情報保護學會論文誌
第14券 第3號, 2004. 6

30 라운드 SHACAL-2의 불능 차분 공격*

홍 석 희[a)†], 김 종 성[a)], 김 구 일[a)], 이 창 훈[a)], 성 재 철[b)‡], 이 상 진[a)]
고려대학교 정보보호기술연구센터[a)], 서울시립대학교 수학과[b)]

Impossible Differential Attack on 30-Round SHACAL-2

Seokhie Hong[a)†], Jongsung Kim[a)], Guil Kim[a)], Changhoon Lee[a)],
Jae-chul Sung[b)‡], Sangjin Lee[a)]
Center for Information of Security of Technologies, Korea University[a)]
Department of Mathematics, University of Seoul[b)]

요 약

SHACAL-2는 국제 표준 해쉬 알고리즘 SHA-2의 압축 함수에 기반을 둔 최대 512 비트 키 크기를 가지는 256 비트 블록 암호이다. 최근에 SHACAL-2는 NESSIE 프로젝트의 256 비트 블록 암호에 선정되었으며, 현재까지 SHACAL-2의 안전성에 대한 문제점은 제기되지 않았다. 본 논문에서는 불능 차분 공격에 대한 SHACAL-2의 안전성을 논의한다. 본 논문은 두 가지 형태의 14 라운드 불능 차분 특성을 구성한다. 이를 이용하여 512 비트 키를 사용하는 30 라운드 SHACAL-2의 공격을 소개한다. 공격 결과를 요약하면 744개의 선택 평문을 가지고 $2^{495.1}$ 30 라운드 SHACAL-2 암호화 과정의 시간 복잡도로 전수 조사 과정보다 빠른 30 라운드 SHACAL-2의 공격이 가능하다.

ABSTRACT

SHACAL-2 is a 256 bit block cipher with various key sizes based on the hash function SHA-2. Recently, it was recommended as one of the NESSIE selections. Up to now, no security flaws have been found in SHACAL-2. In this paper, we discuss the security of SHACAL-2 against an impossible differential attack. We propose two types of 14 round impossible characteristics and using them, we attack 30 round SHACAL-2 with 512 bit key. This attack requires 744 chosen plaintexts and has time complexity of $2^{495.1}$ 30 round SHACAL-2 encryptions.

Keywords : SHACLA-2, IDC(Impossible differential cryptanalysis), NESSIE, SHA-2

Ⅰ. 서 론

SHACAL-2[2]는 NESSIE(New European Schemes for Signatures, Integrity, and Encryption) 프로젝트에 제안된 블록 암호로서 H. Handschuh와 D. Naccache에 의해 설계된 64 라운드 블록 암호이다. 이는 국제 표준 해쉬 알고리즘 SHA-2[4]의 압축 함수에 기반을 두었으며, 최근 NESSIE 프로젝트의 256 비트 블록 암호로 선정 되었다.

SHACAL-2[2]는 블록 암호로서 다음과 같은 몇 가지 이점을 갖는다. 우선 SHACAL-2는 해쉬 함수 SHA-2[4]에 기반을 두고 있기 때문에, 다양한 환경에 적용 가능한 SHA-2의 구현을 공유할 수 있다. 그리고 SHA-2와 SAHCAL-2의 분석 과정은 밀접한 관계가 있으므로, SHA-2에 대한 분석 결과는

접수일 : 2004년 3월23일 ; 채택일 : 2004년 5월 27일
* 본 연구는 정보통신부 대학 IT 연구센터 육성·지원 사업의 연구 결과로 수행되었습니다.
† 주저자, hsh@cist.korea.ac.kr
‡ 교신저자, jcsung@uos.ac.kr

SHACAL-2의 안전성을 평가하는데 큰 도움을 줄 수 있다. 현재까지 SHA-2의 안전성에 대한 문제점은 제기되지 않았으며, 이는 SHACAL-2가 안전한 블록 암호라는 신뢰성을 증가 시켜준다.

본 논문에서는 SHACAL-2의 축소 라운드(전체 64 라운드 중 30 라운드)가 불능 차분 공격[1,3]에 취약할 수 있음을 보인다. 본 논문은 두 가지 형태의 11 라운드 불능 차분 특성과 각각에 3 라운드 비선형 방정식을 결합한 두 가지 형태의 14 라운드 불능 차분 특성을 구성한다. 이를 이용하여 744 선택 평문의 데이터 복잡도와 $2^{495.1}$ 30 라운드 SHACAL-2 암호화 과정의 시간 복잡도를 가지고 30 라운드 SHACAL-2를 공격한다.

Ⅱ. SHACAL-2 블록 암호의 소개

SHACAL-2[2]는 다양한 키 길이(최대 512 비트)를 가지는 256 비트 블록 암호이다. 이는 NIST에 의해 소개된 국제 표준 해쉬 함수 알고리즘 SHA-2[4]의 압축 함수에 기반을 두고 있다. SHACAL-2 암호화 과정은 다음과 같다.

256 비트 평문은 여덟 개의 32 비트 워드 A, B, C, D, E, F, G, H로 분할된다. 32 비트 워드 X^i를 i번째 라운드 입력 값이라 하면, 평문 P는 A^0, B^0, C^0, D^0, E^0, F^0, G^0, H^0으로 표현되며, 64 라운드 과정을 거친 암호문은 A^{64}, B^{64}, C^{64}, D^{64}, E^{64}, F^{64}, G^{64}, H^{64}이 된다. i번째 라운드 암호화 과정은 다음과 같다.

$$T_1^{i+1} = H^i + \sum_1(E^i) + Ch(E^i, F^i, G^i) + K^i + W^i \quad (1)$$

$$T_2^{i+1} = \sum_0(A^i) + Maj(A^i, B^i, C^i) \quad (2)$$

$$H^{i+1} = G^i \quad (3)$$

$$G^{i+1} = F^i \quad (4)$$

$$F^{i+1} = E^i \quad (5)$$

$$E^{i+1} = D^i + T_1^{i+1} \quad (6)$$

$$D^{i+1} = C^i \quad (7)$$

$$C^{i+1} = B^i \quad (8)$$

$$B^{i+1} = A^i \quad (9)$$

$$A^{i+1} = T_1^{i+1} + T_2^{i+1} \quad (10)$$

+는 법 2^{32} 덧셈을 의미하며, W^i는 32 비트 라운드 키, K^i는 32 비트 라운드 상수 값이다(각 라운드 상수 값은 [4]를 참조). 위에 정의된 i번째 라운드 암호화 과정에 사용하는 함수는 다음과 같다.

$$Ch(X,Y,Z) = (X \& Y) \oplus (\neg X \& Z)$$
$$Maj(X,Y,Z) = (X \& Y) \oplus (X \& Z) \oplus (Y \& Z)$$

$$\sum_0(X) = S_2(X) \oplus S_{13}(X) \oplus S_{22}(X)$$

$$\sum_1(X) = S_6(X) \oplus S_{11}(X) \oplus S_{25}(X)$$

$\neg X$는 32 비트 워드 X의 보수를 의미하며, $S_i(X)$는 32 비트 워드 X의 i 비트 오른쪽 순환을 의미한다.

한편, 성질 $X - Y = X + (2^{32} - 1 - Y) + 1 = X + (\neg Y) + 1$을 이용하여, $i+1$번째 라운드 복호화 과정을 다음과 같이 나타낼 수 있다.

$$\begin{aligned} T_1^{i+1} &= A^{i+1} - \sum_0(B^{i+1}) - Maj(B^{i+1}, C^{i+1}, D^{i+1}) \\ &= A^{i+1} + (\neg\sum_0(B^{i+1})) + (\neg Maj(B^{i+1}, C^{i+1}, D^{i+1})) + 2 \end{aligned} \quad (11)$$

$$\begin{aligned} H^i &= T_1^{i+1} - \sum_1(F^{i+1}) - Ch(F^{i+1}, G^{i+1}, H^{i+1}) - K^i - W^i \\ &= T_1^{i+1} + (\neg\sum_1(F^{i+1})) + (\neg Ch(F^{i+1}, G^{i+1}, H^{i+1})) \\ &\quad + (\neg K^i) + (\neg W^i) + 4 \end{aligned} \quad (12)$$

$$G^i = H^{i+1} \quad (13)$$

$$F^i = G^{i+1} \quad (14)$$

$$E^i = F^{i+1} \quad (15)$$

$$D^i = E^{i+1} - T_1^{i+1} = E^{i+1} + (\neg T_1^{i+1}) + 1 \quad (16)$$

$$C^i = D^{i+1} \quad (17)$$

$$B^i = C^{i+1} \quad (18)$$

$$A^i = B^{i+1} \quad (19)$$

SHACAL-2의 키는 최대 512 비트이며, 512 비트 보다 작은 키에 대해서는 0 비트 스트링을 패딩하여 총 512 비트를 생성한 후 사용한다. 하지만

SHACAL-2에서 128비트보다 작은 키의 사용은 지양한다.

512 비트 키 스트링을 $W=[W^0 \| W^1 \| \cdots \| W^{15}]$와 같이 표시하면, 2048 비트 키로의 확장 과정은 다음과 같다.

$$W^i=\sigma_1(W^{i-2})+W^{i-7}+\sigma_0(W^{i-15})+W^{i-16},\ 16\le i\le 63.$$
$$\sigma_0(x)=S_7(x)\oplus S_{18}(x)\oplus R_3(x)$$
$$\sigma_1(x)=S_{17}(x)\oplus S_{19}(x)\oplus R_{10}(x)$$

$R_i(x)$는 32 비트 워드 X의 i 비트 오른쪽 쉬프트를 의미한다.

Ⅲ. SHACAL-2 불능 차분 특성

본 장에서는 두 가지 형태의 14 라운드 SHACAL-2의 불능 차분 특성을 소개한다. 이 특성은 11 라운드 불능 차분 특성과 3 라운드 비선형 방정식을 결합하여 얻어진다. 먼저 두 가지 형태의 11 라운드 부정 차분 특성을 구성하고, 이 차분 특성이 불능 차분 특성으로 변화될 수 있음을 설명한다. 두 가지 형태의 11 라운드 불능 차분 특성은 첫 번째 라운드 키 W^0의 최상위 비트 값에 따라 결정된다. 즉, 만약 W^0의 최상위 비트 값이 0이라면, 두 가지 불능 차분 특성 중 하나가 확률 1로 만족하며, W^0의 최상위 비트 값이 1이라면, 또 다른 하나의 불능 차분 특성이 확률 1로 만족한다. 다음 과정은 확률 1을 가지는 3라운드 비선형 방정식을 복호화 과정을 통해 유도한다. 3 라운드 비선형 방정식은 두 가지 형태의 11 라운드 불능 차분 특성을 14 라운드 불능 차분 특성으로 확장시킬 수 있다. 차분특성식의 설명에 앞서 본 논문에서 사용하는 표기법을 정의한다. 단, 워드의 비트 위치는 가장 오른쪽 최하위 비트부터 0으로 시작 하며, 왼쪽으로 갈수록 증가한다.

- P : 256 비트 평문, $P=(A^0,\cdots,H^0)$.
- P^r: r번째 라운드의 256 비트 입력값, $P^r=(A^r,\cdots,H^r)$.
- x_i^r : X^r의 i번째 비트, $X^r\in\{A^r\cdots,H^r,W^r,K^r\}$
- $t_{1,i}^r$: T_1^r의 i번째 비트.
- ? : 알 수 없는 32 비트 워드.
- e_i : i번째 비트를 제외한 모든 자리에 0 값을 갖는 32 비트 워드.
- $\sim e_i$: $0\sim(i-1)$번째 자리의 값은 0, i번째 자리의 값은 1, $(i+1)\sim 31$번째 자리의 값은 알지 못하는 값을 갖는 워드.
- $e_{i_1,\cdots,i_k}$: $e_{i_1}\oplus\cdots\oplus e_{i_k}$

3.1. 11 라운드 불능 차분 특성

SHACAL-2는 r 라운드에서 라운드 $r+10$까지 확률 1을 가지는 11 라운드 부정 차분 특성이 존재한다. 본 논문에서는 라운드 0-10에 대한 두 가지 형태의 11 라운드 불능 차분 특성을 소개한다. 첫 번째로 라운드 2-10에 대해 확률 1로 만족하는 9 라운드 부정 차분 특성을 설명한다. 확률 1을 가지는 부정 차분 특성은 불능 차분 특성으로 바꾸어 생각할 수 있으며 본 논문은 불능 차분 특성을 이용한다. 두 번째로 라운드 1과 라운드 0의 입력 차분 형태를 구성하는 방법을 설명한다.

표 1은 라운드 2-10에 대한 확률 1을 가지는 9라운드 부정 차분 특성을 나타낸다. 표 1에서 각 행은 XOR 차분을 나타낸다. 표 1은 다음과 같은 차분 성질을 이용하여 쉽게 확인할 수 있다.

성질 1. $X\oplus X^*=e_i$라면, $\sum_0$의 출력 차분은 다음과 같다.

$$\sum_0(X)\oplus\sum_0(X^*)=e_{i-2(\mathrm{mod}\ 32),i-13(\mathrm{mod}\ 32),i-22(\mathrm{mod}\ 32)}$$

성질 2. $X\oplus X^*=e_i$라면, $\sum_1$의 출력 차분은 다음과 같다.

$$\sum_1(X)\oplus\sum_1(X^*)=e_{i-6(\mathrm{mod}\ 32),i-11(\mathrm{mod}\ 32),i-25(\mathrm{mod}\ 32)}$$

성질 3. $X\oplus X^*=\sim e_i$, $Y\oplus Y^*=\sim e_j$, 그리고 $i>j$ 라면, 다음을 만족한다.

$$(X+Y)\oplus(X^*+Y^*)=\sim e_j$$

표 1은 $(0,0,0,e_{31},0,0,0,e_{31})\rightarrow(?,?,?,?,?,?,?,\sim$

e_6)형태인 9 라운드 부정 차분 특성을 보여준다. 이 부정 차분 특성은 입력 차분 형태가 $(0,0,0,e_{31},0,0,0,e_{31})$라면, 9 라운드 후에 여덟 번째 워드의 최하위 비트 출력 차분 Δh_0^{11}은 0이 됨을 의미하며, 이는 Δh_0^{11}이 절대로 1이 될 수 없음을 의미한다. 이 사실은 다음과 같은 9 라운드 불능 차분 특성을 가능케 한다.(ΔH^{11}의 최하위 비트는 1이다)

표 1. 확률 1을 가지는 9-라운드 부정 차분 특성

라운드 (r)	ΔA^r	ΔB^r	ΔC^r	ΔD^r	ΔE^r	ΔF^r	ΔG^r	ΔH^r
입력 (r = 2)	0	0	0	e_{31}	0	0	0	e_{31}
3	e_{31}	0	0	0	0	0	0	0
4	$\sim e_9$	e_{31}	0	0	0	0	0	0
5	?	$\sim e_9$	e_{31}	0	0	0	0	0
6	?	?	$\sim e_9$	e_{31}	0	0	0	0
7	?	?	?	$\sim e_9$	e_{31}	0	0	0
8	?	?	?	?	$\sim e_6$	e_{31}	0	0
9	?	?	?	?	?	$\sim e_6$	e_{31}	0
10	?	?	?	?	?	?	$\sim e_6$	e_{31}
출력	?	?	?	?	?	?	?	$\sim e_6$

$$(0,0,0,e_{31},0,0,0,e_{31}) \nrightarrow (?,?,?,?,?,?,?,?,\Delta H^{11}) \quad (20)$$

본 논문에서는 표 1에 나타나 있는 9 라운드 부정 차분 특성 대신에 (20)에 나타난 9 라운드 불능 차분 특성을 사용한다.

지금부터 라운드 1과 라운드 0의 입력 차분의 구성 방법에 대해 살펴보자. 먼저 라운드 1의 입력 차분을 구성한다. 평문 쌍을 (P,P^*)라 표시하면, 2 라운드 차분 $P^2 \oplus P^{*2}=(0,0,0,e_{31},0,0,0,e_{31})$을 만족하기 위해서, 1 라운드 차분 형태는 최소한 $\Delta A^1=\Delta B^1=\Delta E^1=\Delta F^1=0$, $\Delta C^1=\Delta G^1=e_{31}$을 만족해야 한다. 하지만, $a_{31}^1, b_{31}^1, e_{31}^1, a_{31}^{*1}, b_{31}^{*1}, e_{31}^{*1}$의 값을 고려하지 않고, 단지 ΔD^1그리고 ΔH^1 을 조절하여 P^2, P^{*2}의 원하는 차분 특성을 꾸밀 수 없다. 따라서, ΔD^1, ΔH^1뿐만 아니라, $a_{31}^1, b_{31}^1, e_{31}^1, a_{31}^{*1}, b_{31}^{*1}, e_{31}^{*1}$값을 조절해야 한다. 조사 결과 여덟 가지 형태의 P^1, P^{*1}쌍이 $P^2 \oplus P^{*2}=(0,0,0,e_{31},0,0,0,e_{31})$을 만족하며, 각 차분 형태와 상태 값은 표 2에 나타나 있다.

다음은 라운드 0의 입력 차분, 즉, 평문쌍 P,P^*의 차분을 구성하는 방법을 설명한다. $a_{31}^1, e_{31}^1, a_{31}^{*1}, e_{31}^{*1}$ 값은 라운드 키 W^0의 영향을 받고, 그 값들은 표 2에서와 같이 고정된 값을 갖는다. 따라서, 표 2에 나타난 라운드 1의 입력 차분 및 상태 값을 만족하기 위해서는 P,P^*의 특정 비트 뿐만 아니라, 라운드 키 W^0의 최상위 비트 w_{31}^0까지 고려해야 한다. 즉, w_{31}^0값에 따라 P,P^*의 특정 비트를 고정하여 $P^1 \oplus P^{*1}$의 값이 표 2에서 제시된 8개의 형태 중의 하나가 되게 하는 방법을 사용한다.

표 2. 라운드 1의 여덟 가지 형태의 입력 차분

형태	ΔA^1	ΔB^1	ΔC^1	ΔD^1	ΔE^1	ΔF^1	ΔG^1	ΔH^1	상태
0	0	0	e_{31}	0	0	0	e_{31}	0	$a_{31}^1=0, b_{31}^1=0, e_{31}^1=1,$ $(a_{31}^{*1}=0, b_{31}^{*1}=0, e_{31}^{*1}=1)$
1	0	0	e_{31}	0	0	0	e_{31}	0	$a_{31}^1=1, b_{31}^1=1, e_{31}^1=1$ $(a_{31}^{*1}=1, b_{31}^{*1}=1, e_{31}^{*1}=1)$
2	0	0	e_{31}	0	0	0	e_{31}	e_{31}	$a_{31}^1=0, b_{31}^1=0, e_{31}^1=0$ $(a_{31}^{*1}=0, b_{31}^{*1}=0, e_{31}^{*1}=0)$
3	0	0	e_{31}	0	0	0	e_{31}	e_{31}	$a_{31}^1=1, b_{31}^1=1, e_{31}^1=0$ $(a_{31}^{*1}=1, b_{31}^{*1}=1, e_{31}^{*1}=0)$
4	0	0	e_{31}	e_{31}	0	0	e_{31}	0	$a_{31}^1=1, b_{31}^1=0, e_{31}^1=0$ $(a_{31}^{*1}=1, b_{31}^{*1}=0, e_{31}^{*1}=0)$
5	0	0	e_{31}	e_{31}	0	0	e_{31}	0	$a_{31}^1=0, b_{31}^1=1, e_{31}^1=0$ $(a_{31}^{*1}=0, b_{31}^{*1}=1, e_{31}^{*1}=0)$
6	0	0	e_{31}	e_{31}	0	0	e_{31}	e_{31}	$a_{31}^1=0, b_{31}^1=1, e_{31}^1=1$ $(a_{31}^{*1}=0, b_{31}^{*1}=1, e_{31}^{*1}=1)$
7	0	0	e_{31}	e_{31}	0	0	e_{31}	e_{31}	$a_{31}^1=1, b_{31}^1=0, e_{31}^1=1$ $(a_{31}^{*1}=1, b_{31}^{*1}=0, e_{31}^{*1}=1)$

차분 $(0,e_{31},0,0,0,e_{31},0,0)$을 갖는 평문쌍 P,P^*는 다음과 같은 조건을 만족한다고 가정하자.

$$A^0=C^0=0,\ D^0=2^{31},\ e_{31}^0=g_{31}^0=0$$

$$H^0=-(\sum\nolimits_1(E^0)+Ch(E^0,F^0,G^0)+K^0)$$
$$A^{*0}=C^{*0}=0,\ D^{*0}=2^{31},\ e_{31}^{*0}=g_{31}^{*0}=0$$

$$H^{*0}=-(\sum\nolimits_1(E^{*0})+Ch(E^{*0},F^{*0},G^{*0})+K^{*0}) \quad (21)$$

위의 조건을 만족하고 $w_{31}^0=0$인 경우, P,P^*의 1 라운드 암호화 과정 후 P^1,P^{*1} 차분은 표 2의 형태 0을 나타낸다. 이유는 다음과 같다.

암호화 과정을 통해 $\Delta B^1=\Delta D^1=\Delta F^1=\Delta H^1=0$과 $\Delta C^1=\Delta G^1=e_{31}$을 만족한다. 위의 조건 (21)로부터 $T_1^1=T_1^{*1}=W^0$, $T_2^1=T_2^{*1}=0$ 와 $b_{31}^1=b_{31}^{*1}=0$을 확인할 수 있다. 또한 이 값을 식 (6)과 (10)에 적용하여 E^1과 E^{*1}은 W^0+2^{31}과 같음을 확인할 수 있고(즉, $\Delta E^1=0$), A^1과 A^{*1}은 W^0과 같음을 확인할 수 있다(즉, $\Delta A^1=0$). 따라서 $w_{31}^0=0$인 경우, $a_{31}^1=a_{31}^{*1}=0$과 $e_{31}^1=e_{31}^{*1}=1$을 만족됨을 알 수

있다. 그러므로 표 2에 나타난 P^1, P^{*1}의 차분 형태 0을 만족하는 P, P^*를 구성할 수 있다. 위와 같은 상태를 만족하는 평문쌍 (P, P^*)의 차분을 D_0이라고 표시한다. 즉, $P \oplus P^* = D_0$(표 3).

다음은 차분 $(0, e_{31}, e_{31}, 0, 0, e_{31}, 0, 0)$을 갖고, 조건 (22)를 만족하는 평문쌍 P, P^{**}를 가정하자.

$$A^0 = C^0 = 0,\ D^0 = 2^{31},\ b_{31}^0 = 1, e_{31}^0 = g_{31}^0 = 0,$$
$$H^0 = -(\sum_1(E^0) + Ch(E^0, F^0, G^0) + K^0$$
$$A^{**0} = C^{**0} = 0,\ D^{**0} = 2^{31},\ b_{31}^{**0} = 0,\ e_{31}^{**0} = g_{31}^{**0} = 0,$$
$$H^{**0} = -(\sum_1(E^{**0}) + Ch(E^{**0}, F^{**0}, G^{**0}) + K^{**0} \quad (22)$$

위의 조건을 만족하고 $w_{31}^0 = 1$인 경우, P, P^{**}의 1라운드 암호화 과정 후 P^1, P^{**1} 차분은 표 2의 형태 4를 만족함을 알 수 있다. 이러한 경우 (P, P^{**})의 차분을 D_1으로 표시한다. 즉, $P \oplus P^* = D_1$(표 3). 위 두 가지 경우를 정리하면, 조건 (21)과 조건 (22)를 만족하는 차분 D_0과 D_1 은 각각 1 라운드 암호화 과정 후 표 2의 형태 0과 4를 만족하며, 2 라운드 암호화 과정 후에는 표 1의 입력 차분 값을 만족한다.

표 3. 라운드 0의 두 가지 형태의 입력 차분

차분	ΔA^0	ΔB^0	ΔC^0	ΔD^0	ΔE^0	ΔF^0	ΔG^0	ΔH^0	상태
D_0	0	e_{31}	0	0	0	e_{31}	0	0	(21)
D_1	0	e_{31}	e_{31}	0	0	e_{31}	0	0	(22)

그러므로 한 비트 키 w_{31}^0의 값에 따라 확률 1로 만족하는 두 가지 형태의 11 라운드 불능 차분 특성을 구성할 수 있다. 두 가지 11 라운드 불능 차분 특성은 다음과 같이 요약할 수 있다.

성질1-1. $w_{31}^0 = 0$인 경우, 차분 D_0을 만족하는 임의의 평문쌍에 대해서(즉, $P \oplus P^* = D_0$), 11 라운드 암호화 과정 후에 여덟 번째 워드의 최하위 비트는 1이 될 수 없다(즉, $h_0^{11} \oplus h_0^{*11} \neq 1$).

성질1-2. $w_{31}^0 = 1$인 경우, 차분 D_1을 만족하는 임의의 평문쌍에 대해서(즉, $P \oplus P^{**} = D_1$), 11 라운드 암호화 과정 후에 여덟 번째 워드의 최하위 비트는 1이 될 수 없다(즉, $h_0^{11} \oplus h_0^{**11} \neq 1$).

3.2. 14 라운드 불능 차분 특성

본 절에서는 11 라운드 불능 차분 특성에 3 라운드 비선형 방정식을 결합하는 방법을 소개한다. 본 논문에서 사용하는 불능 차분 특성 (20)은 단지 ΔH^{11}의 최하위 비트 Δh_0^{11}에 관심이 있다. h_0^{11}의 값은 복호화 과정을 통해 $A^{14}, B^{14}, \cdots, H^{14}, K^{11}, K^{12}, K^{13}, W^{11}, W^{12}, W^{13}$의 특정 비트로 표현 가능하다. 즉, h_0^{11}의 3 라운드 비선형 방정식을 유도할 수 있으며, 이를 이용하여 14 라운드 불능 차분 특성으로 확장한다. 이 과정 중에 최하위 비트의 덧셈은 XOR 연산과 같음을 이용한다. 유도과정은 다음과 같다.

먼저 방정식 (12)를 사용하여 h_0^{11}은 (23)과 같이 $A^{12}, B^{12}, \cdots, H^{12}, K^{11}, W^{11}$의 특정 비트의 비선형 방정식으로 표현할 수 있다.

$$h_0^{11} = a_0^{12} \oplus (\neg(b_2^{12} \oplus b_{13}^{12} \oplus b_{22}^{12})) \oplus (\neg((b_0^{12} \& c_0^{12}) \oplus (b_0^{12} \& d_0^{12}) \oplus (c_0^{12} \& d_0^{12}))) \oplus (\neg(f_6^{12} \oplus f_{11}^{12} \oplus f_{25}^{12})) \oplus (\neg((f_0^{12} \& g_0^{12}) \oplus ((\neg f_0^{12}) \& h_0^{12}))) \oplus (\neg k_0^{11}) \oplus (\neg w_0^{11}) \quad (23)$$

복호화 과정을 사용하여, h_0^{11}은 (24)와 같이 $A^{13}, B^{13}, \cdots, H^{13}, K^{11}, K^{12}, W^{11}, W^{12}$의 특정 비트의 비선형 방정식으로 표현할 수 있다.

$$h_0^{11} = b_0^{13} \oplus (\neg(c_2^{13} \oplus c_{13}^{13} \oplus c_{22}^{13})) \oplus (\neg((c_0^{13} \& d_0^{13}) \oplus (c_0^{13} \& (e_0^{13} \oplus t_{1,0}^{13})) \oplus (d_0^{13} \& ((e_0^{13} \oplus t_{1,0}^{13})))) \oplus (\neg(g_6^{13} \oplus g_{11}^{13} \oplus g_{25}^{13})) \oplus (\neg((g_0^{13} \& h_0^{13}) \oplus ((\neg g_0^{13}) \& h_0^{12}))) \oplus (\neg k_0^{11}) \oplus (\neg w_0^{11}) \quad (24)$$

비선형 방정식 (24)의 $t_{1,0}^{13}$과 h_0^{12}는 방정식 (11)과 (23)을 사용하여 비선형 방정식 (25)와 (26)으로 표현할 수 있다.

$$t_{1,0}^{13} = a_0^{13} \oplus (\neg(b_2^{13} \oplus b_{13}^{13} \oplus b_{22}^{13})) \oplus (\neg((b_0^{13} \& c_0^{13}) \oplus (b_0^{13} \& d_0^{13}) \oplus (c_0^{13} \& d_0^{13}))) \quad (25)$$

$$h_0^{12} = a_0^{13} \oplus (\neg(b_2^{13} \oplus b_{13}^{13} \oplus b_{22}^{13})) \oplus (\neg((b_0^{13} \& c_0^{13}) \oplus (b_0^{13} \& d_0^{13}) \oplus (c_0^{13} \& d_0^{13}))) \oplus (\neg(f_6^{13} \oplus f_{11}^{13} \oplus f_{25}^{13})) \oplus (\neg((f_0^{13} \& g_0^{13}) \oplus ((\neg f_0^{13}) \& h_0^{13}))) \oplus (\neg k_0^{12}) \oplus (\neg w_0^{12}) \quad (26)$$

유사한 방법으로, h_0^{11}은 (27)과 같이 $A^{14}, B^{14}, \cdots, H^{14}, K^{11}, K^{12}, K^{13}, W^{11}, W^{12}, W^{13}$의 특정 비트의 비선형 방정식으로 표현할 수 있다.

$$h_0^{11} = c_0^{14} \oplus (\neg(d_2^{14} \oplus d_{13}^{14} \oplus d_{22}^{14})) \oplus (\neg((d_0^{14} \& (e_0^{14} \oplus t_{1,0}^{14})) \oplus (d_0^{14} \& (f_0^{14} \oplus t_{1,0}^{13})) \oplus ((e_0^{14} \oplus t_{1,0}^{14}) \& (f_0^{14} \oplus t_{1,0}^{13})))) \oplus (\neg(h_6^{14} \oplus h_{11}^{14} \oplus h_{25}^{14})) \oplus (\neg((h_0^{14} \& h_0^{13}) \oplus ((\neg h_0^{14}) \& h_0^{12}))) \oplus (\neg k_0^{11}) \oplus (\neg w_0^{11}) \quad (27)$$

비선형 방정식 (27)의 $h_0^{12}, t_{1,0}^{13}, h_0^{13}, t_{1,0}^{14}$은 비선형 방정식 (24), (25), (26)을 이용하여 (28), (29), (30), (31)과 같이 표현할 수 있다.

$$h_0^{12} = b_0^{14} \oplus (\neg(c_2^{14} \oplus c_{13}^{14} \oplus c_{22}^{14})) \oplus (\neg((c_0^{14} \& d_0^{14}) \oplus (c_0^{14} \& (e_0^{14} \oplus t_{1,0}^{14})) \oplus (d_0^{14} \& ((e_0^{14} \oplus t_{1,0}^{14})))) \oplus (\neg(g_6^{14} \oplus g_{11}^{14} \oplus g_{25}^{14})) \oplus (\neg((g_0^{14} \& h_0^{14}) \oplus ((\neg g_0^{14} \& h_0^{13}))) \oplus (\neg k_0^{12}) \oplus (\neg w_0^{12}) \quad (28)$$

$$t_{1,0}^{13} = b_0^{13} \oplus (\neg(c_2^{14} \oplus c_{13}^{14} \oplus c_{22}^{14})) \oplus (\neg((c_0^{13} \& d_0^{14}) \oplus (c_0^{14} \& (e_0^{14} \oplus t_{1,0}^{14})) \oplus (d_0^{14} \& (e_0^{14} \oplus t_{1,0}^{14})))) \quad (29)$$

$$h_0^{13} \& = a_0^{14} \oplus (\neg(b_2^{14} \oplus b_{13}^{14} \oplus b_{22}^{14})) \oplus (\neg((b_0^{14} \& c_0^{14}) \oplus (b_0^{14} \& d_0^{14}) \oplus (c_0^{14} \& d_0^{14}))) \oplus (\neg(f_6^{14} \oplus f_{11}^{14} \oplus f_{25}^{14})) \oplus (\neg((f_0^{14} \& g_0^{14}) \oplus ((\neg f_0^{14}) \& h_0^{14}))) \oplus (\neg k_0^{13}) \oplus (\neg w_0^{13}) \quad (30)$$

$$t_{1,0}^{14} = a_0^{14} \oplus (\neg(b_2^{14} \oplus b_{13}^{14} \oplus b_{22}^{14})) \oplus (\neg((b_0^{14} \& c_0^{14}) \oplus (b_0^{14} \& d_0^{14}) \oplus (c_0^{14} \& d_0^{14}))) \quad (31)$$

따라서, h_0^{11}는 비선형 함수 $NF(A^{14}, B^{14}, \cdots, H^{14}, K^{11}, K^{12}, K^{13}, W^{11}, W^{12}, W^{13})$로 표현 가능하다(이 함수를 간단하게 NF^{14}로 표시한다). 그러므로 14 라운드 SHACAL-2에 대한 불능 차분 특성을 다음과 같이 나타낼 수 있다.

성질 2. $P \oplus P^* = D_0$와 $P \oplus P^{**} = D_1$을 만족하는 세 개의 평문 (P, P^*, P^{**})을 고려하자.

2-1. 만약 $w_{31}^0 = 0$ 라면, 확률 1을 가지고 $NF^{14} \oplus NF^{*14} \neq 1$이 성립한다.

2-2. 만약 $w_{31}^0 = 1$ 라면, 확률 1을 가지고 $NF^{14} \oplus NF^{**14} \neq 1$이 성립한다.

그러므로 w_{31}^0값에 따라 라운드 0-13에 대한 두 가지 형태의 14 라운드 불능 차분 특성을 구성할 수 있다.

Ⅳ. 512 비트 키를 사용하는 30 라운드 SAHCAL-2의 불능 차분 공격

본 장에서는 앞서 소개한 두 가지 형태의 14 라운드 불능 차분 특성을 이용하여 30 라운드 SHACAL-2의 512 비트 키를 찾는 방법을 설명한다.

(P_i, P_i^*, P_i^{**})은 $i = 1, \cdots, 248$에 대해서 $P_i \oplus P_i^* = D_0$와 $P_i \oplus P_i^{**} = D_1$을 만족하는 세 개의 평문이고, (C_i, C_i^*, C_i^{**})는 (P_i, P_i^*, P_i^{**})에 대응하는 30 라운드 SHACAL-2의 세 개의 암호문 이라고 가정하자. $(NF^{14} \oplus NF^{*14})_i$는 P_i^{11}와 P_i^{*11}의 여덟 번째 워드의 최하위 비트 차분을, $(NF^{14} \oplus NF^{**14})_i$는 P_i^{11}와 P_i^{**11}의 여덟 번째 워드의 최하위 비트 차분을 나타낸다. 위의 가정으로부터 각 세 개의 평문 (P_i, P_i^*, P_i^{**})는 성질 2를 만족한다.

차분값 ΔNF^{14}을 알기 위해서 비선형 방정식 (27)의 키 값 w_{31}^0은 요구되지 않는다. 또한 NF^{14} 값이 아닌 ΔNF^{14}값을 알기 위해서, 라운드 17의 출력쌍을 안다는 가정 아래 $w_0^{14}, w_1^{14}, \cdots, w_{24}^{14}, w_0^{15}, w_1^{15}, \cdots, w_{25}^{15}, w_0^{16}, w_1^{16}, \cdots, w_{25}^{16}$의 키 값만을 요구한다. 따라서 만약 라운드 30 라운드의 암호문쌍을 안다면, 495 비트 키 $W^{29}, W^{28}, \cdots, W^{17}, w_0^{16}, w_1^{16}, \cdots, w_{25}^{16}, w_0^{15}, w_1^{15}, \cdots, w_{25}^{15}, w_0^{14}, w_1^{14}, \cdots, w_{24}^{14}, w_0^{13}, w_0^{12}$을 추측함으로써

복호화 과정을 통해 $(NF^{14} \oplus NF^{*14})_i$와 $(NF^{14} \oplus NF^{**14})_i$을 얻을 수 있다. 하지만 키 스케줄 관찰 결과 $W^{29}, W^{27}, W^{22}, w_3^{14}, w_7^{14}, w_{18}^{14}$을 추측하여 w_0^{13}을 얻을 수 있다. 따라서 총 494 비트 키를 추측하여 성질 2의 여부를 판단할 수 있다.

$k_1, k_2, \cdots, k_{2^{494}}$는 모든 가능한 494 비트 키 값이라고 가정하자. 각각의 k_j에 대한 모든 $i\,(=1,\ldots,248)$ 값에 대해서 $(NF^{14} \oplus NF^{*14})_i = 0$ 또는 $(NF^{14} \oplus NF^{**14})_i = 0$여부를 테스트한다.

만약 k_j가 모든 i에 대해서 $(NF^{14} \oplus NF^{*14})_i = 0$을 만족한다면, k_j와 $w_{31}^0 = 0$을 키 후보로 저장한다. 반면, 모든 i에 대해서 $(NF^{14} \oplus NF^{**14})_i = 0$을 만족한다면, k_j와 $w_{31}^0 = 1$을 키 후보로 저장한다. 모든 과정을 거친 후 키 후보로 저장된 키와 남은 17 비트 키에 대해서 전수조사를 수행한다. 알고리즘 1은 위의 공격과정을 요약한다.

알고리즘 1의 시간 복잡도는 단계 1에 의해 결정된다. 단계 2의 사용되는 키는 단계 1에서 사용되는 2^{494}의 키에 비해 낮은 비율을 차지하므로, 단계 2의 시간 복잡도는 단계 1에 비해 매우 작다. 그러므로 30 라운드 SHACAL-2에 대한 공격은 $744 (= 3 \cdot 248)$개의 선택 평문과 약 $\frac{16}{30} \cdot \sum_{i=0}^{247} (2^{494-2 \cdot i} \cdot 3) \simeq 2^{495.1}$30 라운드 SHACAL-2 암호화 과정을 요구한다.

알고리즘 1. 30 라운드 SHACAL-2 공격

입력값 : $i = 1, \cdots, 248$에 대한, 248 개의 세 개의 암호문 (C_i, C_i^*, C_i^{**})

출력값 : 마스터 키

1. $j = 1, \cdots, 2^{494}$에 대해서
  1.1 $i = 1, \cdots, 248$에 대해서
    1.1.1 k_j를 사용하여 C_i와 C_i^*을 복호화 하고 $a_i = (NF^{14} \oplus NF^{*14})_i$를 계산한다.
    1.1.2 만약 $(a_i = 1)$라면, 1.2단계로 간다.
      그렇지 않고 만약 $(a_i = 0$와$i = 248)$라면, k_j와$w_{31}^0 = 0$를 저장한다.
  1.2 $i = 1, \cdots, 248$에 대해서
    1.2.1 k_j를 사용하여 C_i와 C_i^{**}을 복호화 하고 $b_i = (NF^{14} \oplus NF^{**14})_i$를 계산한다.
    1.2.2 만약 $(b_i = 1)$라면, 1단계로 간다.
      그렇지 않고 만약 $(b_i = 0$와$i = 248)$라면, k_j와$w_{31}^0 = 1$를 저장한다.
2. 단계 1을 통과한 키에 대해서 나머지 17비트와 함께 전수조사를 수행한다.

주의 : 만약 추측한 키가 올바르지 않다면 ΔNF^{14} 값은 랜덤하다고 가정한다. 따라서 단계 1을 통과하는 495 비트 부분키의 기대값은 $0.5 (= 2^{495-2 \cdot 248})$이다. 하지만 구현 결과, 단계 1을 통과하는 키 후보의 개수는 기대값 이상이었다. W^{14}의 25 비트를 제외하고 올바르게 추측한 2^{25}개의 495 비트 키에 약 52.6개의 키가 단계 1을 통과 하였고, W^{15}의 26 비트를 제외하고 올바르게 추측한 2^{26}개 495 비트 키의 경우 약 9.3개의 키가, W^{16}의 26 비트를 제외하고 올바르게 추측한 2^{26}개 495 비트 키의 경우에 약 4.8개의 키가 단계 1을 통과하였다(단계 1을 통과한 키의 개수는 10번 테스트 결과의 평균값이다). 보조 정리 1은 단계 1을 통과하는 키의 개수가 기대값 이상의 수치가 나온 이유를 설명한다.

보조정리 1.

$Z = X + Y, Z^* = X^* + Y^*, X \oplus X^* = e_j, Y = Y^*$라고 가정하자(단, X, Y, X^*, Y^*는 32 비트 워드이다). 그러면 확률 $1/2^k (j + k - 1 \le 31)$으로 $Z \oplus Z^* = e_{j, j+1, \cdots, j+k-1}$이 성립한다.

예를 들어, w_{12}^{14}값을 제외하고 495 비트를 올바르게 추측하였다고 가정하자. 틀리게 추측된 한 비트 키는 보조정리 1로부터 확률 2^{-13}으로 $\Delta NF^{14} = 1$을 만족한다. 따라서 올바르지 못한 키에 대해서도 단계 1을 통과하는 경우가 발생한다. 하지만, $W^{17}, \cdots, W^{29}$의 특정 비트의 올바르지 못한 키 추측은 ΔNF^{14}의 값을 랜덤하게 생성한다. 그러므로 거의 대부분의 495 비트 틀린 키는 ΔNF^{14}값을 랜덤하게 출력하기 때문에 대략 $2^{495.1}$ 30 라운드 SHACAL-2 암호화 과정의 시간 복잡도를 가지고 30 라운드 SHACAL-2를 공격할 수 있다.

V. 결 론

본 논문은 SHACAL-2의 불능 차분 공격을 소개하였다. 첫 번째로 라운드 키의 한 비트에 영향을 받는 확률 1로 성립하는 두 가지 형태의 11 라운드 SHACAL-2 부정 차분을 이용하여 두 가지 형태의 11 라운드 불능 차분 특성을 구성하였다. 두 번째로 복호화 과정을 통해 확률 1을 가지는 3 라운드 비선

형 방정식을 유도하고, 이를 이용하여 첫 번째 라운드 키의 한 비트에 영향을 받는 두 가지 형태의 14 라운드 불능 차분 특성으로 확장하였다. 이 불능 차분 특성을 사용하여 744 선택 평문의 데이터 복잡도와 $2^{495.1}$ 시간 복잡도를 가지고 전수조사 보다 빠른 512 비트 키를 가지는 30 라운드 SHACAL-2를 공격할 수 있다.

참 고 문 헌

[1] E. Biham, A. Biryukov and A. Shamir, *Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials*, Advances in Cryptology-EUROCRYPT'99, LNCS 1592, pp. 12-23, Springer-Verlag, 1999.

[2] H. Handschuh and D. Naccache, *SHACAL : A Family of Block Ciphers*, Submission to the NESSIE project, 2002.

[3] D.J. Moon, K.D. Hwang, W.I. Lee, S.J. Lee and J.I. Lim, *Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA*, FSE 2002, LNCS 2365, pp.49-60, Springer-Verlag, 2002.

[4] U.S. Department of Commerce.*FIPS 180-2*: Secure Hash Standard , Federal Information Processing Standards Publication, N.I.S.T., August 2002.

〈著者紹介〉

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

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~현재 : 고려대학교 정보보호대학원 석사 과정
〈관심분야〉 블록 암호 및 스트림 암호의 분석과 설계

이 창 훈 (Chang-hoon Lee)
2001년 2월 : 한양대학교 수학과 학사
2003년 2월 : 고려대학교 정보보호대학원 석사
2003년 3월~현재 : 고려대학교 정보보호대학원 박사과정
〈관심분야〉 블록 암호 및 스트림 암호 분석 및 설계, 블록 암호 운영모드 분석 및 설계

성 재 철 (Jae-chul Sung) 정회원
1997년 8월 : 고려대학교 수학과 학사
1999년 8월 : 고려대학교 수학과 석사
2002년 8월 : 고려대학교 수학과 박사
2002년 8월~2004년 1월 : 한국정보보호진흥원 선임연구원
2004년 2월~현재 : 서울시립대학교 수학과 전임 강사
〈관심분야〉 블록 암호 및 스트림 암호의 분석 및 설계, 해쉬 함수의 분석.

이 상 진 (Sang-jin 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