Journal of Korea Multimedia Society Vol. 12, No. 5, May 2009(pp. 644-652)

유비쿼터스 환경에 적합한 경량 블록암호 mCrypton에 대한 안전성 분석

이창훈[†], 이유섭[††], 성재철[†††]

요 약

유비쿼터스 센서 네트워크(USN), 휴대 인터넷(WiBro), 무선식별 시스템(RFID) 등의 새로운 통신 환경이 현실화 되고 있다. 이에, 이러한 제약된 자원을 사용하는 통신 환경에서 보안과 프라이버시 보호를 보장하기 위해 mCrypton, HIGHT, SEA, PRESENT와 같은 경량 블록 암호들이 제안되었다. mCrypton은 Crypton의 경량화 버전으로 64-비트, 96-비트, 128-비트 키를 지원하는 64-비트 블록 암호이다. 본 논문에서는 mCrypton에 대한 첫 번째 분석 결과로서, 128-비트 키를 사용하는 8-라운드 mCrypton에 대한 연관키 렉탱글 공격을 제안한다. 이를 위해 7-라운드 연관키 렉탱글 구별자를 구성하기 위해 사용하는 두 개의 연관키 부정 차분 특성을 설명하고 이를 기반으로 8-라운드 mCypton에 대한 연관키 렉탱글 공격을 제안한다. 본 공격은 $2^{45.5}$의 데이터와 $2^{45.5}$의 시간 복잡도를 필요로 한다.

Security Analysis of Light-weight Block Cipher mCrypton Suitable for Ubiquitous Computing Environment

Changhoon Lee[†], Yuseop Lee[††], Jaechul Sung[†††]

ABSTRACT

New communication environments such as USN, WiBro and RFID have been realized nowadays. Thus, in order to ensure security and privacy protection, various light-weight block ciphers, e.g., mCrypton, HIGHT, SEA and PRESENT, have been proposed. The block cipher mCrypton, which is a light-weight version of Crypton, is a 64-bit block cipher with three key size options (64 bits, 96 bits, 128 bits). In this paper we show that 8-round mCrypton with 128-bit key is vulnerable to related-key rectangle attack. It is the first known cryptanalytic result on mCrypton. We first describe how to construct two related-key truncated differentials on which 7-round related-key rectangle distinguisher is based and then exploit it to attack 8-round mCrypton. This attack requires $2^{45.5}$ dada and $2^{45.5}$ time complexities which is faster than exhaustive key search.

Key words: Contents Protection(컨텐츠 보호), Block Cipher(블록 암호), Cryptanalysis(암호분석)

1. 서 론

최근 유비쿼터스 센서 네트워크(USN), 휴대 인터넷(WiBro), 무선식별 시스템(RFID) 등의 새로운 통신 환경이 현실화 되고 있다. 이러한 통신 환경은 사용자의 상황을 인식하며 장소에 구애받지 않고 상호

※ 교신저자(Corresponding Author) : 성재철, 주소 : 서울시 동대문구 전농동 90(130-743), 전화 : 02)2210-5663, FAX : 02)2210-2886, E-mail : jcsung@uos.ac.kr
접수일 : 2009년 3월 2일, 완료일 : 2009년 3월 23일
[†] 정회원, 한신대학교 컴퓨터공학부 전임강사
(E-mail : chlee@hs.ac.kr)
[††] 준회원, 고려대학교 정보경영공학전문대학원 석박사통합과정
(E-mail : yusubi@korea.ac.kr)
[†††] 정회원, 서울시립대학교대학교 수학과 조교수
※ 이 연구는 2008년도 서울시립대학교 교내학술연구비에 의하여 연구되었음

간에 통신이 가능한 장점을 가지고 있다. 하지만, 이러한 통신 환경은 저비용·저전력의 제약된 환경에서 구현되기 때문에, 일반적인 암호 알고리즘을 사용하여 보안과 프라이버시보호를 보장하기 어렵다. 이에 따라, 이러한 환경에서 안전성을 보장할 수 있는 단순하면서도 효율적인 암호 알고리즘들을 필요로 한다. 이에 국내에서 개발한 mCrypton, HIGHT와 유럽에서 개발된 SEA, PRESENT 등이 제안되었다 [1-4].

현재, ISO/IEC JTC 1/SC 27에서 위에서 제시된 저전력, 경량 암호 알고리즘에 대한 표준화가 진행되고 있다. 하지만, 이미 수많은 안전성 검증을 통해 신뢰성을 갖춘 미국 및 ISO 표준인 차세대 블록 암호 AES와 ISO/IEC 표준으로 채택된 Camellia, SEED와 달리, 경량 블록암호들에 대한 명확한 안전성 분석이 수행되지 않아 표준화 작업에 어려움을 겪고 있다.

블록 암호 Crypton의 경량화 버전인 mCrypton은 USN/RFID 환경 같이 제한된 자원을 사용하는 환경에서 매우 효율적으로 설계되었다 [5,1]. 그리하여 작은 처리 능력을 가지는 프로세서를 가지는 저비용의 장치에서도 하드웨어나 소프트웨어로 효율적인 구현이 가능하다. mCrypton은 64-비트, 96-비트, 128-비트의 세 가지 키 길이를 지원하는 64-비트 블록 암호로 전체 12 라운드로 구성된다. 또한 현재까지 알려진 차분 공격과 선형 공격 등에 대하여 충분한 안전성을 가지는 것으로 평가 받고 있다 [6-8].

본 논문에서 128-비트 키를 사용하는 8 라운드 mCrypton에 대한 연관키 렉탱글 공격을 제안한다. 이를 위해 연관키 렉탱글 공격에 사용하는 두 개의 7 라운드 연관키 부정 차분 특성을 소개한다. 그리고 이 부정 차분 특성을 이용하여 렉탱글 구별자를 구성하고, $2^{45.5}$의 데이터와 $2^{45.5}$의 시간 복잡도를 가지는 8 라운드 연관키 렉탱글 공격을 제안한다. 본 공격은 mCrypton에 대한 첫 번째 분석결과로서, 8 라운드 mCrypton의 취약성으로 인해 이를 사용하는 시스템 환경이 취약해질 수 있음을 의미한다.

본 논문에서 사용하는 연관키 렉탱글 공격은 블록 암호에 대한 강력한 암호학적 분석 방법으로 ACISP 2004에서 SHACAL-1에 처음으로 적용되었다 [9]. 그 이후, AES와 KASUMI등과 같이 다른 여러 블록 암호들에 대하여 적용되었다 [10-24]. 최근, 연관키 렉탱글 공격을 변형한 공격인 연관키 부메랑 공격과 연관키 확장된 부메랑 공격이 AES와 MISTY 등에 적용되었다 [10,15,26].

본 논문은 다음과 같이 구성되어 있다. 2절에서는 mCrypton 알고리즘을 소개하고 3절에서는 연관키 렉탱글 공격 기법을 간단히 소개한다. 그리고 4절에서 본격적으로 블록 암호 mCrypton에 대한 분석을 수행한 후 5절에서 결론을 맺는다.

2. 블록 암호 mCrypton

본 절에서는 본 논문에서 사용하는 표기법과 블록 암호 mCrypton을 소개한다.

2.1 표기법

본 논문에서는 다음과 같은 표기법을 사용한다.

- 64-비트 데이터는 16개의 4-비트 니블 $\{a_0, a_1, \cdots, a_{15}\}$로 구성되고 다음과 같이 4×4 니블 행렬로 표현된다. 여기서, $A_r[i]$와 $A_c[i]$는 각각 행렬 A의 i번째 행과 열을 의미한다.

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} = \begin{pmatrix} A_r[0] \\ A_r[1] \\ A_r[2] \\ A_r[3] \end{pmatrix} = (A_c[0]\, A_c[1]\, A_c[2]\, A_c[3])$$

- A^t: 행렬 A의 전치 행렬
- $f \circ g$: 함수 f와 g의 합성함수
- $x^{\lll k}$: 16비트 x의 k 비트 좌측 순환이동 변환
- $\cdot, \oplus$: AND, XOR에 대한 비트 단위 논리 연산

2.2 블록암호 mCrypton의 전체구조

mCrypton은 64-비트, 96-비트, 128-비트 키를 지원하는 입출력 64-비트 블록 암호로서 12번의 반복적인 라운드로 구성된다. 라운드 함수는 다음과 같은 4 단계로 구성된다.

- **비선형 대치** γ. γ는 다음의 표 1과 같이 4개의 4×4 S-박스 S_i로 구성된다($i \le i \le 3$).

입력된 데이터 행렬 A의 i 번째 행(열)인 4 개의 니블 $a = (a_0, a_1, a_2, a_3)$에 대해, $\gamma_i(a)$는 다음과 같은 연산을 수행한다.

$$\gamma_i(a) = (S_i(a_0), S_{i+1}(a_1), S_{i+2}(a_2), S_{i+3}(a_3)).$$

표 1. 열 단위 비트 치환 π

S_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_0	4	15	3	8	13	10	12	0	11	5	7	14	2	6	1	9
S_1	1	12	7	10	6	13	5	3	15	11	2	0	8	4	9	14
S_2	7	14	12	2	0	9	13	10	3	15	5	8	6	4	11	1
S_3	11	0	10	7	13	6	4	2	12	14	3	9	1	5	15	8

γ는 입력된 데이터 행렬 A에 대해 다음과 같이 정의 된다. 여기서, $S_2 = S_0^{-1}, S_3 = S_1^{-1}$이고 $\gamma_i(a) = \gamma_0(a^{\lll (16-4i)})^{\lll 4i}$이다.

$$\gamma(A) = (r_0(A_c[0]), r_1(A_c[1]), r_2(A_c[2]), r_3(A_c[3])) = (r_0(A_r[0]), r_1(A_r[1]), r_2(A_r[2]), r_3(A_r[3])).$$

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} \xrightarrow{\gamma} \begin{pmatrix} S_0(a_0) & S_1(a_1) & S_2(a_2) & S_3(a_3) \\ S_1(a_4) & S_2(a_5) & S_3(a_6) & S_0(a_7) \\ S_2(a_8) & S_3(a_9) & S_0(a_{10}) & S_1(a_{11}) \\ S_3(a_{12}) & S_0(a_{13}) & S_1(a_{14}) & S_2(a_{15}) \end{pmatrix}$$

• **비트 치환** (π). 데이터 행렬 A의 각 열에 대해 π_i를 이용하여 다음과 같이 치환한다. 여기서, $a = (a_0, a_1, a_2, a_3)^t$, $b = (b_0, b_1, b_2, b_3)^t$이고 $m_0 = 1110_2$, $m_1 = 1101_2$, $m_2 = 1011_2$, $m_3 = 0111_2$일 때, 각각의 π_i는 다음과 같이 정의 된다. 또한, $\pi = \pi^{-1}$를 만족한다.

$$\pi(A) = (\pi_0(A_c[0])\, \pi_1(A_c[1])\, \pi_2(A_c[2])\, \pi_3(A_c[3])).$$

$$b = \pi_i(a) \Leftrightarrow b_j = \bigoplus_{k=0}^{3} (m_{i+j+k \bmod 4} \cdot a_k).$$

• **행-열 변환** τ. 데이터 행렬 A의 (i,j)에 있는 니블을 (j,i) 위치로 변환한다. 즉, $B = \tau(A) \Leftrightarrow b_{ji} = a_{ji}$. 또한 $\tau^{-1} = \tau$.

• **키 덧셈** σ. $B = \sigma_K(A)$일 때, $B_r[i] = A_r[i] \oplus K[i]$ $(0 \le i \le 3)$으로 정의된다. 여기서, $K = (K[0], K[1], K[2], K[3])$이다.

mCrypton의 각 라운드 함수 ρ는 $\gamma, \pi, \tau, \sigma$를 차례로 적용하고, 이 때 사용되는 라운드 키 K_i에 의해 다음과 같이 정의된다.

$$\rho_{K_i} = \sigma_{K_i} \circ \tau \circ \pi \circ \gamma.$$

마스터 키가 K인 mCrypton의 암호화 함수 E_K는 초기키 덧셈 σ_{K_0}와 12번의 라운드 함수 ρ를 반복적으로 적용하고, 최종 변환 ϕ으로 다음과 같이 구성된다.

$$E_K = \phi \circ \rho_{K_{12}} \circ \rho_{K_{11}} \circ \cdots \circ \rho_{K_2} \circ \rho_{K_1} \circ \sigma_{K_0}.$$

최종 변환 $\phi = \tau \circ \pi \circ \tau$이다. 또한, 최종 변환 ϕ는 마지막 12 라운드에 포함하여 다음과 같이 표현할 수 있다. 여기서, $K_{eq} = \phi(K_{12})$이다.

$$\phi \circ \rho_{K_{12}} = \tau \circ \pi \circ \tau \circ (\sigma_{K_{12}} \circ \tau \circ \pi \circ \gamma). = (\sigma_{K_{eq}} \circ \tau \circ \pi \circ \gamma).$$

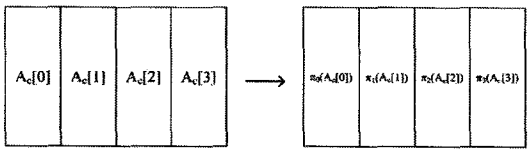


그림 1. 열 단위 비트 치환 π

2.3 mCrypton의 키 스케줄

mCrypton은 64, 96, 128 비트의 세 가지 키 길이를 지원한다. 하지만 본 논문에서는 12 라운드를 사용하는 128-비트 키를 사용하는 mCrypton의 키 스케줄만 다룬다. 키 스케줄은 크게 두 단계로 구성된다. 우선, 비선형 S-박스 변환을 적용하고, 워드 기반 순환이동과 워드 안에서 비트 단위의 순환이동 변환을 적용한다.

마스터 키 $K = \{K[i]\}_{i=0}^{7} = (K[0], K[1], \cdots, K[7])$이고, $C[i]$는 라운드 상수로 정의한다. $K[i]$와 $C[i]$는 16-비트 워드이고, 라운드 상수 $C[i]$는 동일한 네 개의 니블로 구성된다 ($C[i] = c_i c_i c_i c_i$). 여기서, c_i는 기약다항식 $f(x) = x^4 + x + 1$로 생성된 $GF(2^4)$의 x를 통하여 계산된다. 즉, $c_0 = 1, c_1 = 2, \cdots, c_4 = 3, c_5 = 6, \cdots$이다. 키 스케줄에서 상태 업데이트를 위한 키 레지스터 $U = \{U[i]\}_{i=0}^{7}$를 사용한다.

우선, 키 레지스터 U를 K로 초기화 하고, 각 라운드 키 K_r $(r = 0, 1, 2, \cdots, 12)$을 다음과 같이 계산한다.

$T \leftarrow S(U[0]) \oplus C[r]$,
$T_i \leftarrow T \cdot M_i (0 \le i \le 3)$,
$K_r \leftarrow (U[1] \oplus T_0, U[2] \oplus T_1, U[3] \oplus T_2, U[4] \oplus T_3)$,
$U \leftarrow (U[5], U[6], U[7], U[0]^{\ll 3}, U[1], U[2], U[3], U[4]^{\ll 8})$.

여기서, S-박스 연산은 키 레지스터의 $U[0]$의 4개의 니블에 대하여 동일한 S_0를 적용하는 연산이고, $M_0 = 0xf000$, $M_1 = 0x0f00$, $M_2 = 0x00f0$, $M_3 = 0x000f$이다.

3. 연관키 렉탱클 공격 기법 소개

연관키 렉탱글 공격은 ACISP 2004에서 SHACAL-1을 기반으로 하는 SHA-1을 분석하기 위해 처음으로 제안되었다[9]. 그 이후, 이 분석 방법은 AES와 KASUM 등 여러 블록 암호를 분석하는 도구로 널리 사용되었다[10-13]. 본 절에서는 연관키 부정 차분 특성을 이용하여 연관키 구별자를 구성하는 방법과 연관키 렉탱글 공격에 대해 설명한다.

블록암호 $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$으로 정의할 때, 이를 두 개의 부분 $E = E^1 \circ E^0$으로 나눈다. 다시 말해서, $E_K = E^1_K(E^0_K(P))$, P는 n-비트 평문이고, K는 k-비트 비밀 키이고, E^0, E^1, E는 k 비트 비밀 키에 대한 n 비트 치환 함수이다. 연관키 렉탱글 공격은 구별자를 구성하기 위해 여러 연관키 차분 특성을 사용한다.

- E^0에 대한 확률 p_β를 가지는 $\alpha \rightarrow \beta$인 연관키 차분 특성 : $\Pr_{X,K}[E^0_K(X) \oplus E^0_{K \oplus K^*}(X+\alpha) = \beta] = p_\beta$.
- E^1에 대한 확률 p_γ를 가지는 $\gamma \rightarrow \delta$인 연관키 차분 특성 : $\Pr_{X,K}[E^1_K(X) \oplus E^1_{K \oplus K'}(X+\gamma) = \delta] = q_\gamma$.

여기서, K^*와 K'은 공격자가 선택한 0이 아닌 키 차분이다. $\hat{p} = \sqrt{\sum_\beta p_\beta^2}$, $\hat{q} = \sqrt{\sum_\gamma q_\gamma^2}$로 정의할 때, $\hat{p} \cdot \hat{q} > 2^{-n/2}$이면, 공격자는 연관키 렉탱글 구별자를 다음과 같이 구성한다.

- **단계 1.** 차분 α인 m개의 평문 쌍 (P, P^*)와 차분 α인 m개의 평문 쌍 (P', P'^*)를 선택한다. 그리고 P, P^*, P', P'^*를 각각 K, K^*, K', K'^*를 이용하여 암호화하여 C, C^*, C', C'^*을 얻는다. 여기서, $K^* = K \oplus \Delta K^*$, $K' = K \oplus \Delta K'$, $K'^* = K \oplus \Delta K^* \oplus \Delta K'$ 이다.
- **단계 2.** 다음을 만족하는 암호문 쿼텟을 계산한다.

$$C \oplus C' = C^* \oplus C'^* = \delta. \quad (1)$$

단계 1에서 평균적으로 $m \cdot p_\beta$개의 평문 쌍 (P, P^*)와 $m \cdot p_\beta$개의 평문 쌍 (P', P'^*)이 E^0에 대한 $\alpha \rightarrow \beta$인 연관키 차분 특성을 만족할 것이다. 그러므로 E^0에 대한 연관키 차분특성을 만족하는 $m^2 \cdot p_\beta^2$개의 쿼텟을 구성할 수 있다. 더욱이, 모든 가능한 값이 균일한 분포를 따른다면 $E^0_K(P) \oplus E^0_{K'}(P') = \gamma$를 만족할 확률은 2^{-n}이다. $E^0_K(P) \oplus E^0_{K^*}(P^*) = E^0_{K'}(P') \oplus E^0_{K'^*}(P'^*) = \beta$ (확률 p_β^2), $E^0_K(P) \oplus E^0_{K'}(P') = \gamma$(확률 2^{-n})일 때, $E^0_{K^*}(P^*)\, E^0_{K'^*}(P'^*) = \gamma$일 확률은 1이다. 또한, $(E^0_K(P), E^0_{K'}(P'))$와 $(E^0_{K^*}(P^*), E^0_{K'^*}(P'^*))$이 E^1에 대한 $\gamma \rightarrow \delta$ 인 연관키 차분 특성을 만족할 확률이 q_γ이므로, 각각의 β, γ에 대해서 평균적으로 $m^2 \cdot p_\beta^2 \cdot q_\beta^2 \cdot 2^{-n}$의 쿼텟이 식 (1)을 만족한다. 그러므로 모든 옳은 쿼텟의 수(식 (1)을 만족하는 쿼텟의 수)는 평균적으로 다음과 같다.

$$\sum_{\beta,\gamma} m^2 \cdot p_\beta^2 \cdot q_\beta^2 \cdot 2^{-n} = m^2 \cdot \hat{p}^2 \cdot \hat{q}^2 \cdot 2^{-n}.$$

반면, 랜덤한 암호의 경우 이러한 쿼텟의 수의 기댓값은 $m^2 \cdot 2^{-2n}$개다. 그러므로 $\hat{p} \cdot \hat{q} > 2^{-n/2}$이면 연관키 차분 구별자를 이용하면 랜덤한 경우와 구별이 가능하다.

4. 8-라운드 mCrypton에 대한 연관키 차분 공격

본 절에서는 mCrypton에 대한 7-라운드 연관키 렉탱글 구별자를 설명하고, 이를 이용한 128-비트 키를 사용하는 8-라운드 블록 암호 mCrypton에 대한 연관키 차분 공격을 제안한다. 본 공격에서 사용하는 표기법은 다음과 같다.

- $K_0, K_0^*, K_0', K_0'^*$: 각각 마스터 키 K, K^*, K', K'^*로 생성된 0 라운드 화이트닝 키
- $K_i, K_i^*, K_i', K_i'^*$: 각각 마스터 키 K, K^*, K', K'^*로 생성된 i 라운드 서브키
- a: 고정된 0이 아닌 니블 값
- b: 입력 차분이 a일 때, S-박스의 출력 차분.
- *: 알려지지 않은 니블 값
- $\Delta K^*, \Delta K', \Delta P^*, \Delta I'$: 그림 2와 3의 차분
- $E_K(\cdot)$: K를 사용하는 8-라운드 암호화 함수
- $E^0_K(\cdot)$: K를 사용하는 1~4 라운드 함수(4 라운드)

• $E_K^1(\cdot)$: K를 사용하는 5~7 라운드 함수(3 라운드)

4.1 7-라운드 연관키 렉탱글 구별자

그림 2와 3은 본 논문에서 제안하는 연관키 구별자에서 사용하는 확률 1인 두 개의 연관키 부정 차분을 나타낸다. 마스터 키의 차분이 $\Delta K^*(\Delta K')$이면, 1-4(5-7) 라운드의 서브키의 차분은 $\Delta K_0^*, \Delta K_1^*, \Delta K_2^*, \Delta K_3^*, \Delta K_4^*(\Delta K_5', \Delta K_6', \Delta K_7')$이다.

• **E^0에 대한 4-라운드 차분 특성.** K, K^*, K', K'^*는 연관키 차분 $\Delta K^* = K \oplus K^* = K' \oplus K'^*$을 만족하는 연관키 쿼텟이고, P, P^*, P', P'^*는 차분 $\Delta P^* = \Delta P^* = P \oplus P^* = P' \oplus P'^*$을 만족하는 평문 쿼텟이고, P, P^*, P', P'^*는 각각 $E_K^0, E_{K^*}^0, E_{K'}^0, E_{K'^*}^0$을 사용하여 암호화 한다. 이러한 평문 쌍 (P, P^*)와 (P', P'^*)는 그림 2에서 설명하는 연관키 차분 특성을 따른다. 즉, 입력 키들이 앞의 연관키 차분을 만족할 때, 입력 차분은 ΔP^*이면 4 라운드 후 출력 차분의 모든 바이트는 모두 0이 아닌 특성을 가진다.

• **E^1에 대한 3-라운드 차분 특성.** 유사한 방법으로 E^1에 대한 연관키 부정 차분 특성을 구성한다. K, K^*, K', K'^*는 연관키 차분 $\Delta K' = K \oplus K' = K^* \oplus K'^*$을 만족하는 연관키 쿼텟이다. 이 때, K^*와 K'은 $K^* = K \oplus \Delta K^*$, $K' = K \oplus \Delta K'$, $K'^* = K \oplus \Delta K^* \oplus \Delta K'$을 만족하는 키 차분이다. 이 때, $E_K^0(P) \oplus E_{K'}^0(P') = E_{K^*}^0(P^*) \oplus E_{K'^*}^0(P'^*) = \Delta I'$가 성립하면, $(E_K^0(P), E_{K'}^0(P'))$과 $(E_{K^*}^0(P^*), E_{K'^*}^0(P'^*))$는 그림 3에서 설명하는 연관키 차분 특성을 따른다. 여기서, 3-라운드 차분 특성의 출력 차분은 ΔT의 하나의 원소이고, 그림 3에서 b는 S-박스의 입력 차분이 a일 때, 가능한 7개의 출력 차분 중 하나를 의미한다. 즉, E^1에서 키들이 연관키 차분 특성을 따를 때, 입력 차분이 $\Delta I'$이면 3 라운드 후 출력 차분은 1, 2, 3, 4, 13 번째 바이트만 0이 아니고, 나머지 바이트는 0이 됨을 말한다.

• **$E^1 \circ E^0$에 대한 7-라운드 렉탱글.** 위에서 설명한 두 개의 연관키 부정 차분 특성을 이용하여 7-라운드 높은 확률을 갖는 연관키 렉탱글 구별자를 구성

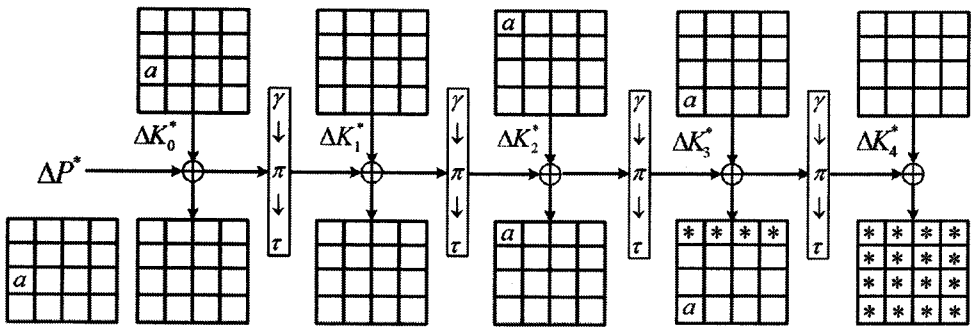


그림 2. E^0에 대한 4-라운드 부정 차분 특성

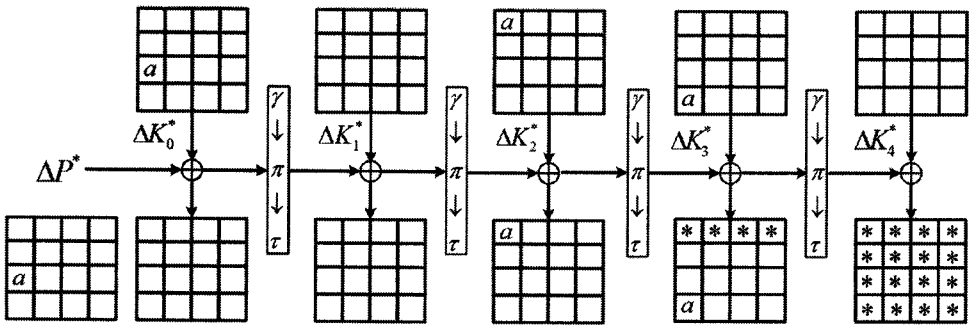


그림 3. E^1에 대한 3-라운드 부정 차분 특성

하고, 확률을 계산하기 위해서 다음과 같이 A_1과 A_2를 가정한다.

[A_1] 키 쿼텟 $[K,K^*,K',K'^*]$은 다음을 만족한다.

$$K\oplus K^* = \Delta K^* = (0,0,0,\alpha,0,0,0,0). \quad (2)$$

$$K'\oplus K'^* = \Delta K^* = (0,0,0,\alpha,0,0,0,0). \quad (3)$$

여기서, $0=(0_4,0_4,0_4,0_4)$, $\alpha=(a,0_4,0_4,0_4)$, $\alpha'=(a_L,a_R,0_4,0_4)\in\{0,1\}^{16}$, $0_4=(0,0,0,0)\in\{0,1\}^4$이 고 , $a=(a_1,a_2,a_3,a_4)$, $a_L=(0,0,0,a_1)$, $a_R=(a_2,a_3,a_4,0)$이다.

[A_2] 평문 쿼텟 (P,P^*,P',P'^*)은 다음을 만족한다.

$$P\oplus P^* = P'\oplus P'^* = \Delta P^* = (0,0,\alpha,0)^T.$$

I,I^*,I',I'^*가 각각 $E_K^0(P),E_{K^*}^0(P^*),E_{K'}^0(P')$, $E_{K'^*}^0(P'^*)$ 일 때, $I\oplus I^*$과 $I'\oplus I'^*$가 같은 확률은 $(2^{-16}\cdot 2^{-2})^2\cdot 2^{16}+(2^{-16}\cdot 2^{-3})^2\cdot 6\cdot 2^{16}=\frac{3}{2}\cdot 2^{-22}$이 된다. 하나의 S-박스의 입력 차분이 a이고, 4 개의 S-박스에 차분이 발생한다. 또한, π와 τ는 선형이므로 확률 1이다. 그러므로 $\hat{p}=\sqrt{1.5\cdot 2^{-22}}$이다.

첫 번째 차분 특성과 두 번째 차분 특성을 연결하기 위해서 $I\oplus I'$과 $I^*\oplus I'^*$가 $\Delta I'$으로 같은 확률을 계산하여야 한다. 암호화 과정에서 중간 값들이 모든 가능한 값들의 균일 분포를 따른다고 하면, $I\oplus I^*=I'\oplus I'^*$인 경우에서 $I\oplus I'=I^*\oplus I'^*=\Delta I'$일 확률은 2^{-64}이다. 다음을 만족한다.

$$I\oplus I^*=I'\oplus I'^* \text{이고 } I\oplus I'=I^*\oplus I'^*=\Delta I'. \quad (4)$$

임의의 중간 값이 위의 식 (4)를 만족일 확률은 $\frac{3}{2}\cdot 2^{-22}\cdot 2^{-64}=\frac{3}{2}\cdot 2^{-86}$이다. E^1에 대한 연관키 차분 특성의 확률이 1이므로, $E_K^1(I)\oplus E_{K'}^1(I')$과 $E_{K^*}^1(I^*)\oplus E_{K'^*}^1(I'^*)$이 차분 집합 ΔT에 포함될 확률은 $\frac{3}{2}\cdot 2^{-22}\cdot 2^{-64}=\frac{3}{2}\cdot 2^{-86}$이다. 반면에 ΔT의 개수가 7이므로 동일한 상황이 랜덤 암호에서 발생할 확률은 $(2^{-64}\cdot 7)^2=2^{-133}$이다. 식 (4)를 만족하는 평문 쿼텟 (P,P^*,P',P'^*)을 옳은 쿼텟으로 정의한다.

4.2 8-라운드 키 복구 공격

본 논문에서 제안하는 8-라운드 공격은 7-라운드 연관키 렉탱글 구별자를 이용하여 그림 3의 ΔO에서 $*$로 표시된 각 서브키 $K_{eq},K_{eq}^*,K'_{eq},K'^*_{eq}$의 5 바이트를 복구한다. 여기서, $K_{eq}=\phi(K_8),K_{eq}^*=\phi(K_8^*)$ $K'_{eq}=\phi(K_8'),K'^*_{eq}=\phi(K'^*_8)$을 의미한다. K,K^*,K',K'^*의 관계를 만족하는 키 쿼텟의 수는 2^{40}이다. 8 라운드 서브키의 관계는 그림 4와 같다.

공격의 기본 아이디어는 다음과 같다. (P,P^*,P',P'^*)이 옳은 쿼텟이라 할 때, 이에 대응하는 암호문 쿼텟을 (C,C^*,C',C'^*)이라 하고, $D_k(\cdot)$을 8 라운드의 5-바이트 후보 키를 이용한 복호화 연산으로 정의한다. 공격자는 5-바이트 키 쿼텟 (k,k^*,k',k'^*)을 추측하고, $D_k(C)\oplus D_{k'}(C')\in\Delta T^5$와 $D_{k^*}(C^*)\oplus D_{k'^*}(C'^*)\in\Delta T^5$를 검사한다. 여기서, ΔT^5는 그림 3에서 회색으로 표시된 5 개의 니블의 가능한 집합을 의미한다. 만약 위의 검사를 통과한 암호문 쿼텟의 수가 적절한 임계치보다 큰 경우, 이 때 추측한 키 쿼텟을 옳은 키로 결정한다.

공격 알고리즘을 단계별로 표현하면 다음과 같다.

- **단계 1.** $2^{43.5}$개의 평문 쌍 (P_i,P_i^*)와 $2^{43.5}$개의 평문 쌍 (P'_j,P'^*_j)를 선택한다. 이 때, $P_i\oplus P_i^*=P'_j\oplus P'^*_j=\Delta P^*$를 만족한다. 각 평문 P_i,P_i^*,P'_j,P'^*_j를 K,K^*,K',K'^*를 사용하여 암호화한 (C_i,C_i^*,C'_j,C'^*_j)를 얻는다. 이 암호문을 테이블에 저장한다.
- **단계 2.** 모든 i,j에 대해서, $C_i\oplus C'_j\in\Delta O$와 $C_i^*\oplus C'^*_j\in\Delta O$인지 검사한다. 이 검사를 통과하지 않는 암호문 쿼텟을 필터링한다.
- **단계 3.** 8 라운드의 5 바이트 키 쿼텟 (k,k^*,k',k'^*)을 추측한다.
  - **단계 3.1.** 단계 2를 통과한 호문 쿼텟에 대해 $D_k(C)\oplus D_{k'}(C')\in\Delta T^5$와 $D_{k^*}(C^*)\oplus D_{k'^*}(C'^*)\in\Delta T^5$를 검사한다.
  - **단계 3.2.** 단계 1을 통과한 암호문 쿼텟의 수가 2 보다 크거나 같으면, 이 때 추측한 키 쿼텟 (k,k^*,k',k'^*)을 옳은 8 라운드 키 쿼텟으로 결정한다. 2 보다 작은 경우는 단계 3으로 돌아간다.

본 공격에서는 $2^{43.5}$개의 원소를 갖는 두 개의 평문 쌍 집합과 이에 대응하는 암호문 쌍을 저장할 메모리를 필요로 한다. 그러므로 데이터 복잡도는 $2^{45.5}$개의 선택 평문이고, 메모리 복잡도는 $5\cdot 2^{47.5}=(2^{45.5}\cdot 20)$ 바이트이다.

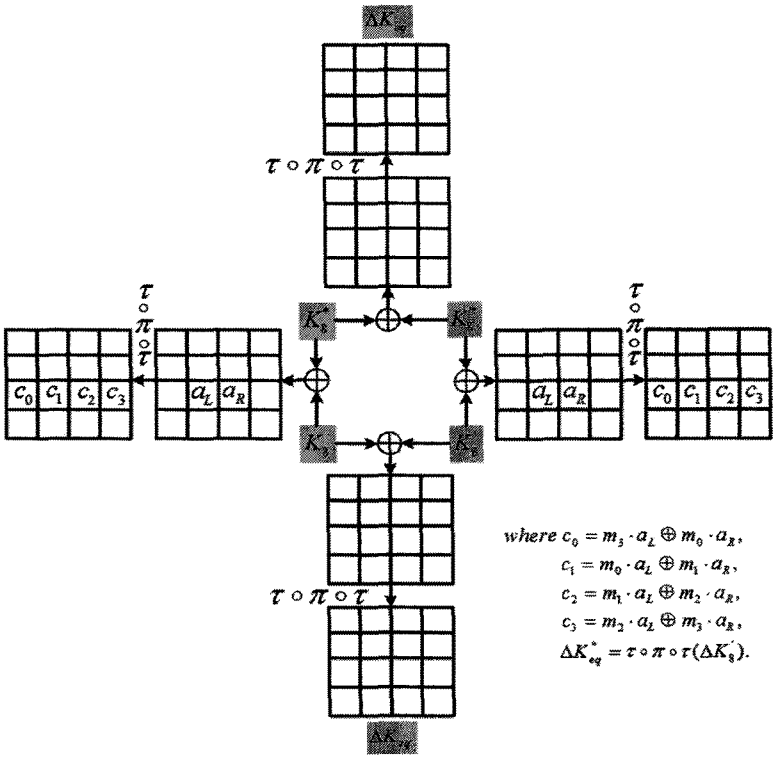


그림 4. mCrypton 1 ~ 8 라운드에서 4개의 연관키 차분 특성

단계 2에서 $2^{43.5}$개의 암호문 쌍에 대해 $2^{43.5}$번의 검색이 필요하다. 이 과정은 암호문 쿼텟의 정렬을 통해 효율적으로 구현 가능하다. 단계 2의 검사를 통해 88-비트 필터링이 수행된다 (틀린 암호문 쿼텟에 대해 $C_i \oplus C_j' \in \Delta O$와 $C_i^* \oplus C_j'^* \in \Delta O$를 만족할 확률은 $2^{-88}(2^{-11 \cdot 4 \cdot 2})$이다). 그러므로 단계 2를 통과하는 암호문 쿼텟의 기댓값은 $3.5\left(\approx 2^{87} \cdot \left(\frac{3}{2} \cdot 2^{-86} + 2^{-88}\right)\right)$이다. 즉, $3\left(= 2^{87} \cdot \frac{3}{2} \cdot 2^{-86}\right)$개의 옳음 암호문 쿼텟이 7-라운드 렉탱글 구별자를 통과할 것으로 기대되고, 랜덤하게 통과하는 암호문 쿼텟의 기댓값은 1보다 작다. 이러한 기댓값을 이용하여 단계 3의 시간 복잡도를 계산한다. 다시 말해서, 단계 3에서는 평균적으로 $2^{40}\left(\approx 2^{40} \cdot 3.5 \cdot 4 \cdot \frac{1}{8} \cdot \frac{1}{2}\right)$의 8-라운드 mCrypton 암호화 연산량이 필요하다. 그리하여 공격에 필요한 시간 복잡도는 단계 1의 시간 복잡도에 의해 결정된다. 그러므로 본 공격의 시간 복잡도는 $2^{45.5}$의 8-라운드 mCrypton 암호화 연산량이다.

본 공격의 성공 확률은 다음과 같이 계산 가능하다. 옳은 키 쿼텟에 대해 2 개 이상의 암호문 쿼텟이 단계 3.1의 검사를 통과할 확률은 다음과 같다.

$$0.8\left(\approx \sum_{i=2}^{2^{87}} \binom{2^{87}}{i} \left(\frac{3}{2} \cdot 2^{86}\right)^i \left(1 - \frac{3}{2} \cdot 2^{86}\right)^{2^{87}-i}\right).$$

반면에, 틀린 키가 공격 알고리즘에 의해 통과할 확률은 다음과 같다.

$$2^{-33}\left(2^{40} \cdot \sum_{i=2}^{2^{87}} \left(2^{-123}\right)^i \left(1 - 2^{-123}\right)^{2^{87}-i}\right).$$

그러므로 본 공격의 성공확률은 약 0.8 $(\approx 0.8 \cdot (1 - 2^{-33}))$이다.

5. 결 론

USN/WBro/RFID 등의 새로운 통신 환경이 현실화 되면서 이러한 제약된 환경에서 보안과 프라이버시 보호를 위한 블록 암호 알고리즘이 필요하다. mCrypton은 Crypton의 설계를 바탕으로 제한된 자원을 사용하는 환경에 적합하도록 소프트웨어와 하드웨어 효율성이 향상되도록 설계되어 RFID 태그나

USN의 센서등과 같이 제약된 자원을 사용하는 환경에 적합하다.

본 논문에서는 연관키 렉탱글 공격을 통해 128-비트 키를 사용하는 8-라운드 mCrypton에 대하여 $2^{45.5}$의 데이터와 $2^{45.5}$의 시간 복잡도를 가지는 공격을 제안하였다. 이는 mCrypton에 대한 첫 번째 분석 결과이다. 본 논문의 기법을 다른 경량 블록 암호알고리즘의 안전성 분석에 적용하는 것은 의미있는 연구가 될 것이다. 더 나아가 단순한 키 스케쥴을 이용하면서 안전성을 보장할 수 있는 방법에 대한 연구는 향후 연구로 의미가 있을 것이다.

참 고 문 헌

[1] C. Lim and T. Korkishko, "mCrypton - A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors," *WISA 2005, LNCS* 3786, pp. 243-258, Springer-Verlag, 2005.

[2] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K.Jeong, H. Kim, J. Kim, and S. Chee, "HIGHT: a new block cipher suitable for low-resource device," *CHES 2006, LNCS* 4249, pp. 46-59, Springer-Verlag, 2006.

[3] F. Standaert, G. Piret, N. Gershenfeld, and J. Quisquater, "SEA: A Scalable Encryption Algorithm for Small Embedded Applications," *CARDIS 2006, LNCS* 3928, pp. 222-236, Springer-Verlag, 2006.

[4] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," *CHES 2007, LNCS* 4227, pp. 450-466, Springer-Verlag, 2007.

[5] C. Lim, Crypton, "A Revised Version of CRYPTON: CRYPTON v1.0," *FSE 1999, LNCS* 1636, pp. 31-45, Springer-Verlag, 1999.

[6] 김태현, 김종성, 성재철, 홍석희, "축소된 20-라운드 SMS4에 대한 차분 공격," *정보보호학회논문지*, Vol.18, No.4, pp. 37-44, 2008.

[7] 김종성, 정기태, 이상진, 홍석희, "새로운 블록암호 구조에 대한 차분/선형 공격의 안전성 증명," 정보보호학회논문지, Vol.17, No. 1, pp. 121-125, 2007.

[8] 김구일, 김종성, 홍석희, 이상진, "축소 라운드 SHACAL-2의 차분-선형 유형 공격," *정보보호학회논문지*, Vol.15, No.1, pp.57-66, 2005.

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

[10] E. Biham, O. Dunkelman, and N. Keller, "Related-Key Boomerang and Rectangle Attacks," *EUROCRYPT 2005, LNCS* 3494, pp. 507-525, Springer-Verlag, 2005.

[11] S. Hong, J. Kim, S. Lee, and B. Preneel, "Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192," *FSE 2005, LNCS* 3557, pp. 368-383, Springer-Verlag, 2005.

[12] J. Kim, S. Hong, and B. Preneel, "Related-Key Rectangle Attacks on Reduced AES-192 and AES-256," *FSE 2007, LNCS* 4593, pp. 225-241, Springer-Verlag, 2007.

[13] E. Biham, O. Dunkelman, and N. Keller, "A Related-Key Rectangle Attack on the Full KASUMI," *ASIACRYPT 2005, LNCS* 3788, pp. 443-461, Springer-Verlag, 2005.

[14] O. Dunkelman, N. Keller, and J. Kim, "Related-Key Rectangle Attack on the Full SHACAL-1," *SAC 2006, LNCS* 4356, pp. 28-44, Springer-Verlag, 2006.

[15] J. Kim, G. Kim, S. Lee, J. Lim, and J. Song, "Related-Key Attacks on Reduced-Rounds of SHACAL-2," *INDOCRYPT 2004, LNCS* 3348, pp. 175-190, Springer-Verlag, 2004.

[16] C. Lee, J. Kim, S. Hong, J. Sung, and S. Lee, "Security Analysis of the Full-Round DDO-64 Block Cipher," *Journal of Systems and Software*, Vol.81, No.1, pp. 2328-2335, 2008.

[17] J. Lu, "Related-Key Rectangle Attack on 36

Rounds of the XTEA Block Cipher," *International Journal of Information Security,* in press, online first July 2008.

[18] J. Lu, and J. Kim, "Attacking 44 Rounds of the SHACAL-2 Block Cipher using Related-Key Rectangle Cryptanalysis," *IEICE Transactions*, Vol. 91-A(9), pp. 2588-2596, 2008.

[19] J. Lu, J. Kim, N. Keller, and O. Dunkelman, "Related-Key Rectangle Attack on 42-Round SHACAL-2," *ISC 2006, LNCS* 4176, pp. 85-100, Springer-Verlag, 2006.

[20] J. Lu, J. Kim, N. Keller, and O. Dunkelman, "Differential and Related-Key Rectangle Attacks on Reduced-Round SHACAL-1," *INDOCRYPT 2006, LNCS* 4329, pp. 17-31, Springer-Verlag, 2006.

[21] J. Lu, C. Lee, and J. Kim, "Related-Key Attacks on the Full-Round Cobra-F64a and Cobra-F64b," *SCN 2006, LNCS* 4116, pp. 95-110, Springer-Verlag, 2006.

[22] G. Wang, "Related-Key Rectangle Attack on 43-Round SHACAL-2," *ISPEC 2007, LNCS* 4464, pp. 33-42, Springer-Verlag, 2007.

[23] 김종성, 김구일, 이상진, 임종인, "4 축소 라운드 SHACAL-2의 연관키 공격," *정보보호학회논문지*, Vol.15, No.3, pp. 115-126, 2005.

[24] 김종성, 김구일, 홍석희, 이상진, "SHACAL-1의 축소 라운드에 대한 연관키 Rectangle 공격," *정보보호학회논문지*, Vol.14, No.5, pp. 57-68, 2004.

[25] M. Gorski and S. Lucks, "New Related-Key Boomerang Attacks on AES," *INDOCRYPT 2008, LNCS* 5365, pp. 266-278, Springer-Verlag, 2008.

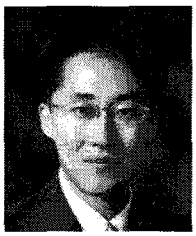
[26] E. Lee, J. Kim, D. Hong, C. Lee, J. Sung, S. Hong, and J. Lim, "Weak-Key Classes of 7-Round MISTY 1 and 2 for Related-Key Amplied Boomerang Attacks," *IEICE Transactions*, Vol. 91-A(2), pp. 642-649, 2008.

이 창 훈

2001년 2월 한양대학교 수학과 학사
2003년 2월 고려대학교 정보보호대학원 석사
2008년 2월 고려대학교 정보보호대학원 박사
2008년 4월~2009년 2월 고려대학교 정보보호연구원 연구교수
2009년 2월~현재 한신대학교 컴퓨터공학부 전임강사
관심분야 : 정보보호, 대칭키 암호 설계 및 분석

이 유 섭

2007년 2월 서울시립대학교 수학과학사
2007년 3월~현재 고려대학교 정보경영공학전문대학원 석박사 통합과정
관심분야 : 대칭키 암호알고리즘 설계 및 분석



성 재 철

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 조교수
관심분야 : 정보보호, 암호 알고리즘 설계 및 분석