情報保護學會論文誌
第17卷 第5號, 2007. 10

연관키 공격에 안전한 의사난수 치환 및 함수 패밀리*

김 종 성,[1†‡] 성 재 철[2], 은 희 천[1]
[1]고려대학교, [2]서울시립대학교

Pseudorandom Permutation and Function Families Secure against Related-Key Attacks

Jongsung Kim,[1†‡] Jaechul Sung[2], Hichun Eun[1]
[1]Korea University, [2]University of Seoul

요 약

본 논문에서는 강력한 의사난수 함수 관점에서 안전한 tweakable 전단사 함수 패밀리를 이용하여 연관키에 안전한 전단사 함수 패밀리를 설계할 수 있음을 보인다. 이를 이용하여 현재까지 알려진 것 중에 가장 빠르면서 연관키 공격에 안전한 전단사 함수 패밀리를 구성한다. 또한, 의사난수 함수 관점에서 안전한 적당한 유형의 함수 패밀리를 이용하여 연관키 공격에 안전한 전단사 함수 패밀리를 구성할 수 있음을 보인다. 이는 기존의 안전성이 증명된 MAC 알고리즘을 이용하면 연관키 공격에 안전한 스킴을 구성할 수 있음을 나타낸다. 끝으로, 본 논문에서는 연관키 공격에 대한 여러 안전성 개념(indistinguishability, non-malleability)을 정의하고, 그들 사이의 관계를 살펴본다.

ABSTRACT

In this paper, we observe that secure tweakable permutation families in the sense of strong pseudorandom permutation (SPRP) can be transformed to secure permutation families in the sense of SPRP against related-key attacks (SPRP-RKA). This fact allows us to construct a secure SPRP-RKA which is the most efficient to date. We also observe that secure function families of a certain form in the sense of a pseudorandom function (PRF) can be transformed to secure permutation families in the sense of PRP-RKA. We can exploit it to get various secure constructions against related-key attacks from known MAC algorithms. Furthermore, we define other security notions for related-key attacks, namely indistinguishability and non-malleability, and look into the relations between the security notions for related-key attacks. 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 related-key attacks.

Keywords : *Related-key attacks, Pseudorandom permutation families, Peudorandom function families*

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2006-(C1090-0603-0025))

† ‡ 주저자, 교신저자: joshep@cist.korea.ac.kr

접수일: 2007년 6월 12일; 채택일: 2007년 8월 21일

I. Introduction

In 1992 and 1993, Knudsen[17] and Biham[4] independently introduced a very useful cryptanalytic technique which exploits related keys in a differential attack. After this kind of attack, called a related-key attack, was introduced, it has been widely used to evaluate the security of block ciphers[4,11-13,18]. The related-key attack has been also extended into various cryptanalytic techniques such as a related-key differential-linear attack[10], a related-key impossible differential attack[11], a related-key boomerang and rectangle attacks[5,14] and so on. Related-key attacks are well-known to be very powerful tools to analyze block ciphers. Up to now, the best (in terms of the number of attacked rounds) known attacks against AES[16], KASUMI[6], XTEA[18] and GOST[18] are related-key attacks. Furthermore, related-key attacks can be used to evaluate the security of message authentication schemes and block cipher based enciphering modes (refer to [3] as an example).

The related-key attack is very difficult or even infeasible to conduct in many cryptographic applications, since it would certainly be unlikely that an attacker could persuade a sender to encrypt plaintexts under related keys unknown to the attacker. However, as demonstrated in [12], the related-key attack is feasible in some of the current real-world applications such as the IBM 4758 cryptoprocessor, key-exchange protocols that do not guarantee key integrity, and key-update protocols that updates session keys using a known function.

Related-key attacks allow an adversary to obtain plaintext and ciphertext pairs by using different, but related keys. The general aim of these attacks is to retrieve some or all portions of the related keys by using collected plaintext and ciphertext pairs. However, 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. 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 (or E, E^{-1}) and a randomly chosen permutation family G (or 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) (or a strong pseudorandom permutation (SPRP)) against related-key attacks (RKA), simply, we say that E is a secure PRP-RKA (or 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. In [3], 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 such as 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 (for any ciphers there exist classes of related-key attacks against which they are not secure). They also gave a construction of secure PRP-RKA cipher. In [21] 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 secure permutation families against some classes of related-key attacks from constructions which are already known to be secure. The second goal of this paper is to define various security notions for related-key attacks and to show the relationships of those security notions.

In this paper, we observe that secure tweakable permutation families in the sense of SPRP can be transformed to secure permutation families in the sense of SPRP-RKA, and secure function families of a certain form in the sense of PRF can be transformed to secure permutation families in the sense of PRP-RKA. This enables us to construct various SPRP-RKA or PRP-RKA ciphers from known design methods. Especially, we present a construction of se-

cure SPRP-RKA cipher which is more efficient than the mentioned above two secure PRP-RKA ciphers. Furthermore, we define other security notions for related-key attacks, indistinguishability and non-malleability, and look into the relations between the security notions for related-key attacks. 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 related-key attacks.

This paper is organized as follows: Section 2 provides some notations and security notions for related-key attacks. In Sect. 3 and Sect. 4, we observe that various secure permutation families against some classes of related-key attacks can be constructed from constructions which are already known to be secure. Section 5 defines various security notions for related-key attacks and shows the relationships of those security notions and Sect. 6 concludes the paper.

Ⅱ. Preliminaries

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

2.1. Notation

- $s \xleftarrow{\$} S$: the operation of selecting s uniformly at random from the set S
- $F\ K \times D \to R$: a family of functions from D to R indexed by keys K, i.e., $F_k(\cdot)$ is a function from D to R for each $k \in K$
- $E: K \times D \to D$: a family of permutations on D indexed by K, i.e., $E_k(\cdot)$8 is a permutation on D for each key $k \in K$
- $\widetilde{E}: K \times T \times D \to D$: a family of permutations on D indexed by $K \times T$, i.e., $\widetilde{E}_k(t, \cdot)$ is a permutation on D for each key $k \in K$ and tweak $t \in T$ (Note that T is not secret information.)
- $Perm(D)$: the set of all permutations on D
- $Perm(K,D)$: the set of all families of permutations with domain D and keys K
- $Rand(D,R)$: the set of all functions from D to R
- $Rand(K,D,R)$: the set of all families of functions with domain D, range R and keys K

In this paper, we call F a function family. We also call E and $\widetilde{E}$ a permutation family and a tweakable permutation family, respectively. According to the above notations, $G \xleftarrow{\$} Perm(K,D)$ represents the se lection of a random permutation family, i.e., for each key $k \in K$, $G_k(\cdot)$ is a permutation randomly chosen from $Perm(D)$. Furthermore, $G \xleftarrow{\$} Rand(K,D,R)$ repre sents the selection of a random function family, i.e., for each key $k \in K$, $G_k(\cdot)$ is a function randomly chosen from $Rand(D,R)$.

2.2. Definitions

Many security notions have been introduced for function and permutation families; in these notions, an adversary A is modeled as a Turing machine that has black-box access to an oracle (or multiple oracles). While the computational power of A is unlimited, the total number of oracle calls is limited to a certain number. For each query of A the oracle gives an answer to A. After making a limited number of queries to the oracle(s) adaptively, A outputs a bit. Sections 3 and 4 considers below four security notions. Some other security notions will be offered in Sect. 5.

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

$$Adv_F^{prf}(A) = \Pr[k \xleftarrow{\$} K: A^{F_k(\cdot)} = 1] - \Pr[g \xleftarrow{\$} Rand(D,R): A^{g(\cdot)} = 1].$$

$A^{O(\cdot)}$ means A with an oracle $O(\cdot)$, which returns $O(M)$ for the adversary's query M.

Definition 2. (SPRP) [22] Let $E: K\times D\rightarrow D$ be a permutation family and A be an adversary. Then the sprp-advantage of A is defined by

$$Adv_E^{sprp}(A)=\Pr[k\xleftarrow{\$}K: A^{E_k(\cdot),E_k^{-1}(\cdot)}=1]-\Pr[g\xleftarrow{\$}Perm(D): A^{g(\cdot),g^{-1}(\cdot)}=1].$$

$A^{O(\cdot),O^{-1}(\cdot)}$ means A with two oracles $O(\cdot),O^{-1}(\cdot)$; for an adversary's query of M (resp. C) to the first (resp. second) oracle it returns $O(M)$ (resp. $O^{-1}(C)$).

Definition 3. (TWEAK-SPRP) [8] Let $\tilde{E}: K\times T\times D\rightarrow D$ be a tweakable permutation family and A be an adversary. Then the tweak-sprp-advantage of A is defined by

$$Adv_E^{tweak-sprp}(A)=\Pr[k\xleftarrow{\$}K: A^{\tilde{E}_k(\cdot,\cdot),\tilde{E}_k^{-1}(\cdot,\cdot)}=1]-\Pr[\tilde{G}\xleftarrow{\$}Perm(T,D): A^{\tilde{G}(\cdot,\cdot),\tilde{G}^{-1}(\cdot,\cdot)}=1].$$

$A^{\tilde{O}(\cdot,\cdot),\tilde{O}^{-1}(\cdot,\cdot)}$ means A with two oracles $\tilde{O}(\cdot,\cdot),\tilde{O}^{-1}(\cdot,\cdot)$ for an adversary's query of (t,M) (resp. (t,C)) to the first (resp. second) oracle it returns $\tilde{O}(t,M)$ (resp. $\tilde{O}^{-1}(t,C)$).

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

$$Adv_{\Phi,E}^{sprp-rka}(A)=\Pr[k\xleftarrow{\$}K: A^{E_{RK(\cdot,k)}(\cdot),E_{RK(\cdot,k)}^{-1}(\cdot)}=1]-\Pr[k\xleftarrow{\$}K; G\xleftarrow{\$}Perm(K,D): A^{G_{RK(\cdot,k)}(\cdot),G_{RK(\cdot,k)}^{-1}(\cdot)}=1].$$

$A^{O_{RK(\cdot,k)}(\cdot),O_{RK(\cdot,k)}^{-1}(\cdot)}$ means A with two oracles $O_{RK(\cdot,k)}(\cdot),O_{RK(\cdot,k)}^{-1}(\cdot)$; for an adversary's query of (ϕ,M) (resp. (ϕ,C)) to the first (resp. second) oracle it returns $O_{\phi(k)}(M)$ (resp. $O_{\phi(k)}^{-1}(C)$).

The PRP-RKA security notion[3] is defined by removing the decryption oracle in Definition 4. This will be used in Sect. 4.

Ⅲ. From Secure Tweakable SPRP Families to Secure SPRP-RKA 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, this proof can be naturally extended into the SPRP security notion.

Theorem 1. Let $\tilde{E}: K\times T\times D\rightarrow D$ be a tweakable permutation family and let $E: (K\times T)\times D\rightarrow D$ be a permutation family defined as $E_{k\|t}(M)=\tilde{E}_k(t,M)$ where k is a secret key in K, t is either a tweak value in T of $\tilde{E}$ or a secret key in T of E, and M is a message in D. If $\tilde{E}$ is a secure tweakble SPRP, then E is a secure SPRP with respect to Φ-restricted RKAs if each function Φ in Φ is a partial transformation for which there exists a function $\phi': T\rightarrow T$ such that $\phi(k,t)=(k,\phi'(t))$. Formally, given a SPRP-RKA adversary A attacking E, we can construct a TWEAK-SPRP adversary B_A attacking $\tilde{E}$ such that

$$Adv_{\Phi,E}^{sprp-rka}(A)\leq Adv_{\tilde{E}}^{tweak-sprp}(B_A)$$

and B_A takes the same amount of time and makes the same number of oracle queries as A.

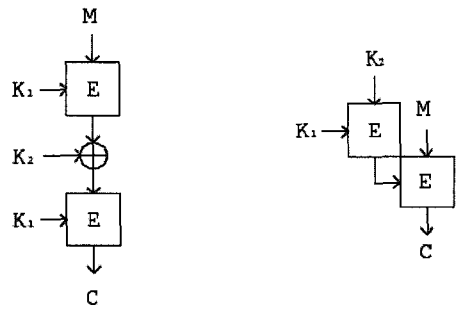
Using Theorem 1 and Theorem 2 of [19], we can construct a secure SPRP-RKA family which is the most efficient to date. See Proposition 1 for the details. In Proposition 1, a set H of functions with domain T and range D is said to be ε-almost 2-xor universal (ε-AXU2) if $\Pr_h[h(x)\oplus h(y)=z]\leq\epsilon$ for all x,y,z [19], where $\Pr_h[]$ is the probability over the function h.

Proposition 1. Let $E: K\times D\rightarrow D$ be a permutation family, let $H: T\rightarrow D$ be an $\epsilon-AXU_2$ family with $\epsilon\geq 1/|D|$ and let $E': (K\times T\times H)\times D\rightarrow D$ be another permutation

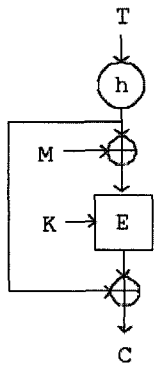
family defined as $E'_{k,t,h}(M) = E_k(M \oplus h(t)) \oplus h(t)$ where (k,t,h) is a secret key in $K \times T \times H$, and M is a message in D. If E is a secure SPRP and H is $\epsilon - AXU_2$ where ϵ is negligible, then E' is a secure SPRP with respect to Φ-restricted RKAs when each function ϕ in Φ is a partial transformation for which there exists a function $\phi' : T \to T$ such that $\phi(k,t,h) = (k,\phi'(t),h)$. Formally, given a SPRP-RKA adversary A attacking E' that queries its oracles with at most q queries, we can construct a SPRP adversary B_A attacking E such that

$$Adv^{sprp-rka}_{\Phi,E'}(A) \le Adv^{sprp}_{E}(B_A) + 3\epsilon q^2$$

and B_A takes the same amount of time and makes the same number of oracle queries as A.



(Construction A) (Construction B)



(Construction C)

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

Figure 1 compares the construction of Proposition 1 with the previous ones. Note that Constructions A and B calls two block ciphers while Construction C does one block cipher and one ϵ-almost 2-xor universal function which is implemented faster than a block cipher. It follows that Construction C is more efficient than the other two constructions. See [3,21] for the concrete security bounds of Constructions A and B.

Theorem 1 can be also exploited to construct various secure permutation families from tweakable enciphering modes which are already known to be secure. The security of tweakable enciphering modes CMC[8], EME[9], EME*[7] 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.

Ⅳ. From Secure PRF Families of a Certain Form to Secure PRP-RKA Families

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 tighter bound of the PRF-RKA/PRP-RKA switching Proposition 8.9 in [3].

Lemma 1. Let 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

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

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

Proof. From Proposition 8.9 in [3] we know that

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

where $\Pr_{g[\cdot]}$ represents the probability in the experiment $k \xleftarrow{\$} K, G \xleftarrow{\$} Rand(K,D,D), A^{G_{RK(\cdot,k)}(\cdot)}$ and D represents the event that, for each related-key that A accesses to its oracle (i.e., $\phi(k)$ where 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

$$\Pr_g[\overline{D}] \le \frac{r \cdot q \cdot NM_\Phi \cdot (q \cdot NM_\Phi - 1)}{2 \cdot |D|}.$$

However, we can bound $\Pr_g[\overline{D}]$ more tightly.

Let $\phi_1, \phi_2, \cdots, \phi_{r'}$, $(r' \le r)$ be transformations in Φ that A queries. Without loss of generality, we assume that $\phi_1(k) = \cdots = \phi_{a_1}(k) = k_1, \phi_{a_1+1}(k) = \cdots = \phi_{a_1+a_2}(k) = k_2, \cdots, \phi_{a_1+\cdots+a_{m-1}}(k) = \cdots = \phi_{a_1+\cdots+a_{m-1}+a_m}(k) = k_m$ where $a_1 + \cdots + a_{m-1} + a_m = r'$ and $k_j \ne k_{j'}$ for $1 \le j < j' \le m$. Since queries at most q times per key transformation, for each k_i the probability of a colli sion in the output of the oracle on distinct inputs is at most $\frac{a_i \cdot q \cdot (a_i \cdot q - 1)}{2 \cdot |D|}$ (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.

$$\Pr_g[\overline{D}] \le \sum_{i=1}^{m} \frac{a_i \cdot q \cdot (a_i \cdot q - 1)}{2 \cdot |D|} \le \sum_{i=1}^{m} \frac{a_i \cdot q \cdot (q \cdot \min\{r', NM_\Phi\} - 1)}{2 \cdot |D|} \le \frac{r \cdot q \cdot (q \cdot \min\{r, NM_\Phi\} - 1)}{2 \cdot |D|}.$$

Using Lemma 1 we can easily show Theorem 2.

Theorem 2. Let $E: (K_1 \times K_2) \times D \to D$ be a permutation family and let $F: K_1 \times (K_2 \times D) \to D$ 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 K_1, k_2 is either a secret key in K_2 of E or a message in K_2 of F, and M is a message in D. If F is a secure PRF, then E is a secure PRP with respect to Φ-restricted RKAs if each function Φ in Φ is a partial transformation for which there exists a function $\phi' : K_2 \to K_2$ such that $\phi(k_1, k_2) = (k_1, \phi'(k_2))$. Formally, given a PRP-RKA adversary 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 B_A attacking F such that

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

and B_A takes the same amount of time and makes the same number of oracle queries as A.

Proof. Let B_A be the F adversary that works as follows.

<Adversary $B_A^{O(\cdot)}$>

1. Select k_2 at random from K_2.
2. Obtain A's request $(\phi(=(id, \phi')), M)$ by running A.
3. Return $O(\phi'(k_2) \| M)$ to A.
4. If A outputs b, then output b. Otherwise, go to Step 2.

When B_A is given access to F, A computes E with related keys. So the following equality holds:

$$\Pr[k_1 \xleftarrow{\$} K_1 : B_A^{F_{k_1}(\cdot)} = 1] = \Pr[(k_1, k_2) \xleftarrow{\$} K_1 \times K_2 : A^{E_{RK(\cdot,(k_1,k_2))}(\cdot)} = 1].$$

When B_A is given access to G where G is randomly chosen from $Rand(K_2 \times D, D)$, B_A replies to A using an independently selected random function on D for each $\phi'(k_2)$. So the equation

$$\Pr[G \xleftarrow{\$} Rand(K_2 \times D, D) : B_A^{G(\cdot)} = 1] = \Pr[(k_1, k_2) \xleftarrow{\$} K_1 \times K_2, G \xleftarrow{\$} Rand(K_1 \times K_2, D, D) :$$

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

$$Adv_{\Phi,E}^{prp-rka}(A) = \Pr[(k_1,k_2) \xleftarrow{\$} K_1 \times K_2 : A^{E_{RK(\cdot,\cdot),(k_1,k_2)}(\cdot)} = 1]$$
$$- \Pr[(K_1,K_2) \xleftarrow{\$} K_1 \times K_2, G \xleftarrow{\$} Rand(K_1 \times K_2, D, D) : A^{G_{RK(\cdot,\cdot),(k_1,k_2)}(\cdot)} = 1]$$
$$+ \Pr[(k_1,k_2) \xleftarrow{\$} K_1 \times K_2, G \xleftarrow{\$} Rand(K_1 \times K_2, D, D) : A^{G_{RK(\cdot,\cdot),(k_1,k_2)}(\cdot)} = 1]$$
$$- \Pr[(k_1,k_2) \xleftarrow{\$} K_1 \times K_2, G \xleftarrow{\$} Perm(K_1 \times K_2, D) : A^{G_{RK(\cdot,\cdot),(k_1,k_2)}(\cdot)} = 1]$$
$$\le Adv_F^{prf}(B_A) + \frac{r \cdot q \cdot (q \cdot \min r, \mathrm{NM}_\Phi - 1)}{2 \cdot |D|}.$$

Theorem 2 can be exploited to construct various permutation families from MAC algorithms which are already known to be secure in the sense of PRF. Consider for example OMAC 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.

V. Relationships between Security Notions

In this section, we introduce some other security notions that give more information on permutation families and then clarify their relations. We first give a definition of indistinguishability, which is the same as the left-or-right security notion of Bellare et al. [1].

Definition 5. (TWEAK-IND) [8] Let $\tilde{E}: K \times T \times D \to D$ be a tweakable permutation family and A be an adversary. Then the tweak-ind advantage of A is defined by

$$Adv_{\tilde{E}}^{\mathrm{tweak-ind}}(A) = \Pr[k \xleftarrow{\$} K : A^{\tilde{E}_k(\cdot,\cdot)^1, \widetilde{E_k^{-1}}(\cdot,\cdot)^1} = 1]$$
$$- \Pr[k \xleftarrow{\$} K : A^{\tilde{E}_k(\cdot,\cdot)^0, \widetilde{E_k^{-1}}(\cdot,\cdot)^0} = 1].$$

$A^{\tilde{O}(\cdot,\cdot)^b, \widetilde{O^{-1}}(\cdot,\cdot)^b}(b = 0 \text{ or } 1)$ means A with two oracles $\tilde{O}(\cdot,\cdot)^b, \widetilde{O^{-1}}(\cdot,\cdot)^b$; 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 $\tilde{O}(T_b,M_b)$ (resp. $\widetilde{O^{-1}}(T_b,C_b)$).

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

Definition 6. (IND-RKA) Let $E: K \times D \to D$ be a permutation family and Φ be a set of functions over K. Let A be an adversary that is restricted to queries within $\Phi \times D$. Then the ind-rka advantage of A is defined by

$$Adv_{\Phi,E}^{\mathrm{ind-rka}}(A) = \Pr[k \xleftarrow{\$} K : A^{E_{RK(\cdot,\cdot),k}(\cdot)^1, E_{RK(\cdot,\cdot),k}^{-1}(\cdot)^1} = 1]$$
$$- \Pr[k \xleftarrow{\$} K : A^{E_{RK(\cdot,\cdot),k}(\cdot)^0, E_{RK(\cdot,\cdot),k}^{-1}(\cdot)^0} = 1].$$

$A^{O_{RK(\cdot,\cdot)}(\cdot)^b, O_{RK(\cdot,\cdot)}^{-1}(\cdot)^b}(b = 0 \text{ or } 1)$ means A with two oracles $O_{RK(\cdot,\cdot)}(\cdot)^b$, $O_{RK(\cdot,\cdot)}^{-1}(\cdot)^b$; 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 $O_{\phi_b(k)}(M_b)$ $(resp. O_{\phi_b(K)}^{-1}(C_b))$.

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 [8] for the disallowed queries of a tweak-ind adversary.

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

- $M(t)$: a set of all M such that A asks $\tilde{E}_k(\cdot,\cdot)$ to encrypt (t,M) or A asks $\widetilde{E_k^{-1}}(\cdot,\cdot)$ to decrypt (t,C) and its answer is M.
- $C(t)$: a set of all C such that A asks $\widetilde{E_k^{-1}}(\cdot,\cdot)$

to decrypt (t, C) or A asks $\widetilde{E}_k(\cdot,\cdot)$ to encrypt (t, M) and its answer is C.

- $M(t, C)$: a set $\widetilde{E_k^{-1}}(t, C)$ if $C \in C(t)$, and a set $D - M(t)$ otherwise.

Definition 7. (TWEAK-NM) [8] Let $\widetilde{E}: K \times T \times D \to D$ be a tweakable permutation family and A be an adversary. Then the tweak-nm advantage of A is defined by

$$Adv_{\widetilde{E}}^{tweak-nm}(A) = \Pr[k \xleftarrow{\$} K, (t,C,f) \xleftarrow{\$} A^{\widetilde{E}_k(\cdot,\cdot),\widetilde{E_k^{-1}}(\cdot,\cdot)}, M = \widetilde{E_k^{-1}}(t,C) : f(M)=1] - \Pr[k \xleftarrow{\$} K, (t,C,f) \xleftarrow{\$} A^{\widetilde{E}_k(\cdot,\cdot),\widetilde{E_k^{-1}}(\cdot,\cdot)}, M \xleftarrow{\$} M(t,C) : f(M)=1].$$

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

Similarly, we can define non-malleability of a permutation family $E: K \times D \to D$ against related-key attacks. In related-key attack models, an nm-rka adversary 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 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 D. The three sets are defined as follows.

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

Definition 8. (NM-RKA) Let $E: K \times D \to D$ be a permutation family and Φ be a set of functions over K. Let A be an adversary that is restricted to queries within $\Phi \times D$. Then the nm-rka advantage of A is defined by

$$Adv_{\Phi,E}^{nm-rka}(A) = \Pr[k \xleftarrow{\$} K, (\phi,C,f) \xleftarrow{\$} A^{E_{RK(\cdot,k)}(\cdot),E^{-1}_{RK(\cdot,k)}(\cdot)}, M = E^{-1}_{\phi(k)}(C) : f(M)=1] - \Pr[k \xleftarrow{\$} K, (\phi,C,f) \xleftarrow{\$} A^{E_{RK(\cdot,k)}(\cdot),E^{-1}_{RK(\cdot,k)}(\cdot)}, M \xleftarrow{\$} M(\phi,C) : f(M)=1].$$

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

The following three theorems clarify the relationships between these newly defined security notions IND-RKA, NM-RKA and the SPRP-RKA security notion. Theorem 3 shows that SPRP-RKA security implies IND-RKA security and Theorem 4 shows the converse. Theorem 5 shows that SPRP-RKA security implies NM-RKA

security. The proofs of Theorems 3, 4, 5 are similar to the proofs of [8], so we omit them.

Theorem 3. Let $E: K \times D \to D$ be a permutation family and Φ be a set of functions over 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 A that queries its oracles with at most q queries, we can construct a Φ-restricted SPRP-RKA adversary B_A such that

$$Adv_{\Phi,E}^{ind-rka}(A) \le 2 \cdot Adv_{\Phi,E}^{sprp-rka}(B_A) + \frac{2 \cdot q^2}{|D| - q}$$

and B_A takes almost same amount of time and makes the same number of oracle queries as A.

Theorem 4. Let $E: K \times D \to D$ be a permutation family and Φ be a set of functions over 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 A that queries its oracles with at most q queries, we can construct a Φ-restricted IND-RKA adversary B_A such that

$$Adv_{\Phi,E}^{sprp-rka}(A) \le Adv_{\Phi,E}^{\in d-rka}(B_A)$$

and B_A takes almost same amount of time and makes the same number of oracle queries as A.

Theorem 5. Let $E: K\times D\rightarrow D$ be a permutation family and Φ be a set of functions over 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 A that queries its oracles with at most q queries, we can construct a Φ-restricted SPRP-RKA adversary B_A such that

$$Adv_{\Phi,E}^{nm-rka}(A) \leq Adv_{\Phi,E}^{sprp-rka}(B_A)$$

and B_A takes almost same amount of time as A and makes one more query than 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 6. Let $\tilde{E}: K\times T\times D\rightarrow D$ be a tweakable permutation family and let $E: (K\times T)\times D\rightarrow D$ 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 $\phi': T\rightarrow T$ such that $\phi(k,t)=(k,\phi'(t))$. Formally, given a Φ-restricted IND-RKA adversary A attacking E, we can construct a TWEAK-IND adversary B_A attacking $\tilde{E}$ such that

$$Adv_{\Phi,E}^{\mathrm{ind-rka}}(A) \leq Adv_{\tilde{E}}^{\mathrm{tweak-ind}}(B_A)$$

and B_A takes the same amount of time and makes the same number of oracle queries as A.

Proof. Let B_A be the $\tilde{E}$ adversary that works as follows.

<Adversary>

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

Since the adversary B_A is given access to $\tilde{E}_k(\cdot,\cdot)^b$, $\widetilde{E_k^{-1}}(\cdot,\cdot)^b$ where k is randomly chosen from K, B_A computes $E_{RK(\cdot,k\|t)}(\cdot)^b, E^{-1}_{RK(\cdot,k\|t)}(\cdot)^b$ by running A. So the equality

$$\Pr[k\xleftarrow{\$}K: B_A^{\tilde{E}_k(\cdot,\cdot)^b,\widetilde{E_k^{-1}}(\cdot,\cdot)^b}=1] =$$
$$\Pr[k\xleftarrow{\$}K, t\xleftarrow{\$}T: A^{E_{RK(\cdot,k\|t)}(\cdot)^b, E^{-1}_{RK(\cdot,k\|t)}(\cdot)^b}=1]$$

holds. This completes the proof.

Theorem 7. Let $\tilde{E}: K\times T\times D\rightarrow D$ be a tweakable permutation family and let $E: (K\times T)\times D\rightarrow D$ 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 $\phi': T\rightarrow T$ such that $\phi(k,t)=(k,\phi'(t))$. Formally, given a Φ-restricted NM-RKA adversary A attacking E, we can construct a TWEAK-NM adversary B_A attacking $\tilde{E}$ such that

$$Adv_{\Phi,E}^{nm-rka}(A) \leq Adv_{\tilde{E}}^{tweak-nm}(B_A)$$

and B_A takes the same amount of time and makes the same number of oracle queries as A.

Proof. Let B_A be the $\tilde{E}$ adversary that works as follows.

<Adversary>

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

Since the adversary B_A is given access to $\tilde{E}_k(\cdot,\cdot)$, $\widetilde{E_k^{-1}}(\cdot,\cdot)$where k is chosen uniformly at random from K, B_A computes

$E_{RK(\cdot,k\|t)}(\cdot), E^{-1}_{RK(\cdot,k\|t)}(\cdot)$ by running A. So it is easy to see that

$$\begin{aligned}&Adv^{tweak-nm}_{E}(B_A)\\&= \Pr[k\xleftarrow{\$}K, t\xleftarrow{\$}T, (\phi(=(id,\phi')), C, f)\xleftarrow{\$}A^{E_{RK(\cdot,k\|t)}(\cdot), E^{-1}_{RK(\cdot,k\|t)}(\cdot)},\\&\qquad M=\widetilde{E_k^{-1}}(\phi'(t), C): f(M)=1]\\&-\Pr[k\xleftarrow{\$}K, t\xleftarrow{\$}T, (\phi(=(id,\phi')), C, f)\xleftarrow{\$}A^{E_{RK(\cdot,k\|t)}(\cdot), E^{-1}_{RK(\cdot,k\|t)}(\cdot)},\\&\qquad M\xleftarrow{\$}M(\phi'(t), C): f(M)=1].\end{aligned}$$

Since $f(\widetilde{E_k^{-1}}(\phi'(t), C))=1$ if and only if $f(E^{-1}_{k\|\phi'(t)}(C))=1$, the equality

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

holds. Furthermore, for all $\phi=(id,\phi')$ and C $M(\phi'(t), C)$ of B_A takes the same distribution with $M(\phi, C)$ of A and thus the equation

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

holds. This completes the proof.

VI. Conclusion

We have presented a SPRP construction that is secure against related-key attacks (SPRP-RKA) 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. Our observations can stimulate the design and analysis of SPRP (or PRP) that are secure against related-key attacks.

Acknowledgements. We thank Bart Preneel for his helpful comments.

참고문헌

[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, 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 — Proceedings of 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 —Proceedings of 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 — Proceedings of 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 KASUMI,* Advances in Cryptology — Proceedings of ASIACRYPT 2005, to appear.

[7] S. Halevi, *EME* : eXtending EME to handle arbitrary-length messages with associated data,* 2004. Available at the ePrint archive, http://eprint.iacr.org/2004/125/.

[8] S. Halevi and P. Rogaway, *A Tweakable Enciphering Mode,* Advances in Cryptology — Proceedings of CRYPTO 2003, LNCS 2729, Springer-Verlag, pp.482-499, 2003.

[9] S. Halevi and P. Rogaway, *A Parallelizable Enciphering Mode,* Proceedings of 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/.

[10] P. Hawkes, *Differential-Linear Weak-Key Classes of IDEA,* Advances in Cryptology—Proceedings of EUROCRYPT 1998, LNCS 1403, pp.112-126, Springer-Verlag, 1998.

[11] G. Jakimoski and Y. Desmedt, *Related-Key Differential Cryptanalysis of 192-bit Key AES Variants,* Proceedings of SAC 2003, LNCS 3006, Springer-Verlag, pp.208-221, 2003.

[12] J. Kelsey, B. Schneier and D. Wagner, *Key-schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES,* Advances in Cryptology —Proceedings of CRYPTO 1996, LNCS 1109, Springer-Verlag, pp.237-251, 1996.

[13] J. Kelsey, B. Schneier and D. Wagner, *Related-key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA,* Information and Communications Security 1997, LNCS 1334, Springer-Verlag, pp.233-246, 1997.

[14] J. Kim, G. Kim, S. Hong, S. Lee and D. Hong, *The Related-Key Rectangle Attack - Application to SHACAL-1,* Proceedings of ACISP 2004, LNCS 3108, Springer-Verlag, pp.123-136, 2004.

[15] J. Kim, G. Kim, S. Lee, J. Lim and J. Song, *Related-Key Attacks on Reduced Rounds of SHACAL-2,* Proceedings of INDOCRYPT 2004, LNCS 3348, Springer-Verlag, pp.175-189, 2004.

[16] J. Kim, S. Hong and B. Preneel, *Related-Key Rectangle Attacks on Reduced AES-192 and AES-256,* Proceedings of FSE 2007, to appear.

[17] L.R. Knudsen, *Cryptanalysis of LOKI91,* Advances in Cryptology—Proceedings of AUSCRYPT 1992, LNCS 718, Springer-Verlag, pp.196-208, 1993.

[18] 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 FSE 2004, LNCS 3017, Springer-Verlag, pp.299-316, 2004.

[19] M. Liskov, R. L. Rivest and D. Wagner, *Tweakable Block Ciphers,* Advances in Cryptology —Proceedings of CRYPTO 2002, LNCS 2442, Springer-Verlag, pp.31-46, 2002.

[20] M. Luby and C. Rackoff, *How to Construct Pseudorandom Permutations from Peudorandom Function,* SIAM J. Computation, Vol.17, No.2, 1988.

[21] S. Lucks, *Ciphers Secure against Related-Key Attacks,* Proceedings of FSE 2004, LNCS 3017, Springer-Verlag, pp.359-370, 2004.

[22] 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.

〈著者紹介〉

김 종 성 (Jongsung Kim) 정회원
2000년 8월 : 고려대학교 수학과 학사
2002년 8월 : 고려대학교 수학과 석사
2006년 11월 : K.U.Leuven, ESAT/SCD-COSIC 박사
2007년 2월 : 고려대학교 정보보호대학원 박사
2007년 3월-현재 : 고려대학교 정보보호기술연구센터 연구전임강사
<관심분야> 대칭키 암호의 분석 및 설계

성 재 철 (Jaechul Sung) 종신회원
1997년 8월 : 고려대학교 수학과 학사
1999년 8월 : 고려대학교 수학과 석사
2002년 8월 : 고려대학교 수학과 박사
2002년 7월-2004년 1월 : 한국정보보호진흥원 선임연구원
2004년 2월-현재 : 서울시립대학교 수학과 조교수
<관심분야> 대칭키 암호의 분석 및 설계

은 희 천 (Hichun Eun) 정회원
1969년 2월 : 고려대학교 수학과 학사
1974년 2월 : 고려대학교 수학과 석사
1982년 2월 : 고려대학교 수학과 박사
1982년 3월-현재 : 고려대학교 자연과학대학 정보수학과 교수