情報保護學會論文誌
第14券 第5號, 2004. 10

SHACAL-1의 축소 라운드에 대한 연관키 Rectangle 공격

김 종 성†, 김 구 일, 홍 석 희, 이 상 진‡
고려대학교 정보보호기술연구센터

Related-Key Rectangle Attacks on Reduced Rounds of SHACAL-1

Jongsung Kim†, Guil Kim, Seokhie Hong, Sangjin Lee‡
Center for Information Security Technologies, Korea University

요 약

블록 암호 분석 기법 중 Rectangle 공격과 연관키 공격은 잘 알려진 강력한 블록 암호 분석 도구이다. 본 논문에서는 Rectangle 공격과 연관키 공격을 결합한 연관키 Rectangle 공격을 소개한다. 두 가지 분석 기법의 특징과 장점을 적절히 이용하는 연관키 Rectangle 공격은 512-비트 키를 사용하는 59-라운드 SHACAL-1에 효과적으로 적용된다. 59-라운드 SHACAL-1의 연관키 Rectangle 공격은 $2^{149.72}$ 개의 선택 평문과 대략 $2^{498.30}$ 번의 59-라운드 SHACAL-1 암호화 과정으로 연관키를 구할 수 있다.

ABSTRACT

The rectangle attack and the related-key attack on block ciphers are well-known to be very powerful. In this paper we combine the rectangle attack with the related-key attack. Using this combined attack we can attack the SHACAL-1 cipher with 512-bit keys up to 59 out of its 80 rounds. Our 59-round attack requires a data complexity of $2^{149.72}$ chosen plaintexts and a time complexity of $2^{498.30}$ encryptions, which is faster than exhaustive search.

Keywords : *Related-Key Rectangle Attack, SHACAL-1*

Ⅰ. 서 론

블록 암호 분석 기법 중 가장 강력한 분석 기법 중 하나로 1990년 Biham과 Shamir에 의해 소개된 차분 공격[1]이 있다. 차분 공격 기법은 다양한 블록 암호에 적용되어 블록 암호의 안전성 평가 및 설계 방법 기준에 많은 기여를 하였으며 1990년 소개된 이후, 부정 차분 공격[14], 고계 차분 공격[14], 불능 차분 공격[3], 부메랑 공격[16] 등으로 다양하게 응용 발전하였다.

차분 공격의 변형 공격중 하나인 부메랑 공격[16]은 1999년 Wagner에 의해 소개된 선택 평문/능동 선택 암호문 공격이다. 하지만 Kelsey, Kohno, Schneier는 부메랑 공격이 선택 평문 공격으로 전환될 수 있음을 보였으며, 이 공격법을 확장된 부메랑 공격[12]이라 불렀다. 또한 확장된 부메랑 공격은 Biham, Dunkelman, Keller에 의해 Rectangle 공격[4]으로 발전하였다. 확장된 부메랑 공격에서 Rectangle 공격으로의 발전은 확장된 부메랑 특성

접수일 : 2004년 5월 7일 ; 채택일 : 2004년 7월 8일
* 본 연구는 정보통신부 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었습니다.
† 주저자 : joshep@cist.korea.ac.kr
‡ 교신저자 : sangjin@korea.ac.kr

확률을 극대화 시킴으로써 공격 성공률을 높였다.

1994년 Biham에 의해 소개된 연관키 공격은 서로 다르지만 연관된 키를 사용하는 블록 암호에 대한 공격으로 키 스케줄의 약점을 이용하는 공격법이다. 연관키 공격은 다소 이론적이지만 [2,6,9-11,15]에서 보듯이 블록 암호의 안전성 평가에 중요한 도구로 사용되고 있다.

본 논문에서는 Rectangle 분석 기법과 연관키 분석 기법의 특징과 장점을 적절히 이용한 연관키 Rectangle 분석 기법을 소개한다. 연관키 Rectangle 분석 기법에는 두 가지 형태의 distinguisher를 갖는다. 첫 번째 형태의 연관키 rectangle distinguisher는 키 k를 사용하는 평문 P와 키 k^*를 사용하는 선택 평문 P^*를 이용한다. 단, 키 k와 k^*는 서로 다르지만 연관된 키이다(첫 번째 형태의 distinguisher를 연관키 rectangle distinguisher-1로 표기). 반면, 두 번째 형태의 연관키 rectangle distinguisher는 키 k를 사용하는 선택 평문 P, P'와 키 k^*를 사용하는 선택 평문 P^*, P'^*를 이용한다(두 번째 형태의 distinguisher를 연관키 rectangle distinguisher-2로 표기). 본 논문은 먼저 위의 두 가지 형태의 distinguisher를 묘사한 후, 각각의 연관키 rectangle distinguisher를 블록 암호 SHACAL-1의 축소 라운드에 적용한다.

SHACAL-1[7]은 NESSIE(New European Schemes for Signatures, Integrity, and Encryption) 프로젝트에 제안된 160-비트 블록 암호로써 H. Handschuh와 D. Naccache에 의해 설계되었다. 이는 국제 표준 해쉬 알고리즘 SHA-1의 압축 함수에 기반을 두었으며, NESSIE 프로젝트의 2단계 블록 암호 후보에 선정되었다. 하지만 키 스케줄의 약점으로 인해 최종 추천 블록 암호에는 포함되지 않았다. SHACAL-1 블록 암호의 키 스케줄은 선형 귀한 쉬프트 레지스터 형태로서 확장된 부분 키는 상호간 종속 관계에 있다. 또한 SHACAL-1 블록 암호의 키 스케줄은 확산 효과가 크지 못하다. 이러한 키 스케줄의 약점은 연관키 분석 기법을 가능하게 한다. 본 논문에서는 연관키 특성에 rectangle 분석 기법을 결합하여 46-라운드 SAHCAL-1 연관키 rectangle distinguisher-1을 구성하고, 48-라운드 연관키 rectangle distinguisher-2를 구성한다. 이를 각각 이용하여 512-비트 키를 사용하는 57-라운드와 59-라운드 SHACAL-1을 공격한다. SHACAL-1의 기존 분석 결과와 본 논문의 결과를 요약하면 표 1, 2와 같다.

표 1. SHACAL-1의 Distinguisher 형태

Distinguisher 형태	라운드	확률
차분 특성	0-27	2^{-107}[13]
	0-29	2^{-138}[13]
확장 부메랑 특성	0-35	2^{-76}[13]
Rectangle 특성	0-35	$2^{-73.92}$[5]
	1-35	$2^{-69.92}$[5]
연관키 Rectangle 특성	0-45	$2^{-71.75}$[본 논문]
	0-47	$2^{-66.72}$[본 논문]

표 2. SHACAL-1의 분석 결과

공격유형	라운드	복잡도 데이터/시간
차분 공격	30(0-29)	2^{110}CP/$2^{75.1}$[13]
	41(0-40)	2^{141}CP/2^{491}[13]
확장 부메랑 공격	47(0-46)	$2^{158.5}$CP/$2^{508.4}$[13]
Rectangle 공격	47(0-46)	$2^{151.9}$CP/$2^{482.6}$[5]
	49(22-70)	$2^{151.9}$CP/$2^{508.5}$[5]
	49(29-77)	$2^{151.9}$CP/$2^{508.5}$[5]
연관키 Rectangle 공격	57(0-56)	$2^{154.75}$RK-CP/$2^{503.38}$ [본 논문]
	59(0-58)	$2^{149.72}$RK-CP/$2^{498.30}$ [본 논문]

CP: 선택평문, RK-CP: 연관키 선택 평문, CC: 선택암호문

II. 연관키 Rectangle 공격의 소개

본 장에서는 연관키 rectangle distinguisher의 두 가지 형태를 설명한다. 설명하기에 앞서 본 논문에 전반적으로 사용되는 표기법과 가정 사항을 설명한다.

블록 암호 $E_k: \{0,1\}^n \rightarrow \{0,1\}^n$가 두 개의 부분 암호 E_k^0, E_k^1의 합성 형태 $E_k = E_k^1 \circ E_k^0$로 표현된다고 가정하자. E_k를 함수 $E: \{0,1\}^{|k|} \times \{0,1\}^n \rightarrow \{0,1\}^n$로 나타낸다면, 위의 가정 하에 E는 E^0, E^1의 합성 형태 $E = E^1 \circ E^0$으로 표현할 수 있

다. E^0에 확률 p를 갖는 차분 특성 $\alpha \rightarrow \beta$이 존재하거나, 확률 p^*를 갖는 연관키 차분 특성 $\alpha \rightarrow \beta$(즉, $\Pr[E_k^0(P) \oplus E_{k^*}^0(P^*) = \beta | P \oplus P^* = \alpha] = p^*$이며, k, k^*는 서로 다르지만, 연관된 키이다)이 존재한다고 가정한다. 그리고 E^1에 확률 q를 갖는 차분 특성 $\gamma \rightarrow \delta$이 존재하거나, 확률 q^*를 갖는 연관키 차분 특성 $\gamma \rightarrow \delta$(즉, $Pr[E_k^1(X) \oplus E_{k^*}^1(X^*) = \delta | X \oplus X^* = \gamma] = q^*$이며, k, k^*는 서로 다르지만, 연관된 키이다)이 존재한다고 가정한다.

2.1 연관키 rectangle distinguisher-1(그림 1)

연관키 rectangle distinguisher-1은 몇 가지의 차분 조건을 만족하는 4개의 평문 쌍 (P_i, P_i^*, P_j, P_j^*)에 의해 생성된다. P_i, P_j는 E_k에 의해, P_i^*, P_j^*는 E_{k^*}에 의해 암호화 될 때, 차분 조건 $P_i \oplus P_i^* = P_j \oplus P_j^* = \alpha$이 성립한다고 가정하자. 평문 P_i, P_i^*, P_j, P_j^*에 대한 E^0의 암호문을 각각 X_i, X_i^*, X_j, X_j^*라 하고, X_i, X_i^*, X_j, X_j^*에 대한 E^1의 암호문을 각각 C_i, C_i^*, C_j, C_j^*라 하자. 위의 가정 하에 차분 조건 $X_i \oplus X_i^* = X_j \oplus X_j^* = \beta$와 $X_i \oplus X_j = \gamma$을 만족한다면, $X_i^* \oplus X_j^* = (X_i \oplus \beta) \oplus (X_j \oplus \beta) = \gamma$이 성립한다. 만약 위의 차분 조건 하에 암호문 쌍 C_i, C_j와 C_i^*, C_j^*이 차분 δ를 만족 한다면(즉, $C_i \oplus C_j = C_i^* \oplus C_j^* = \delta$), 위의 4개의 평문 쌍 (P_i, P_i^*, P_j, P_j^*)을 올바른 quartet이라 부른다. 또한, 차분 조건 $X_i \oplus X_i^* = X_j \oplus X_j^* = \beta$와 $X_i \oplus X_j^* = \gamma$을 만족한다면, $X_i^* \oplus X_j = (X_i \oplus \beta) \oplus (X_j^* \oplus \beta) = \gamma$이 성립한다. 만약 암호문 쌍 C_i, C_j^*와 C_i^*, C_j이 차분 δ를 만족한다면(즉, $C_i \oplus C_j^* = C_i^* \oplus C_j = \delta$), 이러한 모든 차분 조건을 만족하는 4개의 평문 쌍 (P_i, P_i^*, P_j, P_j^*) 또한 올바른 quartet이라 부른다. 처음 경우의 올바른 quartet은 그림 1에 나타나 있다.

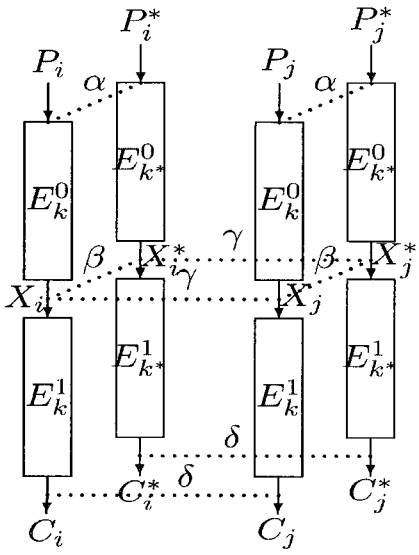


그림 1. 연관키 Rectangle Distinguisher-1

차분 α를 만족하는 m개의 평문 쌍(키 k를 사용하는 한 평문과 키 k^*를 사용하는 다른 한 평문)이 있다고 가정하자. 부분 암호 E^0을 통해 연관키 차분 특성 $\alpha \rightarrow \beta$를 만족하는 쌍은 약 mp^*개 이며, mp^*개의 평문 쌍은 약 $\frac{(mp^*)^2}{2}$개의 quartet을 생성한다. 블록 암호의 암호화 과정에서 중간 과정의 값이 랜덤하게 분포한다고 가정하면, 확률 2^{-n}으로 차분 $X_i \oplus X_j = \gamma$를 얻는다. 이 경우에 올바른 quartet이 되기 위해 X_i, X_j와 X_i^*, X_j^*는 확률 q를 갖는 차분 특성 $\gamma \rightarrow \delta$을 만족해야 한다. 따라서 차분 α를 만족하는 m개의 평문 쌍에 대한 처음 경우의 올바른 quartet의 평균 기대값은 $m^2 \cdot 2^{-n-1} \cdot (p^*)^2 \cdot q^2 (= \frac{(mp^*)^2}{2} \cdot 2^{-n} \cdot q^2)$이다. 다음은 확률 2^{-n}으로 차분 $X_i \oplus X_j^* = \gamma$를 만족하는 경우를 고려해 보자. 이 경우 올바른 quartet이 되기 위해 X_i, X_j^*와 X_i^*, X_j는 확률 q^*를 갖는 연관키 차분 특성 $\gamma \rightarrow \delta$을 만족해야 한다. 따라서 차분 α를 만족하는 m개의 평문 쌍에 대한 경우의 올바른 quartet의 평균 기대값은 $m^2 \cdot 2^{-n-1} \cdot (p^*)^2 \cdot (q^*)^2 (= \frac{(mp^*)^2}{2} \cdot 2^{-n} \cdot (q^*)^2)$이다. 그러므로 올바른 quartet의 총 평균 기대값은 처음 경우와 나중 경우를 고려하여 $m^2 \cdot 2^{-n-1} \cdot (p^*)^2 \cdot (q^2 + (q^*)^2)$이 된다.

랜덤 치환 함수인 경우에 올바른 quartet의 평균 기대값은 약 $m^2 \cdot 2^{-2n} (= \binom{m}{2} \cdot 2 \cdot 2^{-2n})$이므로, 만약 $p^* \cdot (\frac{1}{2} \cdot (q^2 + (q^*)^2))^{1/2} > 2^{-n/2}$)을 만족하고, m이 충분히 크다면, 연관키 rectangle dis-

tinguisher-1을 갖는 E와 랜덤 치환 함수는 구별 가능하다.

하지만 연관키 rectangle 공격은 부분 암호 E^0에 대해 입력 차분이 α를 갖는 모든 연관키 차분 특성과 부분 암호 E^1에 대해 출력 차분이 δ가 되는 모든 차분 특성 및 연관키 차분 특성을 고려한 distinguisher를 이용한다. 즉, 연관키 rectangle 공격에 사용되는 distinguisher는 블록 암호 E의 입력 차분과 출력 차분을 만족하는 모든 차분 특성을 이용한다. 위의 각각의 차분 특성 확률을 $\Pr^*[\alpha\rightarrow\beta']$, $Pr[\gamma'\rightarrow\delta]$, $Pr^*[\gamma''\rightarrow\delta]$라 표현하고, 각각의 확률 합을 $\hat{p}^* = (\sum_{\beta} Pr^{*2}[\alpha\rightarrow\beta'])^{\frac{1}{2}}$, $\hat{q} = (\sum_{\gamma} Pr^2[\gamma'\rightarrow\delta])^{\frac{1}{2}}$, $\hat{q}^* = (\sum_{\gamma} Pr^{*2}[\gamma''\rightarrow\delta])^{\frac{1}{2}}$와 같이 표현하면, 연관키 rectangle distinguisher-1에 대한 올바른 quartet의 평균 기대값은 다음과 같다.

$$\sum_{any\ \beta',\gamma',\gamma'} \frac{(m\cdot Pr^*[\alpha\rightarrow\beta'])^2}{2}\cdot 2^{-n}\cdot (Pr^2[\gamma'\rightarrow\delta]+Pr^{*2}[\gamma''\rightarrow\delta]) = m^2\cdot 2^{-n-1}\cdot(\hat{p}^*)^2\cdot(\hat{q}^2+(\hat{q}^*)^2).$$

그러므로 만약 $\hat{p}^*\cdot(\frac{1}{2}\cdot(\hat{q}^2+(\hat{q}^*)^2))^{1/2} > 2^{-n/2}$을 만족하고, m이 충분히 크다면, 연관키 rectangle distinguisher-1을 갖는 E와 랜덤 치환 함수는 구별 가능하다.

연관키 rectangle distinguisher-1에서 올바른 quartet을 생성하는 두 가지 경로를 설명하였다. 즉, 차분 특성 $\gamma'\rightarrow\delta$(확률 $\hat{q}$와 관계된 특성)와 연관키 차분 특성 $\gamma''\rightarrow\delta$(확률 $\hat{q}^*$와 관계된 특성)를 고려한 경우이다. 두 가지 경우를 모두 사용하여 올바른 quartet의 존재 가능성 확률을 증가시킬 수 있다. 하지만 만약 $\hat{q}$와 $\hat{q}^*$중 높은 확률을 갖는 경우만을 고려한다면, 랜덤 치환 함수와 연관키 rectangle distinguisher-1을 갖는 E에 대한 올바른 quartet의 기대값의 비율은 최적이 된다. 즉, 랜덤 치환 함수에 대한 올바른 quartet의 평균 기대값은 $m^2\cdot 2^{-1}\cdot 2^{-2n}$인 반면, E에 대한 올바른 quartet의 평균 기대값은 $m^2\cdot 2^{-1}\cdot 2^{-n}\cdot(\hat{p}^*\cdot\hat{q})^2$ 또는 $m^2\cdot 2^{-1}\cdot 2^{-n}\cdot(\hat{p}^*\cdot\hat{q}^*)^2$이다. 그러므로 각각의 경우에 대해 $\hat{p}^*\cdot\hat{q} > 2^{-n/2}$ 또는 $\hat{p}^*\cdot\hat{q}^* > 2^{-n/2}$이 성립한다면, 연관키 rectangle distinguisher-1을 구성할 수 있다. 뒤에 소개할 연관키 rectangle distinguisher-1을 이용한 SHACAL-1의 연관키 rectangle 공격에서는 두 가지 경우 중 높은 확률을 갖는 $\hat{p}^*\cdot\hat{q}$을 사용한다.

2.2 연관키 rectangle distinguisher-2(그림 2)

연관키 rectangle distinguisher-1과 유사한 방법으로 그림 2에 나타난 연관키 rectangle distinguisher-2를 구성할 수 있다. P_i, P_i'는 E_k에 의해, $P_j^*, P_j'^*$는 E_{k^*}에 의해 암호화 된다고 가정하자 (단, $P_i\oplus P_i' = P_j^*\oplus P_j'^* = \alpha$이고, k, k^*는 서로 다르지만 연관된 키이다). 평문 $P_i, P_i', P_j^*, P_j'^*$에 대한 E^0의 암호문을 각각 $X_i, X_i', X_j^*, X_j'^*$라 하고, $X_i, X_i', X_j^*, X_j'^*$에 대한 E^1의 암호문을 각각 C_i, C_i', $C_j^*, C_j'^*$라 하자. 위의 가정 하에 차분 조건 $X_i\oplus X_i' = X_j^*\oplus X_j'^* = \beta$와 $X_i\oplus X_j^* = \gamma$를 만족 한다면, $X_i'\oplus X_j'^* = (X_i\oplus\beta)\oplus(X_j^*\oplus\beta) = \gamma$이 성립한다. 만약 위의 차분 조건 하에 암호문 쌍 C_i, C_j^*와 $C_i', C_j'^*$이 차분 조건 차분 δ를 만족한다면(즉, $C_i\oplus C_j^* = C_i'\oplus C_j^* = \delta$), 위의 4개의 평문 쌍 $(P_i, P_i', P_j^*,$

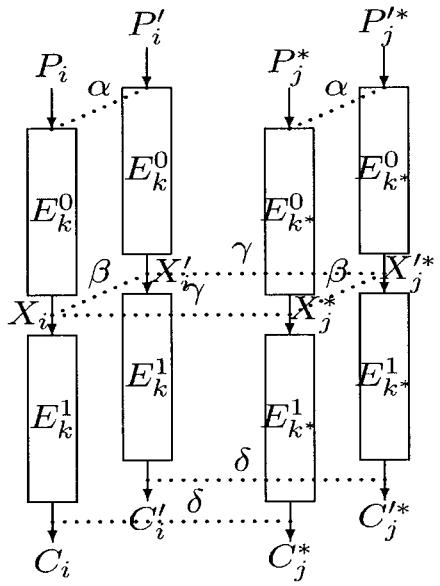


그림 2. 연관키 Rectangle Distinguisher-2

$P_j'^*$)를 올바른 quartet이라 부른다. 또한 차분 조건 $X_i \oplus X_i' = X_j^* \oplus X_j'^* = \beta$와 $X_i \oplus X_j'^* = \gamma$를 만족한다면, $X_i' \oplus X_j^* = (X_i \oplus \beta) \oplus (X_j'^* \oplus \beta) = \gamma$이 성립한다. 만약 암호문 쌍 $C_i, C_j'^*$와 C_i', C_j^*이 차분 조건 δ를 만족 한다면(즉, $C_i \oplus C_j'^* = C_i' \oplus C_j^* = \delta$), 이러한 모든 차분 조건을 만족하는 4개의 평문 쌍 $(P_i, P_i', P_j^*, P_j'^*)$ 또한 올바른 quartet이라 부른다. 처음 경우의 올바른 quartet은 그림 2에 나타나 있다.

차분 α를 만족하는 m_1개의 평문 쌍 P_i, P_i'가 있다고 가정하자. 부분 암호 E^0을 통해 차분 특성 $\alpha \rightarrow \beta$를 만족하는 평문 쌍의 개수는 약 $m_1 p$이다. 또한 차분 α를 만족하는 m_2개의 평문 쌍 $P_j^*, P_j'^*$가 있다고 가정한다면, 부분 암호 E^0을 통해 차분 특성 $\alpha \rightarrow \beta$를 만족하는 평문 쌍의 개수는 약 $m_2 p$이다. 각각의 $m_1 p$, $m_2 p$개의 평문 쌍은 $m_1 m_2 p^2$개의 quartet을 생성한다.

각각의 평문 쌍 P_i, P_i'와 $P_j^*, P_j'^*$이 E^0에 대해 차분 특성 $\alpha \rightarrow \beta$를 만족한다고 가정하자. 블록 암호의 암호화 과정에서 중간 과정의 값이 랜덤하게 분포한다고 가정하면, 확률 2^{-n}으로 차분 $X_i \oplus X_j^* = \gamma$을 얻는다. 이 경우에 올바른 quartet이 되기 위해 X_i, X_j^*와 $X_i', X_j'^*$는 확률 q^*를 갖는 연관키 차분 특성 $\gamma \rightarrow \delta$을 만족해야 한다. 따라서 차분 α을 만족하는 m_1, m_2개의 평문 쌍에 대한 올바른 quartet의 평균 기대값은 $m_1 \cdot m_2 \cdot 2^{-n} \cdot (p \cdot q^*)^2$이다. 다음은 확률 2^{-n}으로 차분 $X_i \oplus X_j'^* = \gamma$을 만족하는 경우를 고려해 보자. 이 경우 올바른 quartet이 되기 위해 $X_i, X_j'^*$와 X_i', X_j^*는 확률 q^*를 갖는 연관키 차분 특성 $\gamma \rightarrow \delta$을 만족해야 한다. 따라서 차분 α를 만족하는 m_1, m_2개의 평문 쌍에 대한 올바른 quartet의 평균 기대값은 $m_1 \cdot m_2 \cdot 2^{-n} \cdot (p \cdot q^*)^2$이다. 그러므로 올바른 quartet의 총 평균 기대값은 처음 경우와 나중 경우를 고려하여 약 $m_1 \cdot m_2 \cdot 2^{-n+1} \cdot (p \cdot q^*)^2$이다.

또한 앞에서 설명한 방법을 이용하여 연관키 rectangle distinguisher-2에 대한 올바른 quartet의 평균 기대값을 $m_1 \cdot m_2 \cdot 2^{-n+1} \cdot (\hat{p} \cdot \hat{q}^*)^2$까지 증가시킬 수 있다(단, $\hat{p} = (\sum_{\beta} Pr^2[\alpha \rightarrow \beta'])^{\frac{1}{2}}$). 랜덤 치환 함수인 경우에 올바른 quartet의 평균 기대값이 약 $m_1 \cdot m_2 \cdot 2^{-2n+1}$이므로, 만약 $\hat{p} \cdot \hat{q}^* > 2^{-n/2}$을 만족하고, m_1, m_2가 충분히 크다면, 연관키 rectangle distinguisher-2를 갖는 E와 랜덤 치환 함수는 구별 가능하다.

2.3 Rectangle distinguisher

$k = k^*$인 경우, 위에서 소개한 두 가지 형태의 연관키 rectangle distinguisher는 기존의 rectangle distinguisher[4]와 같다. 위의 분석 기법을 $k = k^*$인 경우에 적용 한다면, 주어진 m개의 평문 쌍의 올바른 quartet의 평균 기대값은 $m^2 \cdot 2^{-n} \cdot (\hat{p} \cdot \hat{q})^2$이다. 랜덤 치환 함수에 대한 올바른 quartet의 평균 기대값이 약 $m^2 \cdot 2^{-2n}$이므로, 만약 $\hat{p} \cdot \hat{q} > 2^{-n/2}$을 만족하고, m이 충분히 크다면 rectangle distinguisher를 갖는 E와 랜덤 치환 함수는 구별 가능하다.

Ⅲ. SHACAL-1 알고리즘의 소개

SAHCAL-1[7]은 해쉬 함수 SHA-1[17]의 압축 함수에 기반한 다양한 키 길이(최대 512 비트)를 가지는 160-비트 블록 암호이다. SHACAL-1의 암호화 과정은 다음과 같다.

단계 1. 160 비트 평문 $X(= X^1 \mid X^2 \mid X^3 \mid X^4 \mid X^5)$는 다음과 같이 A^0, B^0, C^0, D^0, E^0에 저장 된다. (단, X^i는 32-비트 워드이다.)

$$A^0 = X^1, B^0 = X^2, C^0 = X^3, D^0 = X^4, E^0 = X^5$$

단계 2. A^0, B^0, C^0, D^0, E^0은 총 80 라운드 암호화 과정을 수행한다. i 번째 암호화 과정은 다음과 같다.

$$A^{i+1} = W^i + ROTL_5(A^i) + f^i(B^i, C^i, D^i) + E^i + K^i$$
$$B^{i+1} = A^i$$
$$C^{i+1} = ROTL_{30}(B^i)$$
$$D^{i+1} = C^i$$
$$E^{i+1} = D^i$$

단계 3. $ROTL_j(X)$는 32-비트 워드의 j비트 왼쪽 순환을 나타내며, W^i는 라운드 키, K^i는 라운드 상수값을 의미한다. 라운드 함수 f는 라운드 i에 따라 다음과 같은 함수를 적용한다.

$f^i(B,C,D) = f_{if} = (B\&C) \mid (\neg B\&D), \quad (0 \le i \le 19)$

$f^i(B,C,D) = f_{xor} = B \oplus C \oplus D, \quad (0 \le i \le 39, 60 \le i \le 79)$

$f^i(B,C,D) = f_{maj} = (B\&C) \mid (B\&D) \mid (C\&D), (40 \le i \le 59).$

단계 4. 암호문은 $A^{80}, B^{80}, C^{80}, D^{80}, E^{80}$이다.

SHACAL-1의 키는 최대 512 비트까지 허용되며, 512 비트 보다 작은 키에 대해서는 0 비트 스트링을 패딩하여 총 512 비트를 생성하여 사용한다. 하지만 SHACAL-1은 128 비트 보다 작은 키의 사용은 지양한다. 512 비트 키를 $W=[W^0 \mid W^1 \mid \cdots \mid W^{15}]$와 같이 표시하면(단, W^i는 32-비트 워드), 2560 비트 키 확장 과정은 다음과 같다.

$W^i = ROTL_1(W^{i-3} \oplus W^{i-8} \oplus W^{i-14} \oplus W^{i-16}), \quad (16 \le i \le 79).$

Ⅳ. 57-라운드 SHACAL-1에 대한 연관키 Rectangle 공격

본 장에서는 SHACAL-1의 46-라운드 연관키 rectangle distinguisher-1을 소개하고, 이를 이용하여 57-라운드 SHACAL-1을 공격한다.

4.1. SHACAL-1의 연관키 Rectangle Distinguisher-1

SHACAL-1의 키 스케줄 알고리즘은 선형 쉬프트 귀환 레지스터로 작동한다. 따라서 모든 라운드 키는 임의의 연속된 16 라운드 키의 선형 함수로 표현 가능하다. 즉, 만약 임의의 연속된 16 라운드 키 차분을 안다면, 다른 64개 라운드의 키 차분을 알 수 있다. 연관키 rectangle distinguisher-1을 구성하기 위해 암호화 과정의 키 차분 확산을 최소화 시키는 차분 형태를 구성할 수 있다. 표 3은 trial and error 방법으로 찾아낸 키 차분으로 연관키 rectangle distinguisher-1의 구성을 가능하게 해준다. 표 3에 제시된 마스터 키의 차분은 $\Delta W = (e_{31}, e_{31}, e_{31}, e_{31}, 0, e_{31}, 0, e_{31}, 0, 0, 0, 0, 0, 0, 0, e_{31})$

표 3. SHACAL-1의 57-라운드 공격에 사용되는 연관키 특성

i	$\triangle W^i$	i	$\triangle W^i$	i	$\triangle W^i$	i	$\triangle W^i$	i	$\triangle W^i$	i	$\triangle W^i$
0	e_{31}	10	0	20	0	30	0	40	e_3	50	$e_{3,7}$
1	e_{31}	11	0	21	0	31	e_0	41	e_4	51	e_5
2	e_{31}	12	0	22	0	32	e_1	42	0	52	e_7
3	e_{31}	13	0	23	0	33	0	43	$e_{1,3,4}$	53	e_8
4	0	14	0	24	0	34	e_1	44	e_5	54	0
5	e_{31}	15	e_{31}	25	0	35	e_2	45	$e_{2,3}$	55	$e_{3,5,7,8}$
6	0	16	0	26	0	36	0	46	e_5	56	e_9
7	e_{31}	17	0	27	0	37	$e_{2,3}$	47	$e_{1,2,6}$		
8	0	18	0	28	0	38	e_3	48	e_{31}		
9	0	19	0	29	e_0	39	e_1	49	$e_{3,5,6}$		

이다.

표 4는 확률 2^{-47}를 갖는 33-라운드 연관키 차분 특성 $\alpha \rightarrow \beta$을 설명한다($\alpha = (0, e_{8,22,1}, e_{1,15}, e_{10}, e_{5,31})$, $\beta = (e_{1,5,15,30}, e_{10}, e_3, e_{30}, 0)$). 연관키 차분 특성에 사용되는 평문 쌍 P, P^*는 연관키 차분 특성 확률을 개선하기 위해 (1)과 같이 6 비트 고정된 값을 가진다. 단, 워드 X의 i 번째 비트는 x_i로 표기한다.

표 4. SHAHCAL-1의 E_0에 대한 33-라운드 연관키 차분 특성

라운드 (i)	$\triangle A^i$	$\triangle B^i$	$\triangle C^i$	$\triangle D^i$	$\triangle E^i$	$\triangle W^i$	확률
0	0	$e_{8,22,1}$	$e_{1,15}$	e_{10}	$e_{5,31}$	e_{31}	
1	e_5	0	$e_{6,20,31}$	$e_{1,15}$	e_{10}	e_{31}	2^{-3}
2	0	e_5	0	$e_{6,20,31}$	$e_{1,5}$	e_{31}	2^{-6}
3	$e_{1,15}$	0	e_3	0	$e_{6,20,31}$	e_{31}	2^{-6}
4	0	$e_{1,15}$	0	e_3	0	0	2^{-3}
5	0	0	$e_{13,31}$	0	e_3	e_{31}	2^{-3}
6	e_3	0	0	$e_{13,31}$	0	0	2^{-3}
7	e_8	e_3	0	0	$e_{13,31}$	e_{31}	2^{-3}
8	0	e_8	e_1	0	0	0	2^{-2}
9	0	0	e_6	e_1	0	0	2^{-2}
10	0	0	0	e_6	e1	0	2^{-2}
11	e_1	0	0	0	e_6	0	2^{-2}
12	0	e_1	0	0	0	0	2^{-1}
13	0	0	e_{31}	0	0	0	2^{-1}
14	0	0	0	e_{31}	0	0	2^{-1}
15	0	0	0	0	e_{31}	e_{31}	2^{-1}
16	0	0	0	0	0	0	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
28	0	0	0	0	0	0	1
29	0	0	0	0	0	e_0	1
30	e_0	0	0	0	0	0	2^{-1}
31	e_5	e_0	0	0	0	e_0	2^{-1}
32	e_{10}	e_5	e_{30}	0	0	e_1	2^2
33	$e_{1,5,15,30}$	e_{10}	e_3	e_{30}	0		2^4

표 5. SHAHCAL-1의 E_1에 대한 13-라운드 연관키 차분 특성

라운드 (i)	ΔA^i	ΔB^i	ΔC^i	ΔD^i	ΔE^i	ΔW^i	확률
33	$e_{1,3}$	$e_{1,8}$	0	$e_{3,6,31}$	$e_{1,3,31}$	0	
34	0	$e_{1,3}$	$e_{6,31}$	0	$e_{3,6,31}$	0	2^{-4}
35	e_1	0	$e_{1,31}$	$e_{6,31}$	0	0	2^{-3}
36	e_1	e_1	0	$e_{1,31}$	$e_{6,31}$	0	2^{-2}
37	0	e_1	e_{31}	0	$e_{1,31}$	0	2^{-1}
38	0	0	e_{31}	e_{31}	0	0	2^{-1}
39	0	0	0	e_{31}	e_{31}	0	1
40	0	0	0	0	e_{31}	0	1
41	e_{31}	0	0	0	0	0	1
42	e_4	e_{31}	0	0	0	0	2^{-1}
43	e_9	e_4	e_{29}	0	0	0	2^{-2}
44	e_{14}	e_9	e_2	e_{29}	0	0	2^{-3}
45	e_{19}	e_{14}	e_7	e_2	e_{29}	0	2^{-4}
46	$e_{24,29}$	e_{19}	e_{12}	e_7	e_2		2^{-5}

$$b_{10}=b_{10}^*=1,\quad b_{15}=b_{15}^*=0,\quad c_8=c_8^*=0,$$
$$c_{10}=c_{10}^*=0,\quad d_8=d_8^*=0,\quad d_{15}=d_{15}^*=0. \qquad (1)$$

표 5는 확률 2^{-26}을 가지는 13-라운드 차분 특성 $\gamma\rightarrow\delta$을 설명한다($\gamma=(e_{1,3},e_{1,8},0,e_{3,6,31},e_{1,3,31})$, $\delta=(e_{24,29},e_{19},e_{12},e_7,e_2)$). 연관키 rectangle distinguisher-1의 E^1에 대한 출력 차분 δ를 갖는 연관키 차분 특성 확률은 표 5에 제시된 차분 확률 2^{-26}보다 훨씬 작다. 따라서 E^1에 대해 연관키 차분 특성에 따른 올바른 quartet 생성 경로는 고려하지 않는다.

앞에서 언급 하였듯이 확률 $\hat{p}^*$는 E^0의 입력 차분이 α인 모든 차분 특성의 확률 합을 나타내고, 확률 $\hat{q}$는 E^1의 출력 차분이 δ인 모든 차분 특성의 확률 합을 나타낸다. 하지만 모든 경로를 다루는 것은 계산상으로 불가능하기 때문에, 높은 확률을 가지는 몇 가지 차분 특성을 고려하여 $\hat{p}^*$와 $\hat{q}$의 하한 값의 근사 값을 구한다. 표 4의 33-라운드 연관키 차분 특성 중 처음 31-라운드 특성을 만족하는 연관키 차분 특성을 고려하여 가능한 출력 차분에 따른 확률을 계산한다. 또한 표 5의 13-라운드 차분 특성 중 마지만 11-라운드 특성을 만족하는 차분 특성을 고려하여 가능한 입력 차분에 따른 확률을 계산한다. 표 6은 확률에 따른 차분 특성의 개수를 나타낸다. 따라서 확률 $\hat{p}^*$의 하한 값 $2^{-46.17}$, 확률 $\hat{q}$의 하한 값 $2^{-25.08}$을 계산할 수 있다. 확률 $\hat{p}\cdot\hat{q}^*(\approx 2^{-71.75})$은

표 6. SHAHCAL-1의 46-라운드 Distinguisher에 사용한 확률에 따른 차분 특성 개수

확률(p*)	2^{-47}	2^{-48}	2^{-49}	2^{-50}	2^{-51}	…
연관키 차분 특성 개수	1	4	11	20	42	…
확률(q)	2^{-26}	2^{-27}	2^{-28}	2^{-29}	2^{-30}	…
차분 특성 개수	1	4	13	32	68	…

2^{-80}보다 크기 때문에, 연관키 rectangle distinguisher-1을 이용하여 46-라운드 SHACAL-1과 랜덤 함수를 구별할 수 있다.

4.2. 공격 과정

본 절에서는 SHACAL-1의 46-라운드 연관키 rectangle distinguisher-1을 이용하여 512 비트 키를 사용하는 57-라운드 SHACAL-1 공격 과정을 설명한다.

단계 1. $\lceil 2^{153.75}\rceil$개의 평문 쌍 (P_i,P_i^*), $i=0,1,\cdots,\lceil 2^{153.75}\rceil-1$을 선택한다(단, 차분 $P_i\oplus P_i^*=\alpha$를 만족하고, 고정된 6 비트 조건 (1)을 만족한다). 공격자는 k를 사용한 P_i의 암호문과 k^*를 사용한 P_i^*의 암호문을 요구한다(단, k와 k^*는 표 3의 차분 특성을 만족하는 연관키이며, 공격자는 연관키의 차분 특성만 알고 있다). 따라서 $\lceil 2^{153.75}\rceil$개의 암호문 쌍 (C_i,C_i^*)를 구성할 수 있다.

단계 2. 라운드 46-56의 352-비트 부분키 쌍 (sk,sk^*)을 추측한다. 이 부분키 쌍은 표 3에 나타난 차분 특성을 만족한다.

단계 3. 단계2에서 추측한 352-비트 부분키 쌍 (sk,sk^*)에 대해서 다음 과정을 수행한다.

3-1. 라운드 46-56에 대한 부분키 sk를 사용하여 C_i을 복호화하고, 그 값을 T_i에 저장한다. 또한 라운드 46-56에 대한 부분키 sk^*를 사용하여 C_i^*을 복호화 하고 그 값을 T_i^*에 저장한다.

3-2. $0\le i_1\le i_2\le\lceil 2^{153.75}\rceil-1$인 모든 i_1,i_2에 대해 $T_{i_1}\oplus T_{i_2}=T_{i_1}^*\oplus T_{i_2}^*=\delta$의 성립 여부를

테스트 한다. 만약 이 과정을 통과하는 quartet $(T_{i_1}, T_{i_2}, T^*_{i_1}, T^*_{i_2})$의 개수가 6 미만이면, 단계 2로 돌아간다. 그렇지 않다면, 추측한 352 비트 부분키 쌍에 대해 나머지 160 비트 키에 대한 전수 조사를 수행한다. 만약 추측한 512 비트 키가 전수 조사 테스트를 통과하면 마스터 키로 출력한다. 그렇지 않으면, 단계 2로 돌아간다.

이 공격 과정의 데이터 복잡도는 약 $2^{154.75}$ 연관키 선택 평문이며, 약 $2^{159.07}(=2^{154.75}\cdot 20)$ 메모리 바이트를 요구한다($2^{154.75}$개의 암호문 저장 시 사용한다).

단계 1(데이터 수집 단계)의 시간 복잡도는 $2^{154.75}$ 57-라운드 SHACAL-1 암호화 과정을 요구한다. 단계 3-1의 시간 복잡도는 약 $2^{503.38}(\approx 2^{154.75}\cdot 2^{352}\cdot\frac{1}{2}\cdot\frac{11}{57})$ 57-라운드 SHACAL-1 암호화 과정을 요구한다. $\frac{1}{2}$은 단계 3-1에서 수행하는 352 비트 키 쌍의 평균 조사 비율을 의미한다. 단계 3-2에서 각각의 모든 가능한 quartet은 차분 조건 δ 성립 여부를 테스트 한다. 이는 해쉬 테이블을 사용하여 차분 조건 δ를 효율적으로 테스트할 수 있으므로 많은 시간 복잡도를 요구하지 않는다. 더구나 단계3-2에서 틀린 키에 대한 카운터 값이 6 이상이 될 확률은 약 $2^{-150.85}(\approx \sum_{i=6}^{t}\binom{t}{i}\cdot(2^{-160.2})^i\cdot(1-2^{-160.2})^{t-i})$ 이다(단, t는 $\lceil 2^{153.75}\rceil$개의 평문 쌍으로부터 유도되는 모든 가능한 quartet의 개수 $\lceil 2^{306.50}\rceil$을 나타낸다). 352 비트 부분 키 쌍 중 단계 3-2에서 키에 대한 카운터 값이 6 이상인 부분키 쌍의 평균 기대값은 약 $2^{260.50}(\approx 2^{352}\cdot\frac{1}{2}\cdot 2^{-90.50})$이다. 따라서 단계 3-2의 남은 키에 대한 전수 조사량은 약 $2^{420.50}(\approx 2^{260.50}\cdot 2^{160})$ 57-라운드 SHACAL-1 암호화 과정을 요구한다. 그러므로 이 공격 과정의 시간 복잡도는 약 $2^{503.38}(\approx 2^{154.75}+2^{503.38}+2^{420.50})$ 57-라운드 암호화 과정이다.

이 공격은 확률 $(\hat{p}^*\cdot\hat{q})^2(\approx(2^{-71.75})^2)$을 만족하는 46-라운드 연관키 rectangle distinguisher-1을 이용하였기 때문에, 올바른 부분키 쌍에 대한 카운터의 기대값은 약 $2^3(=\binom{2^{153.75}}{2}\cdot 2^{-160}\cdot(2^{-71.75})^2)$이다. 그러므로 이 공격의 성공 확률, 즉 올바른 부분키의 카운터 값이 6 이상인 경우는 약 $0.80(\approx\sum_{i=6}^{t}\binom{t}{i}\cdot(2^{-159}\cdot(2^{-66.72})^2)^i\cdot(1-2^{-159}\cdot(2^{-66.72})^2)^{t-i})$ 이다(단, t는 $\lceil 2^{306.50}\rceil$).

V. 59-라운드 SHACAL-1의 연관키 Rectangle 공격

본 장에서는 SAHCAL-1의 48-라운드 연관키 rectangle distinguisher-2를 소개하고, 이를 이용하여 59-라운드 SHACAL-1을 공격한다.

5.1. SHACAL-1의 연관키 Rectangle Distinguisher-2

앞에서 언급하였듯이 연관키 rectangle distinguisher-2는 부분 암호화 과정 E^0에 대해 확률 p를 가지는 차분 특성 $\alpha\rightarrow\beta$와 E^1에 대해 확률 q^*를 가지는 연관키 차분 특성 $\gamma\rightarrow\delta$으로 구성된다(단, $p\cdot q^*>2^{n/2}$). SHACAL-1의 연관키 차분 특성 $\gamma\rightarrow\delta$에 사용되는 연관키 특성은 표 7과 같으며, 표 7의 마스터 키의 차분은 $\Delta W=(0, e_{30}, e_{31}, e_{30,31}, e_{31}, e_{30,31}, e_{31}, e_{30,31}, e_{31}, e_{30}, e_{31}, e_{30,31}, e_{31}, e_{30}, e_{31})$이다.

표 8은 확률 2^{-40}을 갖는 21-라운드 차분 특성 $\alpha\rightarrow\beta$를 설명한다($\alpha=(0, e_{22}, e_{15}, e_{10}, e_5)$, $\beta=(e_{2,7,14,24,29}, e_{19}, e_{12}, e_7, e_2)$). 차분 특성 확률을 개선하기 위해 (2)와 같이 평문 쌍 P, P^*는 10 비트 고정된 값을 가진다.

표 7. SHACAL-1의 59-라운드 공격에 사용되는 연관키 특성

i	ΔW^i	i	ΔW^i	i	ΔW^i	i	ΔW^i	i	ΔW^i	i	ΔW^i
0	0	10	e_{31}	20	0	30	0	40	0	50	0
1	e_{30}	11	$e_{30,31}$	21	e_{31}	31	0	41	0	51	$e_{2,3}$
2	e_{31}	12	e_{31}	22	0	32	0	42	0	52	e_3
3	$e_{30,31}$	13	e_{30}	23	0	33	0	43	e_0	53	e_1
4	e_{31}	14	e_{31}	24	0	34	0	44	0	54	e_3
5	$e_{30,31}$	15	e_{31}	25	0	35	0	45	e_0	55	e_4
6	e_{31}	16	e_{31}	26	0	36	0	46	e_1	56	0
7	$e_{30,31}$	17	e_{31}	27	0	37	0	47	0	57	$e_{1,3,4}$
8	e_{31}	18	0	28	0	38	0	48	e_1	58	e_5
9	e_{30}	19	e_{31}	29	e_{31}	39	0	49	e_2		

표 8. SHAHCAL-1의 E_0에 대한 21-라운드 차분 특성

라운드 (i)	ΔA^i	ΔB^i	ΔC^i	ΔD^i	ΔE^i	ΔW^i	확률
0	0	e_{22}	e_{15}	e_{10}	e_5	0	
1	e_5	0	e_{20}	e_{15}	e_{10}	0	2^{-1}
2	0	e_5	0	e_{20}	e_{15}	0	2^{-1}
3	e_{15}	0	e_3	0	e_{20}	0	2^{-3}
4	0	e_{15}	0	e_3	0	0	2^{-2}
5	0	0	e_{13}	0	e_3	0	2^{-2}
6	e_3	0	0	e_{13}	0	0	2^{-2}
7	e_8	e_3	0	0	e_{13}	0	2^{-2}
8	0	e_8	e_1	0	0	0	2^{-2}
9	0	0	e_6	e_1	0	0	2^{-2}
10	0	0	0	e_6	e_1	0	2^{-2}
11	e_1	0	0	0	e_6	0	2^{-2}
12	0	e_1	0	0	0	0	2^{-1}
13	0	0	e_{31}	0	0	0	2^{-1}
14	0	0	0	e_{31}	0	0	2^{-1}
15	0	0	0	0	e_{31}	0	2^{-1}
16	e_{31}	0	0	0	0	0	1
17	e_4	e_{31}	0	0	0	0	2^{-1}
18	e_9	e_4	e_{29}	0	0	0	2^{-2}
19	e_{14}	e_9	e_2	e_{29}	0	0	2^{-3}
20	e_{19}	e_{14}	e_7	e_2	e_{29}	0	2^{-4}
21	$e_{2,7,14,24,29}$	e_{19}	e_{12}	e_7	e_2		2^{-5}

$$a_{15}=a^*_{15}=1,\ a_{20}=a^*_{20}=0,\ b_{10}=b^*_{10}=1,$$
$$b_{15}=b^*_{15}=0,\ b_{17}=b^*_{17}=0,\ c_{10}=c^*_{10}=0,$$
$$c_{20}=c^*_{20}=0,\ c_{22}=c^*_{22}=0,\ d_{15}=d^*_{15}=0,\ d_{22}=d^*_{22}=0. \quad (2)$$

표 9. SHAHCAL-1의 E_1에 대한 27-라운드 연관키 차분 특성

라운드 (i)	ΔA^i	ΔB^i	ΔC^i	ΔD^i	ΔE^i	ΔW^i	확률
21	$e_{1,8}$	0	$e_{3,6,31}$	$e_{1,3,31}$	$e_{3,13,31}$	e_{31}	
22	$e_{1,3}$	$e_{1,8}$	0	$e_{3,6,31}$	$e_{1,3,31}$	0	2^{-4}
23	0	$e_{1,3}$	$e_{6,13}$	0	$e_{3,6,31}$	0	2^{-4}
24	e_1	0	$e_{1,31}$	$e_{6,31}$	0	0	2^{-3}
25	e_1	e_1	0	$e_{1,31}$	$e_{6,31}$	0	2^{-2}
26	0	e_1	e_{31}	0	$e_{1,31}$	0	2^{-1}
27	0	0	e_{31}	e_{31}	0	0	2^{-1}
28	0	0	0	e_{31}	e_{31}	0	1
29	0	0	0	0	e_{31}	e_{31}	1
30	0	0	0	0	0	0	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
42	0	0	0	0	0	0	1
43	0	0	0	0	0	e_0	1
44	e_0	0	0	0	0	0	2^{-1}
45	e_5	e_0	0	0	0	e_0	2^{-1}
46	e_{10}	e_5	e_{30}	0	0	e_1	2^{-3}
47	$e_{1,15}$	e_{10}	e_3	e_{30}	0	0	2^{-4}
48	$e_{6,20}$	$e_{1,15}$	e_8	e_3	e_{30}		2^{-5}

표 10. SHAHCAL-1의 48-라운드 Distinguisher에 사용한 확률에 따른 차분 특성 개수

확률(p)[5]	2^{-40}	2^{-41}	2^{-42}	2^{-43}	2^{-44}	…
차분 특성 개수[5]	1	7	24	73	182	…
확률(q*)	2^{-29}	2^{-30}	2^{-31}	2^{-32}	2^{-33}	…
연관키 차분 특성 개수	1	4	13	32	68	…

표 9는 확률 2^{-29}을 가지는 27-라운드 연관키 차분 특성 $\gamma\rightarrow\delta$을 설명한다($\gamma=(e_{1,8},0,e_{3,6,31},e_{1,3,31},,e_{3,13,31})\delta=(e_{6,29},e_{1,15},e_8,e_3,e_{30})$).

확률 $\hat{p}$, $\hat{q}^*$의 하한 값을 구하기 위해 앞 단원에서 사용한 방법을 이용한다. 표 10에 의하면 확률 $\hat{p}$의 하한 값을 $2^{-38.64}$으로, 확률 $\hat{q}^*$의 하한 값을 $2^{-28.08}$으로 개선할 수 있다. 확률 $\hat{p}\cdot\hat{q}^*(\approx 2^{-66.72})$은 2^{-80}보다 크기 때문에, 연관키 rectangle distinguisher-2를 이용하여 48-라운드 SHACAL-1과 랜덤 함수를 구별할 수 있다.

5.2. 공격 과정

본 절에서는 SHACAL-1의 48-라운드 연관키 rectangle distinguisher-2를 이용하여 512 비트 키를 사용하는 59-라운드 SHACAL-1 공격 과정을 설명한다.

단계 1. $\lceil 2^{147.72}\rceil$개의 평문 쌍 (P_i,P_i')와 같은 수의 평문 쌍 $(P_j^*,P_j'^*)$, $i,j=0,1,\cdots,\lceil 2^{147.72}\rceil-1$을 선택한다(단, 각 평문 쌍은 $P_i\oplus P_i'=\alpha$와 $P_j^*\oplus P_j'^*=\alpha$를 만족하고, 고정된 10 비트 조건 (2)을 만족한다). 공격자는 k를 사용한 P_i와 P_i'의 암호문과 k^*를 사용한 $P_j^*,P_j'^*$의 암호문을 요구한다(단, k와 k^*는 표 7의 차분 특성을 만족하는 연관키이며, 공격자는 연관키의 차분 특성만 알고 있다). 따라서 $\lceil 2^{147.72}\rceil$개의 암호문 쌍 (C_i,C_i')와 같은 수의 암호문 쌍 $(C_j^*,C_j'^*)$을 구성할 수 있다.

단계 2. 라운드 48-58의 352-비트 부분키 쌍 (sk,sk^*)을 추측한다. 이 부분키 쌍은

표 7에 나타난 차분 특성을 만족한다.

단계 3. 단계 2에서 추측한 352-비트 부분키 쌍 (sk, sk^*)에 대해서 다음 과정을 수행한다.

3-1. 라운드 48-58에 대한 부분키 sk를 사용하여 C_i와 C_i'를 복호화하고, 그 값을 T_i, T_i'에 저장한다. 또한 라운드 48-58에 대한 부분키 sk^*를 사용하여 $C_j^*, C_j'^*$을 복호화 하고 그 값을 $T_j^*, T_j'^*$에 저장한다.

3-2. $0 \le i_1 \le i_2 \le \lceil 2^{147.72} \rceil - 1$인 모든 i_1, i_2에 대해 $T_{i_1} \oplus T_{i_2}^* = T_{i_1}' \oplus T_{i_2}'^* = \delta$ 또는 $T_{i_1} \oplus T_{i_2}'^* = T_{i_1}' \oplus T_{i_2}^* = \delta$성립 여부를 테스트 한다. 만약 이 과정을 통과하는 quartet $(T_{i_1}, T_{i_2}^*, T_{i_1}', T_{i_2}'^*)$의 개수가 6 미만이면, 단계2로 돌아간다. 그렇지 않다면, 추측한 352 비트 부분키 쌍에 대해 나머지 160비트 키에 대한 전수 조사를 수행한다. 만약 추측한 512 비트 키가 전수 조사 테스트를 통과하면 마스터 키로 출력한다. 그렇지 않으면, 단계2로 돌아간다.

이 공격 과정의 데이터 복잡도는 약 $2^{149.72}$ 연관키 선택 평문이며, 약 $2^{154.05}$ ($=2^{149.72} \cdot 20$) 메모리 바이트를 요구한다($2^{149.72}$개의 암호문 저장 시 사용한다).

단계 1(데이터 수집 단계)의 시간 복잡도는 $2^{149.72}$ 59-라운드 SHACAL-1 암호화 과정을 요구한다. 단계 3-1의 시간 복잡도는 약 $2^{498.30}$ ($\approx 2^{149.72} \cdot 2^{352} \cdot \frac{1}{2} \cdot \frac{11}{59}$) 59-라운드 SHACAL-1 암호화 과정을 요구한다. $\frac{1}{2}$은 단계 3-1에서 수행하는 352-비트 키 쌍의 평균 조사 비율을 의미한다. 앞에서 언급한 것과 같이 단계 3-2의 차분 δ 만족 여부 테스트는 해쉬 테이블을 이용하여 효율적으로 수행할 수 있다. 단계3-2에서 틀린 키에 대한 카운터 값이 6 이상이 될 확률은 약 $2^{-150.85}$ ($\approx \sum_{i=6}^{t} \left(\binom{t}{i} \cdot (2^{-160.2})^i \cdot (1-2^{-160.2})^{t-i} \right)$)이다(단, t는 $2 \cdot \lceil 2^{147.72} \rceil$개의 평문 쌍으로부터 유도되는 모든 가능한 quartet의 개수 $\lceil 2^{296.44} \rceil$을 나타낸다). 352 비트 부분 키 쌍 중 단계3-2에서 키에 대한 카운터 값이 6 이상인 부분키 쌍의 평균 기대값은 약 $2^{200.15}$ ($\approx 2^{352} \cdot \frac{1}{2} \cdot 2^{-150.85}$)이다. 따라서 단계 3-2의 남은 키에 대한 전수 조사량은 약 $2^{360.15}$ ($\approx 2^{200.15} \cdot 2^{160}$) 59-라운드 SHACAL-1 암호화 과정이다. 그러므로 이 공격 과정의 시간 복잡도는 약 $2^{498.30}$ ($\approx 2^{149.72} + 2^{498.30} + 2^{360.15}$) 59-라운드 암호화 과정을 요구한다.

이 공격은 확률 $(\hat{p} \cdot \hat{q}^*)^2$ ($\approx (2^{-66.72})^2$)을 만족하는 48-라운드 연관키 rectangle distinguisher-2를 이용하였기 때문에, 올바른 부분키 쌍에 대한 카운터의 기대값은 약 2^3 ($= (2^{147.72})^2 \cdot 2^{-159} \cdot (2^{-66.72})^2$)이다. 그러므로 이 공격의 성공 확률, 즉, 올바른 부분키의 카운터 값이 6 이상인 경우는 약 0.80 ($\approx \sum_{i=6}^{t} \left(\binom{t}{i} \cdot (2^{-159} \cdot (2^{-66.72})^2)^i \cdot (1 - 2^{-159} \cdot (2^{-66.72})^2)^{t-i} \right)$)이다(단, t는 $\lceil 2^{295.44} \rceil$).

V. 결 론

Rectangle 공격과 연관키 공격은 매우 잘 알려진 강력한 블록 암호 분석 기법이다. 본 논문에서는 Rectangle 분석 기법과 연관키 분석 기법을 효과적으로 결합하여 512-비트 키를 사용하는 59-라운드 SHACAL-1을 $2^{149.72}$선택 평문과 $2^{498.30}$ 59-라운드 암호화 과정으로 전수 조사 보다 빠른 공격을 소개하였다. 연관키 Rectangle 분석 기법은 안전한 키 스케줄을 사용하는 블록 암호에는 적용이 어렵지만, 알고리즘 설계자는 연관키 Rectangle 분석 기법을 고려하여 블록 암호를 고안하여야 한다.

참 고 문 헌

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like Cryptosystems," Advances in Cryptology-CRYPTO'90, LNCS 537, pp. 2-21, Springer-Verlag, 1990.

[2] E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys," Journal of Cryptology, v. 7, n. 4, pp. 229-246, 1994.

[3] E. Biham, A. Biryukov and A. Shamir, "Cryptanalysis of skipjack re-

duced to 31 rounds using impossible differentials," Advances in Cryptology-EUROCRYPT'99, LNCS 1592, pp. 12-23, Springer-Verlag, 1999.

[4] E. Biham, O. Dunkelman and N. Keller, "The Rectangle Attack-Rectangling the Serpent," Advances in Cryptology-EUROCRYPT'01, LNCS 2045, pp. 340-357, Springer-Verlag, 2001.

[5] E. Biham, O. Dunkelman and N. Keller, "Rectangle Attacks on 49-Round SHACAL-1," Advances in Cryptology-FSE '03, LNCS 2887, pp. 22-35, Springer-Verlag, 2003.

[6] M. Blunden and A. Escott, "Related Key Attacks on Reduced Round KASUMI," Advances in Cryptology-FSE '01, LNCS 2355, pp. 277-285, Springer-Verlag, 2001.

[7] H. Handschuh and D. Naccache, "SHACAL : A Family of Block Ciphers," Submission to the NESSIE project, 2000.

[8] S. Hong, J. Kim, G. Kim, J. Sung, C. Lee and S. Lee, "Impossible Differential Attack on 30-round SHACAL-2," Advances in Cryptology-INDOCRYPT '03, LNCS 2904, pp. 97-106, Springer-Verlag, 2003.

[9] G. Jakimoski and Y.Desmedt, "Related-Key Differential Cryptanalysis of 192-bit Key AES Variants," SAC'03, To appear.

[10] J. Kelsey, B. Schneier and D. Wagner, "Key Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES," Advances in Cryptology-CRYPTO'96, LNCS 1109, pp. 237-251, Springer-Verlag, 1996.

[11] J. Kelsey, B. Schneier and D. Wagner," Related Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA," Advances in Cryptology - ICICS'97, LNCS 1334, pp. 223-246, Springer-Verlag, 1997.

[12] J. Kelsey, T. Kohno, and B. Schneier, "Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent," Advances in Cryptology-FSE'01, LNCS 1978, pp. 75-93, Springer-Verlag, 2001.

[13] 김종성, 문덕재, 이원일, 홍석희, 이상진, "SHACAL의 축소 라운드에 대한 확장된 부메랑 공격," 정보보호학회논문지, 12(5), pp. 87-93, October, 2002.

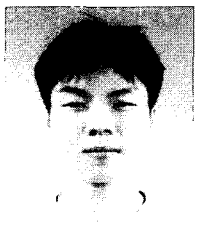
[14] L.R. Knudsen, "Truncated and Higher Order Differenatials," Advances in Cryptology - FSE'96, LNCS 1039, pp. 196-211, Springer-Verlag, 1996.

[15] 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," FSE'04, To appear.

[16] D. Wagner, "The Boomerang Attack," Advances in Cryptology-FSE'99, LNCS 1636, pp. 156-170, Springer-Verlag, 1999.

[17] U.S. Department of Commerce.FIPS 180-1: Secure Hash Standard ,Federal Information Processing Standards Publication, N.I.S.T., April 1995.

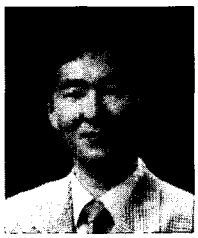
〈著者紹介〉



김 종 성 (Jong-Sung Kim)
2000년 8월 : 고려대학교 수학과 학사
2002년 8월 : 고려대학교 수학과 석사
2002년 8월~현재 : 고려대학교 정보보호대학원 박사 과정
〈관심분야〉 블록 암호 및 스트림 암호의 분석과 설계

김 구 일 (Gu-il Kim)
2002년 2월 : 고려대학교 수학과 학사
2002년 9월 : 고려대학교 정보보호대학원 석사 과정
〈관심분야〉 블록 암호 및 스트림 암호의 분석과 설계

홍 석 희 (Seok-hie Hong) 정회원
1995년 2월 : 고려대학교 수학과 학사
1997년 2월 : 고려대학교 수학과 석사
2001년 2월 : 고려대학교 수학과 박사
2000년 8월~현재 : 고려대학교 정보보호기술연구센터 연구원
〈관심분야〉 정보보호 암호 알고리즘, 비밀키 암호 설계 및 분석, 패스워드 기반 프로토콜



이 상 진 (Samgjin Lee) 종신회원
1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월~현재 : 고려대학교 정보보호대학원 부교수
〈관심분야〉 대칭키 암호의 분석 및 설계, 정보은닉이론, 컴퓨터 포렌식