{\mathcal{A}})$$

and $\mathcal{B}_{\mathcal{A}}$ takes almost same amount of time and makes the same number of oracle queries as $\mathcal{A}$.

[5] B_A takes a slightly higher time than A, as the main loop of B_A is A; before performing A, B_A conducts a certain preparation for the use of A, and after performing A, B_A outputs either 0 or 1, which both require a small time complexity. In the following theorems, the same statement is applied.

Theorem 7 (SPRP-RKA→NM-RKA) *Let $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ be a permutation family and Φ be a set of functions over $\mathcal{K}$. If E is secure in the sense of SPRP-RKA restricted to Φ, then E is also secure in the sense of NM-RKA restricted the Φ. Formally, given a Φ-restricted NM-RKA adversary $\mathcal{A}$ that queries its oracles with at most q queries, we can construct a Φ-restricted SPRP-RKA adversary $\mathcal{B}_{\mathcal{A}}$ such that*

$$\mathbf{Adv}^{\text{nm-rka}}_{\Phi,E}(\mathcal{A}) \leq \mathbf{Adv}^{\text{sprp-rka}}_{\Phi,E}(\mathcal{B}_{\mathcal{A}})$$

and $\mathcal{B}_{\mathcal{A}}$ takes almost same amount of time as $\mathcal{A}$ and makes one more query than $\mathcal{A}$.

The following two theorems show that secure TWEAK-IND (resp. TWEAK-NM) families can be transformed into secure IND-RKA (resp. NM-RKA) families.

Theorem 8 (TWEAK-IND→IND-RKA) *Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{D} \to \mathcal{D}$ be a tweakable permutation family and let $E : (\mathcal{K} \times \mathcal{T}) \times \mathcal{D} \to \mathcal{D}$ be a permutation family defined as in Theorem 1. If $\tilde{E}$ is secure in the sense of TWEAK-IND, then E is secure in the sense of IND-RKA restricted to Φ if each function $\phi \in \Phi$ is a partial transformation for which there exists a function $\phi' : \mathcal{T} \to \mathcal{T}$ such that $\phi(K, T) = (K, \phi'(T))$. Formally, given a Φ-restricted IND-RKA adversary $\mathcal{A}$ attacking E, we can construct a TWEAK-IND adversary $\mathcal{B}_{\mathcal{A}}$ attacking $\tilde{E}$ such that*

$$\mathbf{Adv}^{\text{ind-rka}}_{\Phi,E}(\mathcal{A}) \leq \mathbf{Adv}^{\text{tweak-ind}}_{\tilde{E}}(\mathcal{B}_{\mathcal{A}})$$

and $\mathcal{B}_{\mathcal{A}}$ takes the same amount of time and makes the same number of oracle queries as $\mathcal{A}$.

Proof Let $\mathcal{B}_{\mathcal{A}}$ be the $\widetilde{E}$ adversary that works as follows.

$<$Adversary $\mathcal{B}_{\mathcal{A}}^{\tilde{\mathcal{O}}(\cdot,\cdot)^b, \tilde{\mathcal{O}}^{-1}(\cdot,\cdot)^b}>$

1. Select T at random from $\mathcal{T}$.
2. Obtain $\mathcal{A}$'s request $((\phi_0, M_0), (\phi_1, M_1))$ (or $((\phi_0, C_0), (\phi_1, C_1))$) by running $\mathcal{A}$, where $\phi_0 = (id, \phi'_0)$ and $\phi_1 = (id, \phi'_1)$.
3. Return $\tilde{\mathcal{O}}(\phi'_b(T), M_b)$ (or $\tilde{\mathcal{O}}^{-1}(\phi'_b(T), C_b)$) to $\mathcal{A}$.
4. If $\mathcal{A}$ outputs b', then output b'. Otherwise, go to Step 2.

Since the adversary $\mathcal{B}_{\mathcal{A}}$ is given access to $\tilde{E}_K(\cdot,\cdot)^b, \tilde{E}_K^{-1}(\cdot,\cdot)^b$ where K is randomly chosen from $\mathcal{K}$, $\mathcal{B}_{\mathcal{A}}$ computes $E_{RK(\cdot,K||T)}(\cdot)^b, E^{-1}_{RK(\cdot,K||T)}(\cdot)^b$ by running $\mathcal{A}$. So the equality

$$\begin{aligned}&\Pr\left[K \xleftarrow{\$} \mathcal{K} : \mathcal{B}_{\mathcal{A}}^{\tilde{E}_K(\cdot,\cdot)^b, \tilde{E}_K^{-1}(\cdot,\cdot)^b} = 1\right] = \\ &\Pr\left[K \xleftarrow{\$} \mathcal{K}, T \xleftarrow{\$} \mathcal{T} : \mathcal{A}^{E_{RK(\cdot,K||T)}(\cdot)^b, E^{-1}_{RK(\cdot,K||T)}(\cdot)^b} = 1\right]\end{aligned}$$

holds. This completes the proof. □

Theorem 9 (TWEAK-NM→NM-RKA) *Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{D} \to \mathcal{D}$ be a tweakable permutation family and let $E : (\mathcal{K} \times \mathcal{T}) \times \mathcal{D} \to \mathcal{D}$ be a permutation family defined as in Theorem 1. If $\tilde{E}$ is secure in the sense of TWEAK-NM, then E is secure in the sense of NM-RKA restricted to Φ if each function $\phi \in \Phi$ is a partial transformation for which there exists a function $\phi' : \mathcal{T} \to \mathcal{T}$ such that $\phi(K, T) = (K, \phi'(T))$. Formally, given*

a Φ-restricted NM-RKA adversary $\mathcal{A}$ attacking E, we can construct a TWEAK-NM adversary $\mathcal{B}_{\mathcal{A}}$ attacking $\tilde{E}$ such that

$$\mathbf{Adv}^{\text{nm-rka}}_{\Phi,E}(\mathcal{A}) \leq \mathbf{Adv}^{\text{tweak-nm}}_{\tilde{E}}(\mathcal{B}_{\mathcal{A}})$$

and $\mathcal{B}_{\mathcal{A}}$ takes the same amount of time and makes the same number of oracle queries as $\mathcal{A}$.

Proof Let $\mathcal{B}_{\mathcal{A}}$ be the $\widetilde{E}$ adversary that works as follows.

<Adversary $\mathcal{B}_{\mathcal{A}}^{\tilde{\mathcal{O}}(\cdot,\cdot),\tilde{\mathcal{O}}^{-1}(\cdot,\cdot)}$>

1. Select T at random from $\mathcal{T}$.
2. Obtain $\mathcal{A}$'s request $(\phi^*(=(id,\phi'^*)), M^*)$ (or $(\phi^*(=(id,\phi'^*)), C^*)$) by running $\mathcal{A}$.
3. Return $\tilde{\mathcal{O}}(\phi'^*(T), M^*)$ (or $\tilde{\mathcal{O}}^{-1}(\phi'^*(T), C^*)$) to $\mathcal{A}$.
4. If $\mathcal{A}$ outputs $(\phi(=(id,\phi')), C, f)$, then output $(\phi'(T), C, f)$. Otherwise, go to Step 2.

Since the adversary $\mathcal{B}_{\mathcal{A}}$ is given access to $\tilde{E}_K(\cdot,\cdot), \tilde{E}_K^{-1}(\cdot,\cdot)$ where K is chosen uniformly at random from $\mathcal{K}$, $\mathcal{B}_{\mathcal{A}}$ computes $E_{RK(\cdot,K||T)}(\cdot), E^{-1}_{RK(\cdot,K||T)}(\cdot)$ by running $\mathcal{A}$. Based on Definition 9 we have

$$\begin{aligned}
&\mathbf{Adv}^{\text{tweak-nm}}_{\tilde{E}}(\mathcal{B}_{\mathcal{A}}) = \\
&\Pr\left[K \xleftarrow{\$} \mathcal{K}, T \xleftarrow{\$} \mathcal{T}, (\phi(=(id,\phi')), C, f) \xleftarrow{\$} \mathcal{A}^{E_{RK(\cdot,K||T)}(\cdot), E^{-1}_{RK(\cdot,K||T)}(\cdot)}, \right. \\
&\qquad \left. M = \tilde{E}_K^{-1}(\phi'(T), C) : f(M) = 1\right] \\
-\ &\Pr\left[K \xleftarrow{\$} \mathcal{K}, T \xleftarrow{\$} \mathcal{T}, (\phi(=(id,\phi')), C, f) \xleftarrow{\$} \mathcal{A}^{E_{RK(\cdot,K||T)}(\cdot), E^{-1}_{RK(\cdot,K||T)}(\cdot)}, \right. \\
&\qquad \left. M \xleftarrow{\$} \mathcal{M}(\phi'(T), C) : f(M) = 1\right].
\end{aligned}$$

Since $f(\tilde{E}_K^{-1}(\phi'(T), C)) = 1$ if and only if $f(E^{-1}_{K||\phi'(T)}(C)) = 1$, the equality

$$\begin{aligned}
&\Pr\left[K \xleftarrow{\$} \mathcal{K}, T \xleftarrow{\$} \mathcal{T}, (\phi(=(id,\phi')), C, f) \xleftarrow{\$} \mathcal{A}^{E_{RK(\cdot,K||T)}(\cdot), E^{-1}_{RK(\cdot,K||T)}(\cdot)}, \right. \\
&\qquad \left. M = \tilde{E}_K^{-1}(\phi'(T), C) : f(M) = 1\right] \\
=\ &\Pr\left[K \xleftarrow{\$} \mathcal{K}, T \xleftarrow{\$} \mathcal{T}, (\phi(=(id,\phi')), C, f) \xleftarrow{\$} \mathcal{A}^{E_{RK(\cdot,K||T)}(\cdot), E^{-1}_{RK(\cdot,K||T)}(\cdot)}, \right. \\
&\qquad \left. M = E^{-1}_{K||\phi'(T)}(C) : f(M) = 1\right]
\end{aligned}$$

holds. Furthermore, for all $\phi = (id, \phi')$ and C, $\mathcal{M}(\phi'(T), C)$ of $\mathcal{B}_{\mathcal{A}}$ takes the same distribution with $\mathcal{M}(\phi, C)$ of $\mathcal{A}$ (this is because the output of BA is based on the output of A) and thus the equation

$$\begin{aligned}
&\Pr\left[K \xleftarrow{\$} \mathcal{K}, T \xleftarrow{\$} \mathcal{T}, (\phi(=(id,\phi')), C, f) \xleftarrow{\$} \mathcal{A}^{E_{RK(\cdot,K||T)}(\cdot), E^{-1}_{RK(\cdot,K||T)}(\cdot)}, \right. \\
&\qquad \left. M \xleftarrow{\$} \mathcal{M}(\phi'(T), C) : f(M) = 1\right] \\
=\ &\Pr\left[K \xleftarrow{\$} \mathcal{K}, T \xleftarrow{\$} \mathcal{T}, (\phi(=(id,\phi')), C, f) \xleftarrow{\$} \mathcal{A}^{E_{RK(\cdot,K||T)}(\cdot), E^{-1}_{RK(\cdot,K||T)}(\cdot)}, \right. \\
&\qquad \left. M \xleftarrow{\$} \mathcal{M}(\phi, C) : f(M) = 1\right]
\end{aligned}$$

holds. This completes the proof. □

7 Conclusions

We have presented an SPRP block cipher construction that is secure against related-key attacks (with respect to some set of related keys) built from a tweakable SPRP, which is the most efficient to date. We have also improved a bound for the PRF-RKA/PRP-RKA switching proposition, which provides a tighter security bound for constructing PRP-RKA ciphers from PRF of a certain form. Furthermore, we have presented several key recovery attacks on all known PRP-RKA secure ciphers. Finally, we have defined various RKA security notions and showed their relations. The results obtained from this paper can stimulate the design and analysis of SPRP or PRP constructions that are secure against related-key attacks, and of a broader perspective stimulate the study of provable security of block ciphers.

Acknowledgements We thank Bart Preneel for his helpful comments. Also we thank anonymous referees for their constructive comments.

References

1. M. Bellare, A. Desai, E. Jokipii and P. Rogaway, *A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation*, Proceedings of the 38th Symposium on Foundations of Computer Science (FOCS), IEEE, 1997. The revised version is available at *http://www-cse.ucsd.edu/users/mihir*.
2. M. Bellare, J. Kilian and P. Rogaway, *The Security of the Cipher Block Chaining message authentication code*, Journal of Computer and System Sciences, Vol. 61, No. 3, pp. 362-399, 2000.
3. M. Bellare and T. Kohno, *A Theoretical Treatment of Related-Key Attacks : RKA-PRPs, RKA-PRFs, and Applications*, Advances in Cryptology – EUROCRYPT 2003, LNCS 2654, Springer-Verlag, pp. 491-506, 2003, Full version is available at *http://www.cs.ucsd.edu/users/tkohno/papers/RKA*.
4. E. Biham, *New Types of Cryptanalytic Attack Using Related Keys*, Advances in Cryptology – EUROCRYPT 1993, LNCS 765, pp. 398-409, Springer-Verlag, 1994.
5. E. Biham, O. Dunkelman and N. Keller, *Related-Key Boomerang and Rectangle Attacks*, Advances in Cryptology – EUROCRYPT 2005, LNCS 3494, pp. 507-525, Springer-Verlag, 2005.
6. E. Biham, O. Dunkelman and N. Keller, *Related-Key Rectangle Attack on the Full KA-SUMI*, Advances in Cryptology – ASIACRYPT 2005, LNCS 3788, pp. 443-461, Springer-Verlag, 2005.
7. E. Biham, O. Dunkelman and N. Keller, *New Cryptanalytic Results on IDEA*, Advances in Cryptology – ASIACRYPT 2006, LNCS 4284, pp. 412-427, Springer-Verlag, 2006.
8. E. Biham, O. Dunkelman and N. Keller, *A Simple Related-Key Attack on the Full SHACAL-1*, Topics in Cryptology – CT-RSA 2007, LNCS 4377, pp. 20-30, Springer-Verlag, 2007.
9. E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*. Journal of Cryptology, Vol. 4, No. 1, pp. 3-72, 1991.
10. A. Biryukov and D. Wagner, *Advanced Slide Attacks*, Advances in Cryptology – EUROCRYPT 2000, LNCS 1807, pp. 589-606, Springer-Verlag, 2000.
11. J. Choi, J. Kim, J. Sung, S. Lee and J. Lim, *Related-Key and Meet-in-the-Middle Attacks on Triple-DES and DES-EXE*, Proceedings of Information Security and Hiding (ISH 2005), in conjunction with the International Conference on Computational Science and Its Applications (ICCSA 2005), LNCS 3481, pp. 567-576, Springer, 2005.
12. S. Halevi, *EME* : Extending EME to Handle Arbitrary-length Messages with Associated Data*, 2004. Progress in Cryptology – INDOCRYPT 2004, LNCS 3348, pp. 315-327, Springer-Verlag, 2004. Available at the ePrint archive, *http://eprint.iacr.org/2004/125/*.
13. S. Halevi and P. Rogaway, *A Tweakable Enciphering Mode*, Advances in Cryptology – CRYPTO 2003, LNCS 2729, Springer-Verlag, pp. 482-499, 2003.

14. S. Halevi and P. Rogaway, *A Parallelizable Enciphering Mode*, Topics in Cryptology – CT-RSA 2004, LNCS 2964, Springer-Verlag, pp. 292-304, 2004, Full version is available at the ePrint archive, *http://eprint.iacr.org/2003/147/*.
15. P. Hawkes, *Differential-Linear Weak-Key Classes of IDEA*, Advances in Cryptology – EUROCRYPT 1998, LNCS 1403, pp. 112-126, Springer-Verlag, 1998.
16. M.E. Hellman, E.D. Karnin and J.M. Reyneri, *On the Necessity of Exhaustive Search for System-Invariant Cryptanalysis*, Advances in Cryptology – A Report on CRYPTO 1981, U.C. Santa Barbara, Dept. of Elec. and Computer Eng., ECE Report No 82-04, pp. 2-6, 1982.
17. T. Iwata and K. Kurosawa, *OMAC: One-Key CBC MAC*, Proceedings of Fast Software Encryption (FSE 2003), LNCS 2887, Springer-Verlag, pp. 129-153, 2003.
18. G. Jakimoski and Y. Desmedt, *Related-Key Differential Cryptanalysis of 192-bit Key AES Variants*, Proceedings of Selected Areas in Cryptography (SAC 2003), LNCS 3006, Springer-Verlag, pp. 208-221, 2003.
19. J. Kelsey, B. Schneier and D. Wagner, *Key-schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES*, Advances in Cryptology – CRYPTO 1996, LNCS 1109, Springer-Verlag, pp. 237-251, 1996.
20. J. Kelsey, B. Schneier and D. Wagner, *Related-key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA*, Proceedings of Information and Communications Security (ICICS 1997), LNCS 1334, Springer-Verlag, pp. 233-246, 1997.
21. J. Kilian and P. Rogaway, *How to Protect DES against Exhaustive Key Search (an analysis of DESX)*. Journal of Cryptology, Vol. 14, No. 1, pp. 17-35, 2001.
22. J. Kim, G. Kim, S. Hong, S. Lee and D. Hong, *The Related-Key Rectangle Attack - Application to SHACAL-1*, Proceedings of Information Security and Privacy (ACISP 2004), LNCS 3108, Springer-Verlag, pp. 123-136, 2004.
23. J. Kim, G. Kim, S. Lee, J. Lim and J. Song, *Related-Key Attacks on Reduced Rounds of SHACAL-2*, Progress in Cryptology – INDOCRYPT 2004, LNCS 3348, Springer-Verlag, pp. 175-189, 2004.
24. J. Kim, S. Hong and B. Preneel, *Related-Key Rectangle Attacks on Reduced AES-192 and AES-256*, Proceedings of Fast Software Encryption (FSE 2007), LNCS 4593, Springer-Verlag, pp. 225-241, 2007.
25. L.R. Knudsen, *Cryptanalysis of LOKI91*, Advances in Cryptology – AUSCRYPT 1992, LNCS 718, Springer-Verlag, pp. 196-208, 1993.
26. Y. Ko, S. Hong, W. Lee, S. Lee and J. Kang, *Related Key Differential Attacks on 26 Rounds of XTEA and Full Rounds of GOST*, Proceedings of Fast Software Encryption (FSE 2004), LNCS 3017, Springer-Verlag, pp. 299-316, 2004.
27. M. Liskov, R.L. Rivest and D. Wagner, *Tweakable Block Ciphers*, Advances in Cryptology – CRYPTO 2002, LNCS 2442, Springer-Verlag, pp. 31-46, 2002.
28. M. Luby and C. Rackoff, *How to Construct Pseudorandom Permutations from Peudorandom Functions*, SIAM J. Computation, Vol. 17, No. 2, 1988.
29. S. Lucks, *Ciphers Secure against Related-Key Attacks*, Proceedings of Fast Software Encryption (FSE 2004), LNCS 3017, Springer-Verlag, pp. 359-370, 2004.
30. S. Murphy and M.J.B. Robshaw, *Key-Dependent S-Boxes and Differential Cryptanalysis*. Design, Codes and Cryptography, Vol. 27, No. 3, pp. 229-255, 2002.
31. M. Naor and O. Reingold, *On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisted*, Journal of Cryptology, Vol. 12, No. 1, pp. 29-66, 1999.
32. R.C.-W., Phan, *Related-Key Attacks on Triple-DES and DESX Variants*, Topics in Cryptology – CT-RSA 2004, LNCS 2964, pp. 15-24, Springer-Verlag, 2004.
33. R.C.-W. Phan and H. Handschuh, *On Related-Key and Collision Attacks: the Case for the IBM 4758 Cryptoprocessor*, Proceedings of Information Security (ISC 2004), LNCS 3225, pp. 111-122, Springer-Verlag, 2004.
34. E. Razali and R.C.-W. Phan, *On the Existence of Related-Key Oracles in Cryptosystems Based on Block Ciphers*, On the Move to Meaningful Internet Systems 2006: OTM 2006, LNCS 4277, pp. 425-438, Springer-Verlag, 2006.
35. E. Razali, R.C.-W. Phan and M. Joye, *On the Notions of PRP-RKA, KR and KR-RKA for Block Ciphers*, Proceedings of Provable Security (ProvSec 2007), LNCS 4784, pp. 188-197, Springer-Verlag, 2007.
36. S. Vaudenay, *Decorrelation: A Theory for Block Cipher Security*, Journal of Cryptology, Vol. 16, No. 4, pp. 249-286, 2003.
37. D. Wagner, *Towards a Unifying View of Block Cipher Cryptanalysis*, Proceedings of Fast Software Encryption (FSE 2004), LNCS 3014, Springer-Verlag, pp. 16-33, 2004.
38. R. S. Winternitz and M. E Hellman, *Chosen-Key Attacks on a Block Cipher*, Cryptologia, Vol. 11, No. 1, pp. 16-20, 1987.

A Theorem 2 of [27]

Let $E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ be a permutation family, let $\mathcal{H} : \mathcal{T} \to \mathcal{D}$ be an ϵ-AXU_2 family with $\epsilon \geq 1/|\mathcal{D}|$ and let $E' : (\mathcal{K} \times \mathcal{T} \times \mathcal{H}) \times \mathcal{D} \to \mathcal{D}$ be another permutation family defined as $E'_{K,T,h}(M) = E_K(M \oplus h(T)) \oplus h(T)$ where (K, h) is a secret key in $\mathcal{K} \times \mathcal{H}$, T is a tweak in $\mathcal{T}$ and M is a message in $\mathcal{D}$. If E is a secure SPRP and $\mathcal{H}$ is ϵ-AXU_2 where ϵ is negligible, then E' is a secure TWEAK-SPRP. Formally, given a TWEAK-SPRP adversary $\mathcal{A}$ attacking E' that queries its oracles with at most q queries, we can construct a SPRP adversary $\mathcal{B}_\mathcal{A}$ attacking E such that

$$\mathbf{Adv}^{\text{tweak-sprp}}_{E'}(\mathcal{A}) \leq \mathbf{Adv}^{\text{sprp}}_{E}(\mathcal{B}_\mathcal{A}) + 3\epsilon q^2$$

and $\mathcal{B}_\mathcal{A}$ takes the same amount of time and makes the same number of oracle queries as $\mathcal{A}$.