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, 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, France
marc.joye@thomson.net

Abstract. Security of a modern block cipher is commonly measured in terms of its 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 besides the proof of security for DESX by Kilian and Rogaway, and recent work on the notions of PRP-RKA initiated by Bellare and Kohno. We consider the security of recently proposed PRP-RKA secure block ciphers. We discuss implications of the proven theorems and how they relate to existing types of attacks on block ciphers. Our results are the first known cryptanalysis of these provably secure ciphers.

Keywords: pseudorandom permutation, provable security, cipher, key recovery.

1 Introduction

The right approach to analyzing the security of public-key encryption schemes and protocols is by reduction to an underlying hard problem, so called the provable security approach. In the symmetric-key setting, while provable security results do exist e.g. Luby and Rackoff, security of a modern block cipher is often gauged by its resistance to known attacks. Thus, from the perspective of the provable security community, a block cipher's security may seem heuristic. However, in the context of symmetric encryption schemes where the plaintext is of arbitrary length, security is indeed shown by the reduction approach e.g. see the NIST recommended modes which all come with this kind of proof.

This paper considers the formal provable security approach to analyzing block ciphers. The advantage is clear. Security of a block cipher can be proven in the generic sense, by specifying bounds on the adversary's resources, without assuming the type of approach taken by an adversary. It captures all possible attacks mountable by the adversary given those resources. This compares favourably to 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

performed with respect to the notion of pseudorandomness (PRP). This is advantageous since PRP implies security against key-recovery attacks. Except for [7, 1, 9, 10, 8], we are however not aware of any work that analyzes the security of modern block ciphers in the context of PRP; although the assumption that a block cipher is PRP was used in the security of CBC-MAC.

Background. To the best of our knowledge, the earliest provable security analysis of block ciphers is by Hellman *et al.* [4] where it was shown that any general cryptanalytic attack is equivalent to exhaustive key search. In particular, the security notion was defined in the ideal cipher model (a.k.a. Shannon model or black box model) and in terms of the adversary winning a key-recovery game. We denote this as the KR game. Meanwhile, formalizing the security of block ciphers against related-key attacks in fact dates back to the work of Winternitz and Hellman [13] where it was also considered in the context of a key-recovery game in the ideal cipher model, but here the adversary has access to related-key oracles. We denote this as the KR-RKA game. The first known block cipher with a provable security proof of pseudorandomness (PRP) is DESX [7]. The proof took key-recovery attacks into account. To be precise, it was shown that for a $k + 2n$-bit key $K = \langle K_1, K_2, K_3 \rangle$ where $K_1, K_3 \in \{0,1\}^n$ and $K_2 \in \{0,1\}^k$, the PRP advantage of an adversary A against DESX is upper bounded as

$$\mathbf{Adv}^{\mathsf{PRP}}_{DESX}(A) \leq \frac{2mt}{2^{k+n}},$$

where m is the number of chosen plaintext-ciphertext queries and t is the number of computations of the underlying block cipher E. Note that the ideal cipher model allows the adversary unbounded [4, 7] computational resources.

A provable security proof guarantees nothing more than what it claims. We will see that in the context of the PRP-RKA proofs of the block ciphers in [1, 9, 8], pseudorandomness of a given PRP-RKA block cipher E' is only claimed up to the pseudorandomness (PRP) of the underlying block cipher E. This is in fact a minimalist requirement, since it basically says that at the worst case, the security (with respect to pseudorandomness) of E' should be at least the security of the underlying E. To be precise, the proofs are not meant to say anything about the security of E' against key-recovery attacks although it is often expected that if a cipher is PRP secure it should also be KR secure [7].

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 when related-key oracles are either available (KR-RKA) or not available (KR). Interestingly, doing so brings us back to where it started, since the first results [4, 13] on provable security of block ciphers were in the context of KR and KR-RKA.

Our results. We first revisit the security notions of KR and KR-RKA and discuss how key-recovery attacks can be captured in both KR and PRP types of notions. In fact, in this sense both types of notions only differ in the winning goal of the adversary. We demonstrate both non-related-key and related-key attacks on the Bellare-Kohno block cipher, and a non-related-key attack on the Kim *et al.* cipher. All attacks are less than exhaustive key search over the entire key.

Our results are the first known cryptanalysis of PRP-RKA ciphers. To be fair, our attacks do not contradict the security proofs of these ciphers for two reasons. First, the proofs consider the pseudorandomness of a cipher and do not take key-recovery attacks into account. Second, and more importantly, the proofs are minimalist in the sense that they treat the worst case scenario where E' is expected to be at least as secure as the underlying E, otherwise constructing E' from E gives an even weaker cipher than E itself. In the ideal case, we would require something more, i.e. the security of E' should substantially be higher than E. That our results do not contradict the security proofs does not mean our attacks are actually captured by the proofs. Instead, the security proofs do not explicitly capture key-recovery attacks, so our results are incomparable to what is claimed by the proofs. They do however underline that security reductions do not make a scheme secure per se.

2 Definitions

Consider a family of functions $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$ where $\mathcal{K} = \{0,1\}^k$ is the set of keys of F, $\mathcal{D} = \{0,1\}^l$ is the domain of F and $\mathcal{R} = \{0,1\}^L$ is the range of F, where k, l and L are the key, input and output lengths in bits. $F_K(\mathcal{D})$ is shorthand for $F(K,\mathcal{D})$. By $K \xleftarrow{\$} \mathcal{K}$, we denote randomly selecting a string, K from $\mathcal{K}$. Similar notations apply for a family of permutations $E : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{D}$ where $\mathcal{K} = \{0,1\}^k$ is the set of keys of E and $\mathcal{D} = \{0,1\}^l$ is the domain and range of E. The *related-key-deriving* (RKD) function $\phi \in \Phi$ is a map $\phi : \mathcal{K} \rightarrow \mathcal{K}$, where Φ is a subset of functions mapping $\mathcal{K}$ to $\mathcal{K}$. Given F and $K \in \mathcal{K}$, the *related-key oracle* $F_{RK(K,\cdot)}(\cdot)$ takes two arguments: a function $\phi : \mathcal{K} \rightarrow \mathcal{K}$ and an element $P \in \mathcal{D}$, and returns $F_{\phi(K)}(P)$; where $RK(K,\phi) = \phi(K)$. An attack exploiting access to the oracle $F_{RK(K,\phi)}(\cdot)$ where $\phi \in \Phi$ is a Φ-restricted related-key attack (RKA). Similar definitions apply for E.

2.1 Notions of PRP(-RKA) and KR(-RKA)

For a family of permutations E on $\mathcal{D}$, a PRP adversary A gets oracle access to function g, which is a random permutation on $\mathcal{D}$ or a random instance of cipher E_K; A's advantage in telling between the two, over randomly guessing:

$$\begin{aligned}\mathbf{Adv}_E^{\mathsf{PRP}}(A) = \mid & \Pr[K \xleftarrow{\$} \mathcal{K} : A^{E_K(\cdot)} = 1] \\ & - \Pr[K \xleftarrow{\$} \mathcal{K} : G \xleftarrow{\$} \mathrm{Perm}(\mathcal{D}) : A^{G_K(\cdot)} = 1] \mid .\end{aligned}$$

E is PRP-secure if $\mathbf{Adv}_E^{\mathsf{PRP}}(A)$ is negligible.

Extension of this to include RKAs allows the PRP-RKA adversary A access to *related-key oracles* and make queries of the form (ϕ, x) where ϕ denotes a *related-key deriving* function $\phi : \mathcal{K} \rightarrow \mathcal{K}$, $\phi \in \Phi$ and $x \in \mathcal{D}$. When the inverse of g is available, then PRP-(RK)CCA can be similarly defined [1].

In the security notion against key-recovery attacks (KR), adversary A gets oracle access to function g which is a random instance of cipher E_K for a randomly selected key K, and who has to guess K. His advantage is then:

$$\mathbf{Adv}_E^{\mathsf{KR}}(A) = \Pr[K \xleftarrow{\$} \mathcal{K} : A^{E_K(\cdot)} = K].$$

E is secure against key-recovery attacks (KR) if $\mathbf{Adv}_E^{\mathsf{KR}}(A)$ is negligible. Similar extensions can be done for KR-RKA.

3 Security of Existing PRP-RKA Block Ciphers

Key-recovery attacks can be captured into a key-recovery security (KR) or a pseudorandomness (PRP) notion. In [4], it was shown that the advantage $\mathbf{Adv}_E^{\mathsf{KR}}(A)$ of any KR adversary mounting a generic attack is expressed in terms of the number of verifications t for each key guess, thus a function of exhaustive key search:

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

This bounds the adversary's advantage, i.e. it remains negligible as long as $t \ll 2^k$. Thus, the best that can be done is exhaustive key search attack on E.

In [13], it was similarly shown that the advantage $\mathbf{Adv}_{\Phi,E}^{\mathsf{KR\text{-}RKA}}(A)$ of any KR-RKA adversary mounting a generic related-key attack is as follows:

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

where m is the number of text queries to the E oracle.

In [7] it was shown that for a $k{+}2n$-bit key $K = \langle K_1, K_2, K_3 \rangle$ where $K_1, K_3 \in \{0,1\}^n$ and $K_2 \in \{0,1\}^k$, the PRP advantage against DESX is:

$$\mathbf{Adv}_{DESX}^{\mathsf{PRP}}(A) \leq \frac{2mt}{2^{k+n}}.$$

Thus the best a generic adversary can do is exhaustive search over the keyspace of the first or last two key components of K in a meet-in-the-middle style.

3.1 Bellare-Kohno Block Cipher

Bellare and Kohno presented a PRP-RKA secure block cipher that is essentially a generalization of the 2-key variant of DES-EXE [11] structure, i.e. $C = E_{K_1}(E_{K_1}(P) \oplus K_2)$, where the $E_K(\cdot)$ is not DES-EXE but any block cipher. This cipher is in fact the first known block cipher with provable security against RKA. We state the theorem in [1].

Theorem 1 ([1]). *Let $E : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ be a block cipher, $E' : \{0,1\}^{k+l} \times \{0,1\}^l \to \{0,1\}^l$ be the block cipher defined as $E'_{K_1||K_2}(P) = E_{K_1}(E_{K_1}(P) \oplus K_2)$ where K_1 is k-bits 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 if E is secure, E' is secure with respect to Φ-restricted related-key attacks. Formally, for any adversary 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 B_A against E such that*

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

and B_A makes $2rq$ oracle queries and runs same time as 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'.

Note that the security result above provides guarantees that the pseudorandomness of the Bellare-Kohno cipher E' with respect to related-key attacks (PRP-RKA), is only as much as can be obtained in terms of pseudorandomness under non-related-key attacks (PRP) for the underlying regular cipher E. Nothing more is claimed. Indeed, this is the minimal requirement for a provably secure construction, i.e. at the worst case it should still be as secure as its underlying primitive. PRP-RKA security of this cipher as proven in [1, Theorem 1] 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 work [5, 6, 12] where no such restriction is made on the key but that any part of the key is allowed to vary. Since the key K_1 to the underlying cipher E is not allowed to vary, then E will not be subjected to related-key attacks, thus the result in Theorem 1 above is quite intuitive. In fact, this is saying that if we have a cipher E such that we do not wish to allow an adversary to vary the key of E, we construct another cipher E' from E such that we now allow the adversary to vary some part of the key but yet the key to E still cannot be varied. All existing PRP-RKA ciphers use this approach.

With DES-EXE like structure, one wonders if existing attacks [11, 3] on DES-EXE apply to this variant. We answer in the affirmative. First, we give a meet-in-the-middle (MITM) attack that does not require related-key queries, then we give a differential RKA that requires effort slightly less than the first attack.

MITM Attack.

1. Obtain the ciphertexts C, C' of P, P' under key $K = (K_1, K_2)$.
2. Guess all 2^k values of K_1 and compute

$$S_1 = E_{K_1}(P) \oplus E_{K_1}(P') \tag{1}$$
$$S_2 = E^{-1}_{K_1}(C) \oplus E^{-1}_{K_1}(C'). \tag{2}$$

   Check if $S_1 = S_2$. This happens with a probability of 2^{-l}, leaving $2^k \times 2^{-l}$ remaining values of K_1. When $k \leq l$, e.g. for DES-EXE $k = 56, l = 64$, then only the correct value of K_1 remains.
3. Guess all 2^l values of K_2 and do trial encryption on P, P' to check for C, C',

$$E_{K_1}(E_{K_1}(P) \oplus K_2) = C \tag{3}$$
$$E_{K_1}(E_{K_1}(P') \oplus K_2) = C'. \tag{4}$$

   Each equation gives a match with probability 2^{-l}; meaning $2^l \times 2^{-l} \times 2^{-l} \approx 0$ wrong values thus only the correct value of K_2 remains.

Step 1 requires 2 known plaintexts (KPs), Step 2 $2^k \times 4$ encryptions E_K, and Step 3 $2^l \times 4$ encryptions E_K. To summarize, this attack requires 2 KPs, no

memory and $2^2(2^k+2^l)$ encryptions E_K. This is much less effort than exhaustive search of 2^{k+l} encryptions and shows that the 2-key DES-EXE like Bellare-Kohno block cipher is not much better than double encryption e.g. double DES in the sense that it effectively offers security against key-recovery attacks comparable to single encryption. Remark that if we consider a 2-key variant of DESX i.e. $C = E_{K_2}(P \oplus K_1) \oplus K_1$ it fares slightly better (see Section 3.3).

Recalling the results in [4], any block cipher E' of key length $k+l$ bits is expected to provide the following security level:

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

and similarly for any block cipher E of key length k bits, it should be that

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

Interestingly, the above attack shows that for E' it is in fact

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

Thus the Bellare-Kohno cipher is less secure than expected for any block cipher of its key length of $k+l$ bits. Furthermore for this case, we have

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

meaning that $\mathbf{Adv}^{\mathsf{KR}}_{E'}(A)$ matches (within a constant factor of) the upper bound of $\mathbf{Adv}^{\mathsf{KR}}_{E}(A)$. Thus E' with a $k+l$ bit key is not substantially more secure against k-bit key-recovery attacks than its underlying E of only k bits.

Differential RKA Attack.

1. Obtain the ciphertexts C, C' of P, P' under keys $K = (K_1, K_2)$ and $K' = (K_1, K_2 \oplus \triangle)$ respectively.
2. Guess all 2^k values of K_1 and check if

$$E^{-1}_{K_1}(C) \oplus E^{-1}_{K_1}(C') = \triangle, \tag{5}$$

   with a probability of 2^{-l}, leaving $2^k \times 2^{-l}$ remaining values of K_1. When $k \leq l$, i.e. for DES-EXE $k = 56, l = 64$ only the correct value of K_1 remains.
3. Guess all 2^l values of K_2 and do trial encryption on P, P' to check for C, C',

$$E_{K_1}(E_{K_1}(P) \oplus K_2) = C \tag{6}$$
$$E_{K_1}(E_{K_1}(P') \oplus (K_2 \oplus \triangle)) = C'. \tag{7}$$

   Each equation gives a match with probability 2^{-l}; meaning $2^l \times 2^{-l} \times 2^{-l} \approx 0$ wrong values thus only the correct value of K_2 remains.

Step 1 requires 2 related-key known plaintexts (RK-KPs). Step 2 requires $2^k \times 2$ encryptions E_K. Step 3 requires $2^l \times 4$ encryptions E_K. To summarize, this attack requires 2 RK-KPs, no memory and $2 \times 2^k + 4 \times 2^l$ encryptions E_K. This

RKA effort is slightly less than the MITM attack and thus works better on the Bellare-Kohno block cipher. But allowing RKAs does not incur much difference from a MITM attack; the gain is only by a small factor.

Recalling the results in [13], any block cipher E' of key length $k+l$ bits is expected to provide the following security against generic related-key attacks:

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

and similarly for any block cipher E of key length k bits, it should be that

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

Interestingly, the above attack shows that for E' it is in fact

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

This implies that the Bellare-Kohno cipher is less secure than expected for any block cipher of its key length of $k+l$ bits. We also have:

$$\mathbf{Adv}^{\mathsf{KR\text{-}RKA}}_{\Phi,E'}(A) = \frac{t}{2(2^k) + 2^2(2^l)} \simeq \frac{mt}{2^{k}} + \frac{1}{2^{k}},$$

i.e. $\mathbf{Adv}^{\mathsf{KR\text{-}RKA}}_{\Phi,E'}(A)$ matches (within a constant factor of) the upper bound of $\mathbf{Adv}^{\mathsf{KR\text{-}RKA}}_{\Phi,E}(A)$ *and even* $\mathbf{Adv}^{\mathsf{KR}}_{E}(A)$. So E' with a $k+l$ bit key is no more secure against k-bit key-recovery attacks than its underlying E of k bits.

These results show that a block cipher construction like the Bellare-Kohno which was specifically designed for provable security against RKA, does not have optimal key-recovery resilience. This is in fact inherited from its DESX-like structure. Further, one can argue that if in the presence of related-key oracles E' should at least be as secure as E, then in the absence of related-key oracles E' should be substantially more secure than E.

3.2 Lucks Block Cipher

Lucks [9] argued that Theorem 1 in [1] only applies for large l but for practical values of l the PRP-RKA advantage is significantly higher than the PRP advantage. He proposed a construction with a more meaningful security bound.

Theorem 2 ([9]). *Let $E : \{0,1\}^l \times \{0,1\}^l \rightarrow \{0,1\}^l$ be a block cipher. Let $E' : \{0,1\}^{2l} \times \{0,1\}^l \rightarrow \{0,1\}^l$ be the block cipher defined as $E'_{(K_1,K_2)}(P) = E_{E_{K_1}(K_2)}(P)$ where K_1 is l-bits long and K_2 is l-bits long. Let $K^* = \{0,1\}^{2l}$, Φ a collision-free set of partial transformations. A is a Φ-restricted adversary for E'. Count the transformations in A-queries by $r = |\{\phi \in \Phi \mid \exists \text{ query } (\phi,\cdot)\}|$. Then a chosen plaintext adversary B_A for E exists, making no more oracle queries than A, with the same running time as A and the advantage*

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

The encryption of key K_2 is the final secret key to encrypt the plaintext P, i.e. $C = E_{E_{K_1}(K_2)}(P)$. Further, the RKA adversary is only be allowed to vary K_2 and not K_1. Note that although a $2l$-bit key (K_1, K_2) is used, essentially the adversary just needs to recover the final secret key $E_{K_1}(K_2)$ that is used to key the encryption of P, thus effectively the key length is just l bits. The difference with this way to generate the final secret key $E_{K_1}(K_2)$ is that it is no longer easy for the adversary to control the key difference into the encryption of P since this key is the output of a block cipher E. Thus we have

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

security of E' against key-recovery attacks is exactly equal to its underlying E.

3.3 Kim *et al.* Block Cipher

Kim *et al.* [8] gave a provably secure cipher claimed to be the most efficient to date, compared with previous cipher in [1, 9]; efficient in the sense that only one call to the underlying E.

Theorem 3 ([8]). *Let $E : \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^l$ be a block cipher, let $\mathcal{H} : \{0,1\}^t \times \{0,1\}^h \rightarrow \{0,1\}^l$ be an ϵ-almost 2-xor universal (ϵ-AXU_2) family with $\epsilon \geq \frac{1}{|l|}$ and let $E' : \{0,1\}^{k+t+h} \times \{0,1\}^l \rightarrow \{0,1\}^l$ be another permutation family defined as $E'_{K,T,h}(P) = E_K(P \oplus h(T)) \oplus h(T)$ where (K, T, h) is a secret key in $\{0,1\}^k \times \{0,1\}^t \times \{0,1\}^h$, and $P \in \{0,1\}^l$. If E is* PRP-CCA *secure and $\mathcal{H}$ is ϵ-AXU_2 where ϵ is negligible, then E' is a secure* PRP-CCA *with respect to Φ-restricted RKAs* (PRP-CCRKA) *when each function $\phi \in \Phi$ is a partial transformation for which there exists a function $\phi' : \mathcal{T} \rightarrow \mathcal{T}$ such that $\phi(K, T, h) = (K, \phi'(T), h)$. Formally, given a* PRP-CCRKA *adversary A attacking E' that queries its oracles with at most q queries, we can construct a* PRP-CCA *adversary B_A attacking E which takes the same amount of time and makes the same number of oracle queries as A such that*

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

Recall that DESX [7] is defined as:

$$DESX(x, K_1||K||K_2) = K_2 \oplus E_K(x \oplus K_1)$$

where K_1 and K_2 are the pre- and post-whitening keys respectively, and K is to key the inner E encapsulated by the two outer whitening (XOR) operations. The basic structure of this Kim *et al.* block cipher is like DESX [7] 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.

The security claim is based on this, i.e. even if the RKA adversary can vary the tweak input T, he cannot predict what the key difference is to the pre- and post-whitening parts since the hash function h is ϵ-AXU_2.

MITM Attack. The advanced slide attack [2] was applied to DESX and is basically a MITM attack. We show that a variant of the attack also applies to the Kim *et al.* block cipher. First we make some observations. Consider aligning an encryption with a decryption, slid on the post XOR. Thus for such a slid pair $\langle P, C\rangle$ and $\langle P', C'\rangle$ we get $C \oplus C' = h(T)$ and therefore

$$P' = h(T) \oplus E_K^{-1}(C' \oplus h(T)) = h(T) \oplus E_K^{-1}(C) \tag{8}$$

$$P = h(T) \oplus E_K^{-1}(C'). \tag{9}$$

Combining, we get

$$E_K^{-1}(C) \oplus P = E_K^{-1}(C') \oplus P'. \tag{10}$$

1. Obtain $2^{\frac{l+1}{2}}$ known plaintexts and corresponding ciphertexts $\langle P_i, C_i\rangle$.
2. Guess all 2^k values of K and do
   (a) Insert $\langle E_K^{-1}(C_i) \oplus P_i, i\rangle$ into a hash table keyed by the first component.
   (b) For each $i \neq j$ with $E_K^{-1}(C_i) \oplus P_i = E_K^{-1}(C_j) \oplus P_j$, do
      i. $h(T) = C \oplus C'$.
      ii. Test $\langle h(T), K\rangle$ via trial encryption on a few known $\langle P_i, C_i\rangle$.

Step 1 requires $2^{\frac{l+1}{2}}$ known plaintexts (KPs), Step 2(a) $2^k \times 2^{\frac{l+1}{2}}$ encryptions E_K; Step 2(b) is only performed for a slid pair, and for each this requires $O(1)$ encryptions E_K. It is expected that only $2^k \times 2^l \times 2^{-l} = 2^k$ slid pairs are detected thus about 2^k E_K. To summarize, the attack requires $2^{\frac{l+1}{2}}$ known plaintexts (KPs), $2^{\frac{l+1}{2}}$ memory and $2^k \times 2^{\frac{l+1}{2}}$ encryptions E_K; compared to 2^{k+l} for exhaustive key search. This above attack therefore shows that for E' it is in fact

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

it is less secure than expected for any block cipher of its $k + l$ bits key length. Furthermore, hence $\mathbf{Adv}^{\mathsf{KR}}_{E'}(A)$ matches (within a constant factor of) the upper bound of $\mathbf{Adv}^{\mathsf{KR}}_{E}(A)$ thus E' with a $k+l$ bit key is not substantially more secure against k-bit key-recovery attacks than its underlying E of k bits.

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

Resistance against RKA. On the positive side, it appears that the Kim *et al.* block cipher resists differential RKA 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 An Open Problem

All existing PRP-RKA ciphers do not allow the key component of the underlying cipher E to be varied. It is an open problem if PRP-RKA ciphers exist that allows this.

References

1. Bellare, M., and Kohno, T. A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In *Advances in Cryptology - International Conference on the Theory & Applications of Cryptographic Techniques (Eurocrypt '03)* (2003), E. Biham, Ed., LNCS 2656, Springer, pp. 491–506.
2. Biryukov, A., and Wagner, D. Advanced Slide Attacks. In *Advances in Cryptology - International Conference on the Theory & Applications of Cryptographic Techniques (Eurocrypt '00)* (2000), B. Preneel, Ed., LNCS 1807, Springer, pp. 589–606.
3. 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 *Proceedings of International Conference on Computational Science and Its Applications (ICCSA '05)* (2005), O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar, and C. J. K. Tan, Eds., LNCS 3481, Springer, pp. 567–576.
4. 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 IEEE Workshop on Communications Security (Crypto '81)* (1981), A. Gersho, Ed., -, pp. 2–6.
5. Kelsey, J., Schneier, B., and Wagner, D. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In *Advances in Cryptology - International Cryptology Conference (Crypto '96)* (1996), N. Koblitz, Ed., LNCS 1109, Springer, pp. 237–251.
6. Kelsey, J., Schneier, B., and Wagner, D. Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA. In *Proceedings of International Conference on Information and Communication Security '97* (1997), Y. Han, T. Okamoto, and S. Qing, Eds., LNCS 1334, Springer, pp. 233–246.
7. Kilian, J., and Rogaway, P. How to Protect DES Against Exhaustive Key Search (an Analysis of DESX). *Journal of Cryptology 14*, 1 (2001), 17–35.
8. Kim, J., Sung, J., Lee, S., and Preneel, B. Pseudorandom Permutation and Function Families Secure against Related-Key Attacks. Unpublished manuscript. Thanks to Jongsung Kim for a copy of this.
9. Lucks, S. Ciphers Secure against Related-Key Attacks. In *Proceedings of International Workshop on Fast Software Encryption (FSE '04)* (2004), B. K. Roy and W. Meier, Eds., LNCS 3017, Springer, pp. 359–370.
10. Phan, D. H., and Pointcheval, D. About the Security of Ciphers (Semantic Security and Pseudo-Random Permutations). In *Revised Selected Papers of International Workshop on Selected Areas in Cryptography (SAC '04)* (2004), H. Handschuh and M. A. Hasan, Eds., LNCS 3357, Springer, pp. 182–197.
11. Phan, R. C.-W. Related-Key Attacks on Triple-DES and DESX Variants. In *Topics in Cryptology - The Cryptographer's Track at RSA Conference (CT-RSA '04)* (2004), T. Okamoto, Ed., LNCS 2964, Springer, pp. 15–24.
12. Razali, E., and Phan, R. C.-W. On The Existence of Related-Key Oracles in Cryptosystems based on Block Ciphers. In *Proceedings of International Workshop on Information Security (IS '06), in On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops* (2006), R. Meersman, Z. Tari, and P. Herrero, Eds., LNCS 4277, Springer, pp. 425–438.
13. Winternitz, R. S., and Hellman, M. E. Chosen-key Attacks on a Block Cipher. *Cryptologia 11*, 1 (1987), 16–20.