情報保護學會論文誌
第15券 第1號, 2005. 2

축소 라운드 SHACAL-2의 차분-선형 유형 공격

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

Differential-Linear Type Attacks on Reduced Rounds of SHACAL-2

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

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 선정되었다. 본 논문에서는 차분-선형 공격을 다양하게 확장한 차분-선형 유형 공격에 대한 SHACAL-2의 안전성을 논의한다. SHACAL-2는 전체 64 라운드로 구성되며, 차분-선형 유형 분석 기법을 통하여 512 비트 키를 사용하는 32 라운드 SHACAL-2를 공격한다. 본 논문에서 소개하는 512 비트 키를 가지는 32 라운드 SHACAL-2에 대한 공격은 SHACAL-2 블록 암호에 알려진 분석 결과 중 가장 효과적이다.

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. This paper presents differential-linear type attacks on SHACAL-2 with 512-bit keys up to 32 out of its 64 rounds. Our 32-round attack on the 512-bit keys variants is the best efficient attack on this cipher in published literatures.

Keywords : *Differential Attack, Linear Attack, Differential-Linear Attack, SHACAL-2*

Ⅰ. 서 론

SHACAL-2[4]는 NESSIE(New European Schemes for Signatures, Integrity, and Encryption) 프로젝트에 제안된 256-비트 블록 암호이다. 이는 국제 표준 해쉬 알고리즘 SHA-2[9]의 압축 함수에 기반을 두었으며, 최근 NESSIE 프로젝트의 256-비트 블록 암호로 선정되었다.

현재까지 SHACAL-2[4] 블록 암호에 대한 암호학적 분석 결과는 불능 차분 특성을 이용한 30-라운드 SHACAL-2의 안전성 평가만 이루어졌다.[5] [5]에 의해 소개된 공격은 마지막 3 라운드의 비선형

표 1. SHACAl-2의 분석 결과 비교

	공격 유형	라운드	복잡도 데이터 / 시간/ 메모리
[5]	불능 차분 공격	30	$744CP$ / $2^{495.1}$ / $2^{14.5}$
본 논문	차분-선형 유형 공격	32	$2^{43.4}CP$ / $2^{504.2}$ / $2^{48.4}$
		28	$463 \cdot 2^{32}CP$ / $2^{494.1}$ / $2^{45.9}$

CP: 선택 평문, 시간: 암호화 단위,
메모리: 바이트 단위

접수일 : 2004년 10월 21일 ; 채택일 : 2005년 2월 11일
* 본 연구는 정보통신부 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었습니다.
† 주저자, okim912@cist.korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

관계식을 이용한 14-라운드 불능 차분 특성을 기반으로 하고 있다.

본 논문에서는 14-라운드 부정 차분 특성을 17-라운드 특성으로 확장하고자 [5]에 표현된 3-라운드 비선형 관계식을 이용한다. 확장된 17-라운드 특성은 512-비트 키를 사용하는 32-라운드 SHACAL-2에 대해 전수 조사 공격 보다 빠른 공격을 가능케 한다. 또한 본 논문에서는 10-라운드 포화 특성을 13-라운드 특성으로 확장하기 위해 3-라운드 비선형 관계식을 이용한다. 확장된 13-라운드 특성은 512-비트 키를 사용하는 28-라운드 SHACAL-2에 대해 전수 조사 공격 보다 빠른 공격을 가능케 한다. 본 논문의 분석과 [5]의 분석 결과의 비교는 표 1과 같다.

II. SHACAL-2 블록 암호의 소개

H. Handschuch와 D. Naccache에 의해 제안된 SHACAL-2[4]는 국제 표준 해쉬 함수 알고리즘 SHA-2[9]의 압축 함수에 기반을 두었으며, 다양한 키 길이(최대 512 비트)를 가지는 256-비트 블록 암호이다. 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 $A^0,B^0,C^0,D^0,E^0,F^0,G^0,H^0$으로 표현되며, 64 라운드 과정을 거친 후 암호문은 $A^{64},B^{64},C^{64},D^{64},E^{64},F^{64},G^{64},H^{64}$이다. $i(=0,...,63)$번째 라운드 암호화 과정은 다음과 같다.

여기서 +는 법 2^{32} 덧셈을 의미하며, W^i는 32 비트 라운드 키, K^i는 32 비트 라운드 상수 값이다

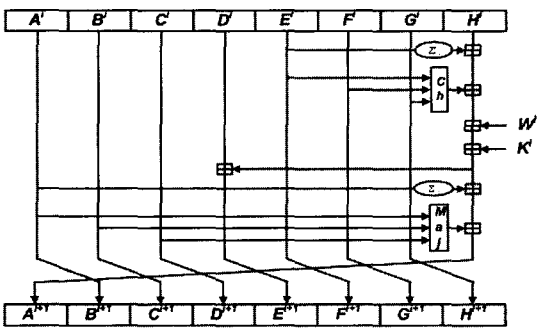


그림 1. SHACAL-2의 i번째 라운드 암호화 과정

(각 라운드 상수값은 [9]을 참조하라). 위에 정의된 i번째 라운드 암호화 과정에 사용하는 함수는 다음과 같다.

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

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

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

$$H^{i+1}=G^i$$
$$G^{i+1}=F^i$$
$$F^{i+1}=E^i$$
$$E^{i+1}=D^i+T_1^{i+1}$$
$$D^{i+1}=C^i$$
$$C^{i+1}=B^i$$
$$B^{i+1}=A^i$$
$$A^{i+1}=T_1^{i+1}+T_2^{i+1}$$

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

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

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

SHACAL-2의 키는 최대 512 비트까지 허용되며 512 비트 보다 작은 키에 대해서는 0 스트링을 패딩하여 총 512 비트를 생성한 후 사용한다. 하지만 SHACAL-2는 128 비트 보다 작은 키의 사용은 지양한다. 512 비트 키 스트링을 $W=[W^0\mid W^1\mid\cdots\mid W^{15}]$와 같이 표시하면, 2048 비트 키 확장 과정은 다음과 같다.

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

여기서 $R_i(x)$는 32 비트 워드 x의 i비트 오른쪽 쉬프트를 의미한다 (즉, $R_i(x)=x\ll i$).

III. 차분-선형 유형 공격

1994년 Langford와 Hellman은 [6]에서 차분

공격[1]과 선형 공격[7]을 결합하는 차분-선형 공격 방법을 소개하였다. 차분-선형 공격 방법(Differential-Linear Cryptanalysis)의 일반화된 형태는 다음과 같다.

차분 특성을 표현하기 위하여 본 논문에서는 입력 차분을 Ω_P으로, 출력 차분을 Ω_T으로 표기한다. 또한 선형 근사식을 표현하기 위하여 입력 비트 마스크, 출력 비트 마스크, 부분 키 비트 마스크를 각각 λ_P, λ_T, λ_K으로 표기한다. E를 블록 암호라 정의할 때, $E = E_1 \circ E_0$라 가정하자. 차분 특성과 선형 근사식의 결합은 부분 암호 E_0에 확률 p를 가지는 차분 특성 $\Omega_P \rightarrow \Omega_T$와, 부분 암호 E_1에 확률 $\frac{1}{2}+q$을 가지는 선형 근사식 $\lambda_P \rightarrow \lambda_T$을 이용한다. P와 P^*를 차분 조건 $P \oplus P^* = \Omega_P$을 만족하는 평문 쌍이라 가정할 때, Langford와 Hellman은 E_0에 확률 1을 가지는 부정 차분 특성 $\Omega_P \rightarrow \Omega_T$을 이용하였다. $E_0(P) \oplus E_0(P^*)$의 값은 확률 1로 특정 위치의 값이 고정된다. 따라서 적당한 비트 마스크 λ_P를 통해 한 비트 방정식을 유도할 수 있다. 즉, $\lambda_P \cdot (E_0(P) \oplus E_0(P^*)) = a$은 확률 1로 성립한다. 단, a의 값은 0 또는 1이며, $a = \lambda_P \cdot \Omega_T$이다. 또한 부분 암호 E_1의 선형 근사식 존재성에 대한 가정에 따라 확률 $\frac{1}{2}+q$ 또는 바이어스 q를 가지는 두 개의 선형 근사식

$$\lambda_P \cdot E_0(P) \oplus \lambda_T \cdot E_1(E_0(P)) \oplus \lambda_K \cdot K = 0 \text{와}$$
$$\lambda_P \cdot E_0(P^*) \oplus \lambda_T \cdot E_1(E_0(P^*)) \oplus \lambda_K \cdot K = 0$$

을 얻을 수 있다. 단, K는 부분 암호 E_1에 사용하는 부분 키이다. 따라서, [7]에 소개된 piling up lemma를 사용하여 확률 $\frac{1}{2}+2q^2 (= \frac{1}{2}+2^{2-1} \cdot q \cdot q)$을 갖는 선형 근사식을 다음과 같이 얻을 수 있다.

$$\lambda_T \cdot E_1(E_0(P)) \oplus \lambda_T \cdot E_1(E_0(P^*)) = a \qquad (1)$$

따라서 (1)을 이용한 선형 공격을 수행하기 위해서 $O(q^{-4})$ 개의 선택 평문 쌍을 요구한다.

2002년 [2]에서 Biham, Dunkleman, Keller는 위의 차분-선형 공격은 차분 특성이 1보다 작은 경우로 확장할 수 있음을 소개하였다. 이러한 분석 방법을 향상된 차분-선형 공격(Enhanced Differential-Linear Cryptanalysis)이라 부르며, 일반화 된 공격 형태는 다음과 같다.

부분 암호 E_0에 확률 $p(\leq 1)$를 가지는 차분 특성 $\Omega_P \rightarrow \Omega_T$이 존재한다고 가정하자. 평문 쌍 P와 P^*가 차분 특성 $\Omega_P \rightarrow \Omega_T$을 만족한다면(확률 p에 따라 성립한다), 확률 1을 가지고 한 비트 방정식 $\lambda_P \cdot (E_0(P) \oplus E_0(P^*)) = a$이 성립한다. 반면, 평문 쌍 P와 P^*가 차분 특성 $\Omega_P \rightarrow \Omega_T$을 만족하지 않는다면(확률 $1-p$에 따라 성립한다), $\lambda_P \cdot (E_0(P) \oplus E_0(P^*))$의 값은 랜덤하게 분포한다고 가정한다. 따라서 위의 두 경우를 모두 고려하여 차분 조건 $P \oplus P^* = \Omega_P$을 만족하는 평문 쌍 P와 P^*는 확률 $\frac{1}{2}+\frac{p}{2} (= p \cdot 1 + (1-p) \cdot \frac{1}{2})$를 가지고 한 비트 방정식 $\lambda_P \cdot (E_0(P) \oplus E_0(P^*)) = a$을 얻을 수 있다. 부분 암호 E_1의 두 개의 선형 근사식

$$\lambda_P \cdot E_0(P) \oplus \lambda_T \cdot E_1(E_0(P)) \oplus \lambda_K \cdot K = 0 \text{와}$$
$$\lambda_P \cdot E_0(P^*) \oplus \lambda_T \cdot E_1(E_0(P^*)) \oplus \lambda_K \cdot K = 0$$

을 이용하여 차분-선형 공격과 유사하게 확률 $\frac{1}{2}+2pq^2 (= \frac{1}{2}+2^{3-1} \cdot \frac{p}{2} \cdot q^2)$로 성립하는 선형 근사식 (1)을 얻을 수 있다. 따라서 향상된 차분-선형 공격을 수행하기 위해서 $O(p^{-2}q^{-4})$개의 선택 평문 쌍을 요구한다. 특별히 선형 근사식의 확률이 1이라면, 확률 $\frac{1}{2}+\frac{p}{2} (= \frac{1}{2}+2^{3-1} \cdot \frac{p}{2} \cdot (\frac{1}{2})^2)$로 선형 근사식 (1)이 성립하며, $O(p^{-2})$개의 선택 평문 쌍을 이용하여 공격할 수 있다.

지금부터 위의 차분-선형 분석 기술을 통해 유도할 수 있는 몇 가지 가능한 차분-선형 유형 공격을 소개한다. 본 논문에서는 차분 공격 또는 차분 공격의 변이 공격과 선형 공격 또는 선형 공격의 변이 공격을 결합하여 분석하는 모든 분석 방법을 차분-선형 유형 공격이라 표현한다.

차분-선형 공격은 평문 쌍을 이용하는 대신에 평문 집합을 이용하는 경우로 확장할 수 있다. 평문 집합은 특정 비트에 포화상태를 만족하는 포화 집합이라고 가정하자. 포화 집합이란 평문의 특정 n비트 자리에 가능한 모든 값이 정확하게 한 번씩 분포되어 있는 집합을 의미한다. 부분 암호 E_0에 확률 1을 갖는 포화 특성[3]이 존재한다고 가정하자. 따라서 특정 n비트 자리에 포화 상태를 만족하는 2^n개로 구

성된 평문 집합을 $P_i(i=0,...,2^n-1)$으로 표현한다면, 적당한 비트 마스크 λ_P를 이용하여 확률 1로 성립하는 한 비트 방정식 $\lambda_P \cdot (\oplus_{i=0}^{2^n-1} E_0(P_i))=0$을 유도할 수 있다. 부분 암호 E_1에 확률 $\frac{1}{2}+q$를 가지는 선형 근사식의 존재에 따라 각 평문 P_i에 대해 선형 근사식 $\lambda_P \cdot E_0(P_i) \oplus \lambda_T \cdot E_1(E_0(P_i)) \oplus \lambda_K \cdot K=0$을 나타낼 수 있다. 따라서 piling up lemma에 의해 확률 $\frac{1}{2}+2^{2^n-1}q^{2^n}$로 성립하는 선형 근사식 (2)를 얻을 수 있다.

$$\lambda_T \cdot (\bigoplus_{i=0}^{2^n-1} E_1(E_0(P_i)))=0 \quad (2)$$

선형 근사식 (2)를 이용한 선형 공격을 수행하기 위해서 $O((2^{2^n-1}q^{2^n})^{-2})$ 개의 선택 평문 쌍이 필요하다. 따라서 위의 공격은 q의 값이 $\frac{1}{2}$에 매우 근접하거나 $\frac{1}{2}$값을 갖는 블록 암호인 경우에 효과적으로 적용할 수 있다. 본 논문에서는 위의 분석 방법에 사용되는 특성을 포화-선형 특성(square-linear distinguisher)이라 부른다.

더 나아가서 본 논문에서는 부분 암호 E_1의 선형 근사식을 이용하는 대신에 비선형 근사식을 이용하는 방법으로 확장한다. 만약 공격에 사용할 수 있는 비선형 근사식이 임의의 선형 근사식 보다 좋은 확률로 성립한다면, 비선형 근사식을 이용하여 블록 암호의 분석에 효과적으로 적용할 수 있다. 본 논문에서는 차분 특성에 비선형 근사식을 결합한 형태를 차분-비선형 특성(differential-nonlinear distinguisher)이라 하고, 포화 특성에 비선형 근사식을 결합한 형태를 포화-비선형 특성(square-nonlinear distinguisher)이라 부른다.

Ⅳ. SHACAL-2에 대한 차분-선형 유형 공격

이 절에서는 축소 라운드 SHACAL-2의 차분-선형 유형 공격에 대한 안전성을 논의한다. 시작에 앞서 본 논문에서 사용하는 표기법을 정의한다. 단, 워드의 비트 위치는 가장 오른쪽 최하위 비트부터 0으로 시작하며, 왼쪽으로 갈수록 커진다.

- □ P: 256 비트 평문, $P=(A,\cdots,H)$ 또는 $P=(A^0,\cdots,H^0)$.
- □ P^r: r번째 라운드의 256 비트 입력 값, $P^r=(A^r,\cdots,H^r)$.
- □ 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 값 또는 알 수 없는 값들의 모임
- □ e_i: i번째 비트를 제외한 모든 비트가 0인 32 비트 워드.
- □ $e_{i_1,\ldots,i_k}$: $e_{i_1} \oplus \cdots \oplus e_{i_k}$ 또는 e_M 단, $M=\{i_1,...,i_k\}$.
- □ $e_{i_1,\ldots,i_k,\sim}$: $i_1,...,i_k$번째 자리의 값은 1, $(i_k+1)\sim 31$번째 자리의 값은 0, 1, 또는 알 수 없는 값이고, $i_1<\cdots<i_k$의 $i_1,...,i_k$를 제외한 자리의 값은 0인 32 비트 워드.
- □ z_i: i번째 자리의 값은 0, i번째를 제외한 모든 자리의 값은 0, 1, 또는 알 수 없는 값을 갖는 32비트 워드.
- □ CS(*Constant Set*) : 하나의 32 비트 상수가 2^{32}개로 구성되어 있는 집합.
- □ PS(*Permutation Set*) : 32 비트에 가능한 모든 값을 한번 씩 순서에 관계없이 포함하는 집합.
- □ $-PS$: 동일 라운드에서 PS 집합의 원소 x를 순서를 고려한다면, $-PS$는 $-x$로 구성된 32 비트 가능한 모든 값을 갖는 집합. 즉, 순서를 고려한 PS의 원소와 $-PS$의 원소의 합은 모두 0이 된다.
- □ BS(*Balanced Set*) : 임의의 값을 갖지만, 그들의 합(XOR)은 0이 되는 2^{32}개로 구성된 집합. 만약 이러한 성질이 0번째 비트에서 만족한다면, BS_0으로 표기한다.

이 절에서 소개하는 모든 공격은 [5]의 3-라운드 비선형 관계식을 이용한다. 3-라운드 비선형 관계식은 다음과 같다.

h_0^r는 비선형 함수 $NF(A^{r+3},B^{r+3},\cdots,H^{r+3},K^r,K^{r+1},K^{r+2},W^r,W^{r+1},W^{r+2})$의 출력 값으로 표현할 수 있다. 이 함수를 간단하게 NF^{r+3}로 표시한다. 단, $0 \le r \le 61$.

$$h_0^r = c_0^{r+3} \oplus d_2^{r+3} \oplus d_{13}^{r+3} \oplus d_{22}^{r+3} \oplus (d_0^{r+3} \& (e_0^{r+3} \oplus t_{1,0}^{r+3})) \oplus (d_0^{r+3} \& (f_0^{r+3} \oplus t_{1,0}^{r+2})) \oplus ((e_0^{r+3} \oplus t_{1,0}^{r+3}) \& (f_0^{r+3} \oplus t_{1,0}^{r+2})) \oplus h_6^{r+3} \oplus h_{11}^{r+3} \oplus h_{25}^{r+3} \oplus (h_0^{r+3} \& h_0^{r+2}) \oplus ((\neg h_0^{r+3}) \& h_0^{r+1}) \oplus k_0^r \oplus w_0^r$$

위 비선형 방정식의 $h_0^{r+1}, t_{1,0}^{r+2}, h_0^{r+2}, t_{1,0}^{r+3}$은 다음과 같이 표현할 수 있다.

$$h_0^{r+1} = t_{1,0}^{r+2} \oplus g_6^{r+3} \oplus g_{11}^{r+3} \oplus g_{25}^{r+3} \oplus (g_0^{r+3} \& h_0^{r+3}) \oplus ((\neg g_0^{r+3}) \& h_0^{r+2}) \oplus k_0^{r+1} \oplus w_0^{r+1}$$

$$t_{1,0}^{r+2} = b_0^{r+3} \oplus c_2^{r+3} \oplus c_{13}^{r+3} \oplus c_{22}^{r+3} \oplus (c_0^{r+3} \& d_0^{r+3}) \oplus (c_0^{r+3} \& (e_0^{r+3} \oplus t_{1,0}^{r+3})) \oplus (d_0^{r+3} \& (e_0^{r+3} \oplus t_{1,0}^{r+3}))$$

$$h_0^{r+2} = t_{1,0}^{r+3} \oplus f_6^{r+3} \oplus f_{11}^{r+3} \oplus f_{25}^{r+3} \oplus (f_0^{r+3} \& g_0^{r+3}) \oplus ((\neg f_0^{r+3}) \& h_0^{r+3}) \oplus k_0^{r+2} \oplus w_0^{r+2}$$

$$t_{1,0}^{r+3} = a_0^{r+3} \oplus b_2^{r+3} \oplus b_{13}^{r+3} \oplus b_{22}^{r+3} \oplus (b_0^{r+3} \& c_0^{r+3}) \oplus (b_0^{r+3} \& d_0^{r+3}) \oplus (c_0^{r+3} \& d_0^{r+3})$$

4.1 차분-비선형 특성을 이용한 32-라운드 SHACAL-2 공격

이 절에서는 14-라운드 부정 차분 특성을 구성하는 방법을 소개한 후, 이 차분 특성에 앞서 설명한 3-라운드 비선형 관계식을 연결하는 방법을 설명한다. 또한 구성된 17-라운드 차분-비선형 특성을 이용한 32-라운드 SHACAL-2 공격을 설명한다. 14-라운드 부정 차분 특성을 구성하기에 앞서 차분 확률을 계산하기 위해 사용하는 SHACAL-2의 두 가지 차분 성질을 소개한다.

SHACAL-2의 첫 번째 차분 성질은 XOR 연산과 법 덧셈 연산의 사용으로부터 유도할 수 있다. $Z = X + Y$, $Z^* = X^* + Y^*$라고 가정하자. 단, 각각의 X, Y, X^*, Y^*는 균일하게 분포하는 32 비트 난수이다.

□ 만약 $X \oplus X^* = e_j$이고 $Y = Y^*$라면, 확률 $\frac{1}{2^k}$를 가지고 $(j < 31, k \geq 1, j+k-1 \leq 30)$, $Z \oplus Z^* = e_{j,j+1,\ldots,j+k-1}$을 만족한다. 특별히 $j = 31$인 경우에 확률 1로 $Z \oplus Z^* = e_{31}$을 만족한다.

□ 만약 $X \oplus X^* = e_j$이고 $Y \oplus Y^* = e_j$라면, 확률 $\frac{1}{2^k}$를 가지고$(j < 31, k \geq 1, j+k-1 \leq 30)$, $Z \oplus Z^* = e_{j+1,\ldots,j+k-1}$을 만족한다. 특별히 $j = 31$인 경우에 확률 1로 $Z \oplus Z^* = 0$을 만족한다.

□ 만약 $X \oplus X^* = e_{i,\sim}$, $Y \oplus Y^* = e_{j,\sim}$이고, $i > j$ 라면, $Z \oplus Z^* = e_{j,\sim}$을 만족한다. 만약 $Z \oplus Z^* = e_{j,\sim}$을 만족한다면, 이는 또한 $Z \oplus Z^* = z_k$임을 의미한다. 단, $0 \leq k < j$.

표 2. 함수 Ch와 Maj의 XOR 차분 분포표

x	y	z	Ch	Maj
0	0	0	0	0
0	0	1	0/1	0/1
0	1	0	0/1	0/1
1	0	0	0/1	0/1
0	1	1	1	0/1
1	0	1	0/1	0/1
1	1	0	0/1	0/1
1	1	1	0/1	1

SHACAL-2의 두 번째 차분 성질은 Ch와 Maj 함수로부터 유도된다. 이 함수는 비트별 연산이므로, 각 함수는 3 비트 입력에 1 비트 출력 값을 갖는 부울 함수로 생각할 수 있다. 표 2는 Ch와 Maj 함수의 비트별 XOR 차분 특성을 나타낸다. 첫 번째 세 개의 열은 x, y, z의 여덟 가지 가능한 입력 차분 값을 표현하며, 다음 두 열은 각 함수 Ch와 Maj의 출력 차분 값을 표현한다. 마지막 두 열에서 0은 출력 차분 값이 항상 0임을 의미하고, 1은 출력 차분 값이 항상 1임을 의미한다. 반면, 0/1은 출력 차분 값이 확률 1/2로 0을 확률 1/2로 1을 만족함을 의미한다.

또한 Ch와 Maj 함수로부터 발생하는 차분 확률은 평문 쌍의 특정 비트를 고정함으로써 조절 가능하다. 즉, 평문 쌍의 특정 비트를 고정하여 처음 몇 라운드에 대한 차분 확률을 극대화 할 수 있다. Ch 함수에 대한 한 가지 예를 설명한다. 만약 Ch의 입력 차분 형태가 (0,0,1)과 같다면, 출력 차분 값은 0/1이다. 하지만 차분 (0,0,1)을 만족하는 두 개의 입력 값을 (1,0,0)와 (1,0,1)으로 선택한다면, Ch의 출력 차분 값은 확률 1을 가지고 0값을 가진다. 따라서 평문 쌍의 특정 비트를 고정하여 처음 몇 라운드의 Ch로부터 발생하는 차분 확률을 극대화 할 수 있다.

지금부터 14-라운드 부정 차분 특성을 구성하는 방법을 소개한다. 평문 쌍 $P = (A, B, C, D, E, F, G, H)$, $P^* = (A^*, B^*, C^*, D^*, E^*, F^*, G^*, H^*)$는 차분 $(0, 0, e_{M_1}, 0, 0, e_{31}, e_{M_2}, 0)$을 만족하고 (단, $M_1 = \{9, 18, 29\}$, $M_2 = \{6, 9, 18, 20, 25, 29\}$), 표 3과 같이 고정된 비트 값을 갖는다고 가정하자. 위의 조건을 만족하는 평문 쌍 P, P^*는 14 라운드 과정 후에 여덟 번째 워드의 최하위 비트 차분 Δh_0^{14}은 확률 2^{-22}로 0를 만족한다. 14-라운드 부정 차분 특성에 대한 자세한

차분 경로는 표 4를 통해 확인할 수 있다. 표 5에 나타나 있는 확률은 SHACAL-2의 두 가지 차분 성질을 이용하여 쉽게 확인할 수 있다.

14-라운드 부정 차분 특성과 3-라운드 비선형 방정식의 결합은 Δh_0^{14}에 의해 이루어진다. 따라서 ΔH^{14}의 값이 z_0가 되는 다양한 부정 차분 특성을 고려하여 위의 14-라운드 부정 차분 특성의 확률을 개선할 수 있다. 표 4의 14-라운드 부정 차분 특성 중 처음 9 라운드 같은 부정 차분 특성을 고려하여, ΔH^{14}의 값이 z_0형태를 가지는 다양한 형태의 ΔE^{10}을 계산할 수 있다(표 4를 참조하라). 이 결과에 기초하여 14-라운드 부정 차분 특성 확률은 $2^{-18.7}(\approx 1 \cdot 2^{-22}+4 \cdot 2^{-23}+9 \cdot 2^{-24}+16 \cdot 2^{-25}+16 \cdot 2^{-26}+42 \cdot 2^{-27}+51 \cdot 2^{-28})$으로 개선할 수 있다.

위에서 구성한 14-라운드 부정 차분 특성의 확률 $2^{-18.7}$은 확률 $2^{-19.7}(=2^{-18.7}+\frac{1}{2} \cdot (1-2^{-18.7}))$을 가지는 선형 근사식 확률로 전환할 수 있다. 즉, 차분 $(0,0,e_{M_1},0,0,e_{31},e_{M_2},0)$를 만족하고, 표 3과 같이 고정된 비트 값을 가지는 평문 쌍 P,P^*는 확률 $\frac{1}{2}+2^{-19.7}$을 가지고 $h_0^{14}=h_0^{*14}$를 만족한다. 확률 $\frac{1}{2}+2^{-19.7}$의 확인을 위해 10개의 다른 키에 대해 2^{34}개의 평문 쌍을 가지고, Δh_0^{14}의 값의 분포를 테스트 하였다. 2^{34}개의 평문 쌍에 대한 이론적인 결과는 $2^{33}+20170(=2^{34} \cdot (\frac{1}{2}+2^{-19.7}))$인 반면, 실제 구현 결과는 $2^{33}+153189$, $2^{33}+159168$,

표 3. 평문 쌍 P,P^*의 고정 비트

A,A^*	$a_9=a_9^*=0$, $a_{18}=a_{18}^*=0$, $a_{29}=a_{29}^*=0$, $a_{31}=a_{31}^*=0$
B,B^*	$b_9=b_9^*=0$, $b_{18}=b_{18}^*=0$, $b_{29}=b_{29}^*=0$, $b_{31}=b_{31}^*=0$
E,E^*	$e_6=e_6^*=1$, $e_9=e_9^*=1$, $e_{18}=e_{18}^*=1$, $e_{20}=e_{20}^*=1$, $e_{25}=e_{25}^*=1$, $e_{29}=e_{29}^*=1$, $e_{31}=e_{31}^*=1$
F,F^*	$f_6=f_6^*=0$, $f_9=f_9^*=0$, $f_{18}=f_{18}^*=0$, $f_{20}=f_{20}^*=0$, $f_{25}=f_{25}^*=0$, $f_{29}=f_{29}^*=0$
G,G^*	$g_{31}=g_{31}^*=0$

표 4. SHACAL-2의 14-라운드 부정 차분 특성에 대한 가능한 ΔE^{10}

ΔE^{10}	확률
$e_{6,9,18,20,25,\sim}$	2^{-22}
$e_{6,9,18,19,20,25,\sim}$	2^{-23}
$e_{6,7,9,18,19,20,25,\sim}$	2^{-24}
$e_{6,9,10,18,20,21,25,\sim}$	2^{-24}
$e_{6,9,18,19,25,\sim}$	2^{-24}
$e_{6,7,9,18,20,25,\sim}$	2^{-23}
$e_{6,9,18,20,21,25,\sim}$	2^{-23}
$e_{6,7,9,18,20,21,25,\sim}$	2^{-24}
$e_{6,9,18,19,20,21,25,\sim}$	2^{-24}
$e_{6,9,18,20,21,22,25,\sim}$	2^{-24}
$e_{6,9,10,18,20,25,\sim}$	2^{-23}
$e_{6,7,9,10,18,20,25,\sim}$	2^{-24}
$e_{6,9,10,18,19,20,25,\sim}$	2^{-24}
$e_{6,7,8,9,18,20,25,\sim}$	2^{-24}

표 5. SHACAL-2의 14-라운드 부정 차분 특성

r	ΔA^r	ΔB^r	ΔC^r	ΔD^r	ΔE^r	ΔF^r	ΔG^r	ΔH^r	확률
0	0	0	e_{M_1}	0	0	e_{31}	e_{M_2}	0	1
1	e_{31}	0	0	e_{M_1}	e_{31}	0	e_{31}	e_{M_2}	2^{-10}
2	0	e_{31}	0	0	0	e_{31}	0	e_{31}	2^{-2}
3	0	0	e_{31}	0	0	0	e_{31}	0	2^{-2}
4	0	0	0	e_{31}	0	0	0	e_{31}	1
5	e_{31}	0	0	0	0	0	0	0	2^{-4}
6	e_{M_1}	e_{31}	0	0	0	0	0	0	1
7	z_0	e_{M_1}	e_{31}	0	0	0	0	0	1
8	?	z_0	e_{M_1}	e_{31}	0	0	0	0	1
9	?	?	z_0	e_{M_1}	e_{31}	0	0	0	2^{-4}
10	?	?	?	z_0	e_{M_3}	e_{31}	0	0	1
11	?	?	?	?	z_0	e_{M_3}	e_{31}	0	1
12	?	?	?	?	?	z_0	e_{M_3}	e_{31}	1
13	?	?	?	?	?	?	z_0	e_{M_3}	1
14	?	?	?	?	?	?	?	z_0	

$M_1=\{9,18,29\}$, $M_2=\{6,9,18,20,25,29\}$, $M_3=\{6,9,18,20,25\}$

$2^{33}+161745$, $2^{33}+168761$, $2^{33}+173142$, $2^{33}+175476$, $2^{33}+177866$, $2^{33}+196441$, $2^{33}+197654$, $2^{33}+217151$의 값을 얻을 수 있었다. 테스트를 통한 결과는 14-라운드 특성의 확률이 이론적인 평가 $\frac{1}{2}+2^{-19.7}$보다 높다는 것을 알 수 있다. 이러한 결과 값의 차이는 ΔH^{14}의 값이 z_0 값을 가지는 부정 차분 특성 중 적은 경우만 고려했기 때문이다. 따라서 14-라운드 선형 근사식 확률은 $\frac{1}{2}+2^{-19.7}$보다 작지 않음을 알 수 있다.

앞서 차분-선형 공격의 일반적인 형태를 언급한 것과 같이 위의 부정 차분 특성에 3-라운드 비선형 방정식을 결합할 수 있다. 위의 조건에 맞게 구성된 평문 쌍 P, P^*는 확률 $\frac{1}{2}+2^{-19.7}$을 가지고 $h_0^{14}=h_0^{*14}$을 만족하기 때문에, 확률 $\frac{1}{2}+2^{-19.7}$을 가지고 다음 식이 성립함을 알 수 있다.

$$NF^{17}=NF^{*17} \tag{3}$$

따라서 확률 $\frac{1}{2}+2^{-19.7}$을 가지는 17-라운드 차분-비선형 특성을 구성할 수 있다.

다음 알고리즘1은 위의 17-라운드 차분-비선형 특성을 이용하여 512 비트 키를 사용하는 32-라운드 SHACAL-2의 공격과정을 설명한다.

알고리즘 1

1. 차분 $(0,0,e_{M_1},0,0,e_{31},e_{M_2},0)$을 가지고, 표 3의 조건을 만족하는 $2^{42.4}(=(2^3)\cdot(2^{-19.7})^{-2})$개의 평문 쌍을 선택한다. 각 평문 쌍에 대응하는 암호문 쌍을 요구한다.
2. 463 비트 키 $W^{31}, W^{30}, \cdots, W^{20}, w_0^{19}, w_1^{19}, \cdots, w_{25}^{19}, w_0^{18}, w_1^{18}, \cdots, w_{25}^{18}, w_0^{17}, w_1^{17}, \cdots, w_{24}^{17}, w_0^{16}, w_0^{15}$의 값을 추측한다. 32-라운드 SHACAL-2의 암호문 쌍을 가지고 ΔNF^{17}의 값을 얻기 위해서는 463 비트 키의 값의 추측을 요구한다. 더욱 자세한 사항은 [5]을 참조하라.
3. 각각의 암호문 쌍과 추측한 키를 사용하여 부분 복호화를 수행하고 식 (3)의 성립 여부를 테스트 한다. 식 (3)를 만족하는 평문 쌍의 수가 $2^{41.4}+2^{22}$와 같거나 크다면, 추측한 키를 저장한다. 만약 그렇지 않다면 단계 2로 돌아간다.
4. 단계 3을 통과한 키에 대해서, 나머지 49 비트에 대한 전수 조사를 수행한다. 만약 추측된 512 비트 키가 옳은 키라면 32-라운드 SAHCAL-2의 마스터 키로 출력하고, 그렇지 않다면, 단계 2로 돌아간다.

알고리즘1의 데이터 복잡도는 2^{43}선택 평문을 요구하며, 공격에 사용되는 메모리는 암호문 쌍의 저장 공간에 의존하므로 약 $2^{48.4}(=2^{43.4}\cdot 32)$ 바이트를 요구한다.

또한 알고리즘1의 계산 복잡도는 다음과 같이 평가할 수 있다. 단계 1의 계산 복잡도는 $2^{43.4}$ 32-라운드 SHACAL-2 암호화 과정을 요구하며 (데이터 수집 단계), 단계 3의 계산 복잡도는 평균 $2^{504.2}(=\frac{1}{2}\cdot\frac{15}{32}\cdot 2^{43.4}\cdot 2^{463})$ 32-라운드 SHACAL -2 암호화 과정을 요구한다. $\frac{1}{2}$은 단계 3에서 수행하는 462 비트 키의 평균 조사 비율을 의미한다. 단계 3을 통과하는 462 비트 키의 수를 평가하기 위하여 다음과 같은 통계적인 방법을 사용한다. 올바르지 않은 키에 대해서는 NF^{17}의 값은 랜덤하게 분포한다. 이는 $NF^{17}=NF^{*17}$을 만족하는 암호문 쌍의 수가 이항분포 $X\sim Bin(2^{42.4},\frac{1}{2})$를 따른다는 것을 의미한다. 이항분포는 쉽게 정규 분포로 근사할 수 있다. 즉, $X\sim N(\mu,\sigma^2)$. 단, $\mu=2^{41.4}$, $\sigma^2=2^{40.4}$. 따라서 $Z(=\frac{X-\mu}{\sigma})\sim N(0,1)$이고, $Pr[X\geq 2^{41.4}+2^{22}]=Pr[Z\geq 3.5813]\approx 2^{-12.7}$을 확인할 수 있다. 단계 3을 통과하는 올바르지 않은 463 비트 키의 기대값은 평균 $2^{449.7}(=\frac{1}{2}\cdot 2^{463}\cdot 2^{-12.7})$이므로, 단계 4의 계산 복잡도는 약 $2^{498.7}(=2^{449.7}\cdot 2^{49})$이다. 따라서 위 공격의 전체 계산 복잡도는 약 $2^{504.2}$ 32-라운드 SHACAL-2 암호화 과정을 요구한다.

위의 분석 과정에 따르면 이항분포 $X\sim Bin(2^{42.4},\frac{1}{2}+2^{-19.7})$을 갖는 옳은 키에 대해서 단계 3을 통과할 확률은 약 98%임을 확인할 수 있다. 따라서 위 공격의 성공 확률은 약 98%이다.

또한 알고리즘1은 [8]에 제시된 키 랭킹 과정으로 바꾸어 생각할 수 있다. 즉, 단계 3에서 $2^{41.4}+2^{22}$보다 크거나 같은 값을 갖는 키를 저장하는 대신에 $(2^{462}-2^{450.3})$개 키의 카운터 값 보다 큰 $2^{450.3}(=2^{463}\cdot 2^{-12.7})$개의 키를 저장할 수 있다. [8]에 제시된 order statistic을 사용하면 키 랭킹 과정을 이용한 공격의 성공 확률이 앞서 제시한 공격의 성공 확률과 같음을 확인할 수 있다. 하지만 키 랭킹 과정은 모든 가능한 2^{463}개의 키를 저장하기 위한 거대한 메모리를 요구한다.

4.2 포화-비선형 특성을 이용한 28-라운드 SHACAL-2 공격

본 문단에서는 13-라운드 포화-비선형 특성을 묘사하고, 이를 이용하여 28-라운드 SHACAL-2의 안전성을 분석한다.

전 절에서는 14-라운드 부정 차분 특성과 3-라운드 비선형 특성을 연결한 17-라운드 차분-비선형 특성을 이용한 공격을 소개하였다. 이와 유사하게 본 절에서는 10-라운드 포화 특성과 앞서 묘사한 3-라운드 비선형 특성을 연결한 13-라운드 포화-비선형 특성을 소개한다. 10-라운드 포화 특성은 다음과 같이 잘 선택된 평문 집합을 통하여 구성할 수 있다. 만약 2^{32}개로 구성된 평문 집합 $P_i \in (\mathbf{0},\mathbf{0},PS,CS,\mathbf{1},CS,-PS,CS)$ $i=0,\ldots,2^{32}-1$를 선택한다면(단, $\mathbf{0}$과 $\mathbf{1}$은 각각 32 비트 워드 00000000_x와 $ffffffff_x$를 나타낸다), 10 라운드 후에 여덟 번째 워드의 최하위 비트는 균일 성질을 만족한다. 즉, $\oplus_{i=0}^{2^{32}-1} h_{i,0}^{10}=0$. 표 6은 확률 1을 만족하는 포화 특성을 자세하게 설명한다. 앞서 설명하였다시피 10-라운드 포화 특성에 3-라운드 비선형 특성을 결합한다. 따라서 13-라운드 포화-비선형 특성은 확률 1로 다음과 같은 식이 성립한다.

$$\bigoplus_{i=0}^{2^{32}-1} NF_i^{13}=0 \tag{9}$$

다음 알고리즘2는 위의 14-라운드 포화-비선형 특성을 이용하여 512 비트 키를 사용하는 32-라운드 SHACAL-2의 공격과정을 설명한다.

알고리즘2

1. $(\mathbf{0},\mathbf{0},PS,CS,\mathbf{1},CS,-PS,CS)$ 형태를 갖는 463개의 집합을 선택한다. 각 평문 집합에 대응하는 암호문 집합을 요구한다.
2. 463 비트 키 $W^{27},W^{26},\cdots,W^{16},w_0^{15},w_1^{15},\cdots,w_{25}^{15}$, $w_0^{14},w_1^{14},\cdots,w_{25}^{14},w_0^{13},w_1^{13},\cdots,w_{24}^{13},w_0^{12},w_0^{11}$의 값을 추측한다.
3. 각각의 암호문 집합에 대해서 추측한 키를 사용하여 부분 복호화를 수행하고 식 (4)의 성립 여부를 테스트 한다. 식 (4)을 만족하지 않는다면, 2 단계로 돌아간다. 만약 그렇지 않다면 추측한 키를 저장한다.
4. 단계 3을 통과한 키에 대해서, 나머지 49 비트에 대한 전수 조사를 수행한다. 만약 추측된 512 비트 키가 옳은 키라면 28-라운드 SHACAL-2의 마스터 키로 출력하고, 그렇지 않다면, 단계 2로 돌아간다.

알고리즘2의 데이터 복잡도는 $463\cdot 2^{32}$선택 평문을 요구하며, 공격에 사용되는 메모리는 $2^{45.9}$ $(=463\cdot 2^{32}\cdot 2^5)$바이트를 요구한다.

또한 알고리즘2의 계산 복잡도는 다음과 같이 평가할 수 있다. 단계 1의 계산 복잡도는 $463\cdot 2^{32}$ 28-라운드 SHACAL-2 암호화 과정을 요구하며(데이터 수집 단계), 단계 3의 계산 복잡도는 평균 $2^{494.1}(=\frac{1}{2}\cdot\frac{15}{28}\cdot(2^{463}\cdot 2^{32}+2^{462}\cdot 2^{32}+\cdots+2^{1}\cdot 2^{32}))$ 28-라운드 SHACAL-2 암호화 과정을 요구한다. 단계 3을 통과하는 키 개수의 기대값은 약 1 $(=2^{463}\cdot 2^{-463})$이므로, 단계 4의 계산 복잡도는 약 2^{49} 28-라운드 SHACAL-2 암호화 과정을 요구한다. 따라서 위 공격의 전체 계산 복잡도는 약 $2^{494.1}$ 28-라운드 SHACAL-2 암호화 과정을 요구한다.

V. 결 론

본 논문은 SHACAL-2의 차분-선형 공격을 다양한 경우로 확장한 차분-선형 유형 공격에 대해 소개하였다. 차분-비선형 특성을 이용하여 $2^{43.4}$ 선택 평문의 데이터 복잡도와 $2^{504.2}$의 계산 복잡도를 가지고 32-라운드 SHACAL-2를 공격하였다. 이는

SHACAL-2에 대한 가장 효과적인 분석 결과이다. 또한 본 논문에서는 포화-비선형 특성을 사용하여 $463 \cdot 2^{32}$ 선택 평문의 데이터 복잡도와 $2^{494.1}$의 계산 복잡도를 가지고 수행할 수 있는 28-라운드 SHACAL-2의 공격을 소개하였다.

본 논문은 기존의 차분-선형 공격을 응용하여 차분 특성 대신 포화 특성, 선형 특성 대신 비선형 특성을 사용함으로써 분석 방법의 다양화를 꾀하였다. 비록 본 논문에서는 다루고 있지 않지만 이밖에 다양한 결합방식의 블록 암호 분석 방법이 존재하며, 이에 대한 연구는 블록 암호의 심도 있는 안전성 평가에 중요한 기여를 할 것이다.

참 고 문 헌

[1] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round DES," Advances in Cryptology - *CRYPTO'92*, LNCS 740, pp. 487-496, Springer-Verlag, 1992.

[2] E. Biham, O. Dunkelman and N. Keller, "Enhanced Differential-Linear Cryptanalysis," Advances in Cryptology - *ASIACRYPT'02*, LNCS 2501, pp. 254-266, Springer-Verlag, 2002.

[3] J. Daeman L. R. Knudsen and V. Rijndael, "The block cipher Square," *FSE'97*, LNCS 1267, pp. 149-165, Springer-Verlag, 1997.

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

[5] 홍석희, 김종성, 김구일, 이창훈, 성재철, 이상진, "30 라운드 SHACAL-2의 불능 차분 공격," 정보보호학회논문지, 14(3), pp. 107-115, June, 2004.

[6] S. K. Langford and M. E. Hellman, "Differential-Linear Cryptanalysis," Advances in Cryptology - *CRYPTO'94*, LNCS 839, pp. 17-25, Springer-Verlag, 1994.

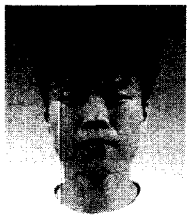
[7] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology - *EUROCRYPT'93*, LNCS 765, pp. 386-397, Springer-Verlag, 1994.

[8] A. A. Selcuk and A. Bicak, "On Probability of Success in Linear and Differential Cryptanalysis," *SCN'02*, LNCS 2576, pp. 174-185, Springer-Verlag, 2002.

[9] 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〉

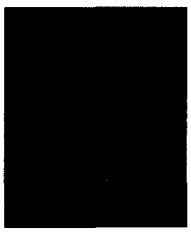
김 구 일 (Gu-il Kim)
2002년 2월 : 고려대학교 수학과 학사
2004년 8월 : 고려대학교 정보보호대학원 석사
2004년 8월~현재 : 고려대학교 정보보호기술연구센터 연구원
〈관심분야〉 블록 암호 및 스트림 암호의 분석과 설계



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

홍 석 희 (Seok-hie Hong) 정회원
1995년 2월 : 고려대학교 수학과 학사
1997년 2월 : 고려대학교 수학과 석사
2001년 2월 : 고려대학교 수학과 박사
2004년 4월~2005년 2월 : 벨기에 COSIC 연구원
2005년 3월~현재 : 고려대학교 정보보호대학원 조교수
〈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



임 종 인 (Jongin Lim) 정회원
1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1999년 2월~현재 : 고려대학교 정보보호대학원 원장, CIST 센터장
〈관심분야〉 암호 이론, 정보보호정책