Published in J.K. Liu and W. Susilo, Eds., *Provable Security − ProvSec 2007*, vol. 4784 of *Lecture Notes in Computer Science*, pp. 188–197, Springer, 2007.

On the Notions of PRP-RKA, KR and KR-RKA for Block Ciphers

Ermaliza Razali[1], Raphael C.-W. Phan[2], and Marc Joye[3]

[1] Information Security Research (iSECURES) Lab
Swinburne University of Technology, Sarawak campus, Kuching, Malaysia
erazali@swinburne.edu.my
[2] Laboratoire de sécurité et de cryptographie, EPFL
Station 14 - Building INF, 1015 Lausanne, Switzerland
raphael.phan@epfl.ch
[3] Thomson R&D France
Technology Group, Corporate Research, Security Laboratory
1 avenue de Belle Fontaine, 35576 Cesson-Sévigné Cedex, France
marc.joye@thomson.net

Abstract. Security of commonly used block ciphers is commonly measured in terms of their resistance to known attacks. While the provable security approach to block ciphers dates back to the first CRYPTO conference (1981), analysis of modern block cipher proposals typically do not benefit fully from this, except for a few cases. This paper considers the security of recently proposed PRP-RKA secure block ciphers and discusses how they relate to existing types of attacks on block ciphers.

Keywords: Provable security, pseudorandom permutation (PRP), key recovery (KR), block cipher, related key attacks (RKA).

1 Introduction

The right approach to analyzing the security of public-key encryption schemes and protocols is by reduction, in a given security model, to an underlying hard problem: the so-called the provable security approach. In the symmetric-key setting, while formal definitions of security do exist (e.g., Luby and Rackoff), security of a modern block cipher is often measured by its resistance to known attacks. Thus, from the perspective of the provable security community, the security of modern block ciphers may seem heuristic.

This paper considers the formal provable security approach to analyzing block ciphers. The advantage is clear. Security of a block cipher can be proved in a generic sense, by specifying bounds on the adversary's resources, without assuming the exact approach taken by the adversary. It encompasses all possible attacks mountable by the adversary given those resources. This compares favorably with the heuristic case where a primitive is designed to resist some list of attacks but may later fall to attacks not considered by the designer. Historically, building on work by Luby and Rackoff, the provable security of block ciphers have been analyzed with respect to the notion of pseudorandomness (PRP). This is advantageous since PRP implies security against key recovery (KR).

Except for a few cases (e.g., [8, 1, 11, 12, 9]), we are however not aware of any work that analyzes the security of modern block ciphers in the context of PRP. We also note that the assumption that the underlying block cipher is a PRP was used in the security analysis of CBC-MAC [2]. To the best of our knowledge, the earliest result on provable security analysis of block ciphers is by Hellman *et al.* [5]. In particular, the security was formalized in the ideal cipher model (a.k.a. Shannon model or black-box model) and in terms of an adversary winning a key-recovery game. The formalization of the security of block ciphers against related-key attacks in fact dates back to the work of Winternitz and Hellman [15], also considered in the context of a key-recovery game in the ideal cipher model, but here in the presence of related-key oracles. The first known block cipher with a provable security proof of pseudorandomness (PRP) is DESX [8].

Since the bulk of block cipher analysis is dedicated to key-recovery attacks, it is sensible to formally cast these PRP-RKA ciphers also in the context of resistance to key-recovery attacks in the presence of related-key oracles (KR-RKA) or not (KR). Interestingly, doing so brings us back to where it started, since the first results [5, 15] on provable security of block ciphers were in the context of KR and KR-RKA.

The rest of this paper is organized as follows. In the next section, we introduce some notation and review different security notions for block ciphers. Section 3 is the core of our paper. We describe several key recovery attacks on some PRP-RKA secure ciphers and relate the corresponding success probability with the security bound derived from a generic attacker. Finally, we conclude in Section 4.

2 Definitions

Consider a family of functions $F : \mathbb{K} \times \mathbb{D} \to \mathbb{R}$, where $\mathbb{K} = \{0,1\}^k$ is the set of keys of F, $\mathbb{D} = \{0,1\}^l$ is the domain of F and $\mathbb{R} = \{0,1\}^L$ is the range of F, and where k, l and L are the key, input and output lengths in bits. We use $F_K(\mathbb{D})$ as a shorthand for $F(K, \mathbb{D})$. By $K \overset{\$}{\leftarrow} \mathbb{K}$, we denote the operation of selecting a string K at random from $\mathbb{K}$. Similar notations apply for a family of permutations $E : \mathbb{K} \times \mathbb{D} \to \mathbb{D}$, where $\mathbb{K} = \{0,1\}^k$ is the set of keys of E and $\mathbb{D} = \{0,1\}^l$ is the domain and range of E.

2.1 Related Keys

The *related-key-deriving* (RKD) function $\phi \in \Phi$ is a map $\phi : \mathbb{K} \to \mathbb{K}$, where Φ is a subset of functions mapping $\mathbb{K}$ to $\mathbb{K}$. Given F and $K \in \mathbb{K}$, the *related-key oracle* $F_{\mathrm{RK}(K,\cdot)}(\cdot)$ takes two arguments: a function $\phi : \mathbb{K} \to \mathbb{K}$ and an element $P \in \mathbb{D}$, and returns $F_{\phi(K)}(P)$, where $\mathrm{RK}(K, \phi) = \phi(K)$. An attack exploiting access to the oracle $F_{\mathrm{RK}(K,\phi)}(\cdot)$ where $\phi \in \Phi$ is called a Φ-restricted related-key attack (RKA). Similar definitions apply for E.

2.2 Security Notions

Suppose that $E : \mathbb{K} \times \mathbb{D} \rightarrow \mathbb{D}$ is a family of permutations on $\mathbb{D}$. A PRP adversary $\mathcal{A}$ gets access to an oracle, which, on input $P \in \mathbb{D}$, either returns $E_K(P)$ for a random key $K \in \mathbb{K}$ or returns $G(P)$ for a random permutation G on $\mathbb{D}$. The goal of $\mathcal{A}$ is to guess the type of oracle it has — by convention, $\mathcal{A}$ returns 1 if it thinks that the oracle is computing $E_K(\cdot)$. The adversary's advantage is defined by:

$$\mathbf{Adv}_E^{\mathsf{PRP}}(\mathcal{A}) = \Pr\big[K \overset{\$}{\leftarrow} \mathbb{K} : \mathcal{A}^{E_K(\cdot)} = 1\big] - \Pr\big[G \overset{\$}{\leftarrow} \mathrm{Perm}(\mathbb{D}) : \mathcal{A}^{G(\cdot)} = 1\big] \ .$$

E is said PRP-secure if $\mathbf{Adv}_E^{\mathsf{PRP}}(\mathcal{A})$ is sufficiently small.

Extension of this to include RKAs allows the PRP-RKA adversary $\mathcal{A}$ to make related-key oracle queries of the form (ϕ, P) for a related-key deriving function $\phi : \mathbb{K} \rightarrow \mathbb{K}$, $\phi \in \Phi$, and $P \in \mathbb{D}$. We so have:

$$\begin{aligned}\mathbf{Adv}_{\Phi,E}^{\mathsf{PRP-RKA}}(\mathcal{A}) = {} & \Pr\big[K \overset{\$}{\leftarrow} \mathbb{K} : \mathcal{A}^{E_{\mathsf{RK}(\cdot,K)}(\cdot)} = 1\big] \\ & - \Pr\big[K \overset{\$}{\leftarrow} \mathbb{K}; G \overset{\$}{\leftarrow} \mathrm{Perm}(\mathbb{K}, \mathbb{D}) : \mathcal{A}^{G_{\mathsf{RK}(\cdot,K)}(\cdot)} = 1\big] \ .\end{aligned}$$

When the inverse of E is available, security under chosen-ciphertext (related-key) attacks (namely, PRP-CCA or PRP-CCRKA) can be similarly defined:

$$\begin{aligned}\mathbf{Adv}_E^{\mathsf{PRP-CCA}}(\mathcal{A}) = {} & \Pr\big[K \overset{\$}{\leftarrow} \mathbb{K} : \mathcal{A}^{E_K(\cdot), E_K^{-1}(\cdot)} = 1\big] \\ & - \Pr\big[G \overset{\$}{\leftarrow} \mathrm{Perm}(\mathbb{D}) : \mathcal{A}^{G(\cdot), G^{-1}(\cdot)} = 1\big]\end{aligned}$$

and

$$\begin{aligned}\mathbf{Adv}_{\Phi,E}^{\mathsf{PRP-CCRKA}}(\mathcal{A}) = {} & \Pr\big[K \overset{\$}{\leftarrow} \mathbb{K} : \mathcal{A}^{E_{\mathsf{RK}(\cdot,K)}(\cdot), E^{-1}_{\mathsf{RK}(\cdot,K)}(\cdot)} = 1\big] \\ & - \Pr\big[K \overset{\$}{\leftarrow} \mathbb{K}; G \overset{\$}{\leftarrow} \mathrm{Perm}(\mathbb{K}, \mathbb{D}) : \mathcal{A}^{G_{\mathsf{RK}(\cdot,K)}(\cdot), G^{-1}_{\mathsf{RK}(\cdot,K)}(\cdot)} = 1\big] \ .\end{aligned}$$

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

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

where $C_i = E_K(P_i)$ for $1 \leq i \leq p$. 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 $\langle P_i, C_i\rangle \in \mathcal{L}$, $E_{\hat{K}}(P_i) = C_i$. We let $\mathrm{Cons}_E(\mathcal{L})$ denote the set of all keys consistent with $\mathcal{L}$. The advantage of KR adversary $\mathcal{A}$ is then given by:

$$\mathbf{Adv}_E^{\mathsf{KR}}(\mathcal{A}) = \Pr\Big[K \overset{\$}{\leftarrow} \mathbb{K}; \mathcal{L} \leftarrow \big\{\langle P_i, E_K(P_i)\rangle\big\} : \mathcal{A}^{\mathcal{L}} = \hat{K} \in \mathrm{Cons}_E(\mathcal{L})\Big] \ .$$

E is KR-secure if $\mathbf{Adv}_E^{\mathsf{KR}}(\mathcal{A})$ is sufficiently small. Again, this can be extended to include RKAs:

$$\begin{aligned}\mathbf{Adv}_{\Phi,E}^{\mathsf{KR-RKA}}(\mathcal{A}) = \Pr\Big[& K \overset{\$}{\leftarrow} \mathbb{K}; \mathcal{L} \leftarrow \big\{\langle P_i, E_K(P_i)\rangle\big\} : \\ & \mathcal{A}^{\mathcal{L}, E_{\mathsf{RK}(\cdot,K)}(\cdot)} = \hat{K} \in \mathrm{Cons}_E(\mathcal{L})\Big] \ .\end{aligned}$$

3 Security of Existing PRP-RKA Block Ciphers

In [5], it was shown that the advantage $\mathbf{Adv}_E^{\mathsf{KR}}(\mathcal{A})$ 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 $E_{K_i}(P_i)$ for any text P_i and any key K_i of the adversary's choice), and on the key bit-length k. More specifically, it was shown that:

$$\mathbf{Adv}_E^{\mathsf{KR}}(\mathcal{A}) \leq \frac{t}{2^k} + \frac{1}{2^k - t} \enspace .$$

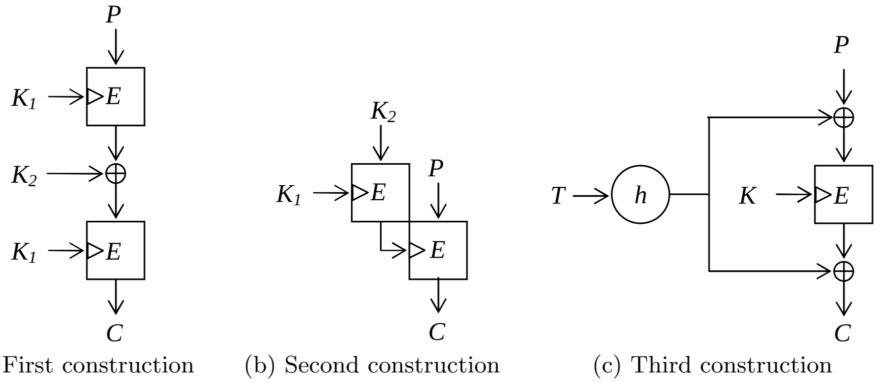
This bounds the advantage of a generic adversary. We see that both terms on the right side of the inequality remain small as long as $t \ll 2^k$. As t relates to an exhaustive key search, this means that a generic adversary must exhaust a significant fraction of key candidates to have a reasonable chance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

Similarly, in [15], it was shown that the advantage $\mathbf{Adv}_{\Phi,E}^{\mathsf{KR-RKA}}(\mathcal{A})$ of any KR-RKA adversary $\mathcal{A}$ mounting a generic related-key attack is bounded by:

$$\mathbf{Adv}_{\Phi,E}^{\mathsf{KR-RKA}}(\mathcal{A}) \leq \frac{mt}{2^k} + \frac{1}{2^k} \enspace ,$$

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 $mt \ll 2^k$.

In the sequel, we analyze and discuss the security of the constructions depicted on Fig. 1.



(a) First construction (b) Second construction (c) Third construction

Fig. 1. Block-cipher based constructs.

3.1 First Construction

In [1], 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 [13] structure (see Fig. 1-a). In particular, they proved:

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

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

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

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

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 [6, 7, 14] where no such restriction is made.

With DES-EXE like structures, one may wonder if existing attacks [13, 4] 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 similar effort.

MITM Attack.

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

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

   and check whether $S_1 = S_2$.
   (b) If so, let $\hat{K}_2 = E^{-1}_{\hat{K}_1}(C) \oplus E_{\hat{K}_1}(P)$ 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 [5], when considering a generic adversary, any block cipher E' of key length $k+l$ bits is expected to provide the following security bound:

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

where t denotes the number of verifications. A closer look at the proof offered in [5] shows that if the generic adversary makes verifications with distinct key candidates then the bound can be sharpened as:

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

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:

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

Interestingly, we observe that

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

and so the block-cipher based construct of Fig. 1-a does not give the best possible security against key recovery.

Differential RKA Attack (DRKA).

1. Let $\langle P, C\rangle$ be any pairs of plaintext/ciphertext in $\mathcal{L}$ with $C = E'_{K_1\|K_2}(P)$.
2. Query the related-key oracle with (P', Δ) and obtain the pair (P', C') with $C' = E'_{K_1\|K_2\oplus\Delta}(P)$.
3. For each key guess, $\hat{K}_1 \in \{0,1\}^k$, do the following.
   (a) Check whether
   $$E_{\hat{K}_1}^{-1}(C) \oplus E_{\hat{K}_1}^{-1}(C') = \Delta \ .$$
   (b) If so, let $\hat{K}_2 = E_{\hat{K}_1}^{-1}(C) \oplus E_{\hat{K}_1}(P)$ 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 [15], 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:

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

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

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

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.

3.2 Second Construction

Lucks [11] argued that Theorem 1 only applies for large l. For practical values of l, one may have that $\mathbf{Adv}_{\Phi,E'}^{\mathsf{PRP-RKA}}(\mathcal{A}) - \mathbf{Adv}_{E}^{\mathsf{PRP}}(\mathcal{B}_{\mathcal{A}})$ is not small. He therefore considered a construction that yields more meaningful security bound. See Fig. 1-b.

Theorem 2 (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*

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

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

$$\frac{\mathbf{Adv}_{\Phi,E''}^{\mathsf{PRP-RKA}}(\mathcal{A})}{r+1} \le \mathbf{Adv}_{E}^{\mathsf{PRP}}(\mathcal{B}_{\mathcal{A}}) \ .$$

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 P, i.e., $C = E_{E_{K_1}(K_2)}(P)$. 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 P, which leads to a total break. For an attacker performing an exhaustive search (XS) on $\widetilde{K}$, we have

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

where t denotes the number of guessed keys. This has to be compared with the security bound given by a generic KR adversary against a $2l$-bit key cipher E'':

$$\mathbf{Adv}_{E''}^{\mathsf{KR}}(\mathcal{A}) \le \frac{t}{2^{2l}} + \frac{1}{2^{2l} - t} \ .$$

We see that the above XS attacker has a substantially larger success probability.

3.3 Third Construction

Kim *et al.* [9] analyzed another block-cipher based construct. See Fig. 1-c. It is more efficient than the two previous ones as it only requires a single call to the underlying E.

Theorem 3 (Kim *et al.*). *Let $E : \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^l$ be a block cipher and let $\mathcal{H} : \{0,1\}^t \rightarrow \{0,1\}^l$ be an ϵ-almost 2-xor universal (ϵ-AXU$_2$) family with $\epsilon \geq \frac{1}{2^l}$. Let $E''' : \{0,1\}^{k+t} \times \mathcal{H} \times \{0,1\}^l \rightarrow \{0,1\}^l$ be the block cipher defined as*

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

where K is k bits long and T is t bits long. Let Φ be any set of RKD functions over $\{0,1\}^{k+t}$ that modify only T and that are independent of K. Then, for any adversary $\mathcal{A}$ against E''' that queries its oracles with at most q queries, we can construct a chosen-ciphertext adversary $\mathcal{B}_{\mathcal{A}}$ against E such that

$$\mathbf{Adv}^{\mathsf{PRP-CCRKA}}_{\Phi,E'''}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{PRP-CCA}}_{E}(\mathcal{B}_{\mathcal{A}}) + 3\epsilon\, q^2$$

and $\mathcal{B}_{\mathcal{A}}$ makes the same number of oracle queries and runs in the same running time as $\mathcal{A}$. □

Recall that DESX [8] is defined as:

$$\text{DESX}(P, K_1\|K\|K_2) = K_2 \oplus E_K(P \oplus K_1)$$

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 the above construction is like DESX [8] 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:

$$K_1 = K_2 = h(T) \ .$$

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 $|K| + |h(T)|$.

There is a restriction attached to this construction as well. Namely, the key K to $E_K(\cdot)$ cannot be varied by an RKA adversary; only T is allowed to vary.

An advanced slide attack [3] was applied to DESX. It is basically a MITM attack. We show that a variant also applies here.

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

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

which yields

$$h(T) \oplus P \oplus P' = E_K^{-1}(C) \oplus P = E_K^{-1}(C') \oplus P' \ .$$

Based on this, we can mount the following attack.

1. Let $\mathcal{L} = \langle P_i, C_i \rangle_{1 \le i \le p}$ be a list of p known pairs of plaintext/ciphertext with, $C_i = E'''_{K\|T,h}(P_i)$.
2. For each key guess, $\hat{K} \in \{0,1\}^k$, do the following.
   (a) For each $1 \le i \le p$, evaluate $E^{-1}_{\hat{K}}(C_i) \oplus P_i$ and insert
   $$\langle E^{-1}_{\hat{K}}(C_i) \oplus P_i, i \rangle$$
   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, $E^{-1}_{\hat{K}}(C_i) \oplus P_i = E^{-1}_{\hat{K}}(C_j) \oplus P_j$, let $h(\hat{T}) = C_i \oplus C_j$ and validate the guessed key $\hat{K}\|\hat{T}$ on all pairs of $\mathcal{L}$.
3. If the guessed key is validated, return (the consistent key) $\hat{K}\|\hat{T}$.

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

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

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

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

Resistance against RKA. On the positive side, it appears that the construction of Fig. 1-c seems to resist differential RKAs since the key K to the inner E_K is not allowed to vary and although T is allowed to vary, the actual key difference due to $h(T)$ cannot be predicted.

4 Concluding Remarks

We have discussed key recovery attacks on some recent proposals to construct a block cipher secure in the sense of PRP-RKA from a block cipher (not necessarily secure against related-key attacks). Our results emphasize that known constructions specifically designed for provable security against related-key attacks do not have optimal key-recovery resilience.

Furthermore, all PRP-RKA secure constructions proposed so far do not allow the key component of the underlying cipher E to be varied. An open problem is to prove (or disprove) the existence of PRP-RKA secure constructions allowing this.

Acknowledgments. We would like to thank Jongsung Kim for sending a copy of [9]. We are also grateful to the anonymous referees for useful comments.

References

1. Bellare, M., and Kohno, T. A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In *Advances in Cryptology − EUROCRYPT 2003*, LNCS 2656, pp. 491–506, Springer, 2003. Full version available at `http://www-cse.ucsd.edu/users/mihir/papers/rka.html`.
2. Bellare, M., Kilian, J., and Rogaway, P. The security of the cipher block chaining message authentication code. *J. Comput. Syst. Sci.* **61**(3):362–399, 2000.
3. Biryukov, A., and Wagner, D. Advanced slide attacks. In *Advances in Cryptology − EUROCRYPT 2000*, LNCS 1807, pp. 589–606, Springer, 2000.
4. Choi, J., Kim, J., Sung, J., Lee, S., and Lim, J. Related-key and meet-in-the-middle attacks on Triple-DES and DES-EXE. In *Computational Science and Its Applications − ICCSA 2005*, LNCS 3481, pp. 567–576, Springer, 2005.
5. Hellman, M. E., Karnin, E. D., and Reyneri, J. M. On the necessity of exhaustive search for system-invariant cryptanalysis. In *Advances in Cryptology − A Report on CRYPTO '81*, U.C. Santa Barbara, Dept. of Elec. and Computer Eng., ECE Report No 82-04, pp. 2–6, 1982.
6. Kelsey, J., Schneier, B., and Wagner, D. Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In *Advances in Cryptology − CRYPTO '96*, LNCS 1109, pp. 237–251, Springer, 1996.
7. Kelsey, J., Schneier, B., and Wagner, D. Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA. In *Information and Communication Security (ICICS '97)*, LNCS 1334, pp. 233–246, Springer, 1997.
8. Kilian, J., and Rogaway, P. How to protect DES against exhaustive key search (an analysis of DESX). *J. Cryptology* **14**(1):17–35,2001.
9. Kim, J., Sung, J., Lee, S., and Preneel, B. Pseudorandom permutation and function families secure against related-key attacks. Unpublished manuscript.
10. Liskov, M., Rivest, R. L., and Wagner, D.. Tweakable block ciphers. In *Advances in Cryptology − CRYPTO 2002*, LNCS 2442, pp. 31–46, Springer, 2002.
11. Lucks, S. Ciphers secure against related-key attacks. In *Fast Software Encryption − FSE 2004*, LNCS 3017, pp. 359–370, Springer, 2004.
12. Phan, D. H., and Pointcheval, D. About the security of ciphers (semantic security and pseudo-random permutations). In *Selected Areas in Cryptography − SAC 2004*, LNCS 3357, pp. 182–197, Springer, 2004.
13. Phan, R. C.-W. Related-key attacks on triple-DES and DESX variants. In *Topics in Cryptology −CT-RSA 2004*, LNCS 2964, pp. 15–24, Springer, 2004.
14. Razali, E., and Phan, R. C.-W. On the existence of related-key oracles in cryptosystems based on block ciphers. In *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, LNCS 4277, pp. 425–438, Springer, 2006.
15. Winternitz, R. S., and Hellman, M. E. Chosen-key attacks on a block cipher. *Cryptologia* **11**(1):16–20, 1987.