通信情報保護學會論文誌
第 9 券 第 3 號, 1999. 09

2-블록 구조 블록 암호에 대한 고차 차분 공격

강주성*, 박상우*, 이상진**

Higher order DC for block ciphers with 2-block structure

Ju-Sung Kang*, Sangwoo Park*, Sangjin Lee**

요 약

DC 및 LC에 대하여 증명 가능한 안전성을 제공하는 2-블록 구조를 라운드 함수의 위치에 따라서 C(Center)-형, R(Right)-형, L(Left)-형으로 구분하고, 각각에 대한 고차 차분 공격 측면의 안전성을 분석한다. 4 라운드 암호화 함수인 경우 세가지 2-블록 구조는 고차 차분 공격에 대하여 동일한 안전성을 제공한다는 사실을 증명하며, 5 라운드 이상의 암호화 함수에 대해서는 병렬 연산이 가능한 R-형 구조가 C-형과 L-형에 비해서 계산 효율성은 높지만 고차 차분 공격 측면의 안전성은 떨어진다는 사실을 밝힌다.

ABSTRACT

We study on the security for the block ciphers with 2-block structure which have provable security against DC and LC on the view point of higher order DC. 2-block structures are classified three types according to the location of round function such as C(Center)-type, R(Right)-type, and L(Left)-type. We prove that in the case of 4 rounds encryption function, these three types provide the equal strength against higher order DC and that in the case of 5 or more rounds, R-type is weaker than C-type and L-type.

I. 서 론

Biham과 Shamir[2,3]에 의해서 1990년에 차분 공격(differential cryptanalysis, DC)이 발표되고,1993년도에 Matsui[9]에 의한 선형 공격(linear cryptanalysis, LC)이 알려진 이래 DC와 LC는 블록 암호(block

* 한국전자통신연구원, ** 고려대학교 자연과학대학

cipher)에 대한 여러 공격들 중에서 가장 강력한 공격으로 자리 매김 하였다. 이에 따라 블록 암호 설계시 DC와 LC 측면의 안전성을 고려하는 것은 필수적인 사항이 되었다.

블록 암호의 DC와 LC에 대한 안전성 강도를 측정하는 방법은 관점에 따라서 몇 가지가 알려져 있는데 이론적으로 가장 완성된 개념은 증명 가능한 안전성(provable security) 측면의 분석으로 보인다. DC 및 LC에 대한 증명 가능 안전성 개념은 최대 차분(differen-tial)과 선형(linear) 확률의 평균에 대한 상한(upper bound) 값을 이론적으로 이끌어 내는 분석 방법으로 Nyberg와 Knudsen [14], Matsui[10], Kaneko 등[5]에 의해서 연구되었다. 이들이 연구한 블록 암호의 구조는 주로 라운드별 입력이 같은 크기의 블록 두개로 나뉘어서 입력되는 "2-블록 구조"이다. DC와 LC에 대해서 증명 가능한 안전성을 제공하는 2-블록 구조 블록 암호는 라운드 함수가 놓인 위치에 따라서 세가지로 대별할 수 있다. 본 논문에서는 이 세 가지 구조 각각에 대해서 고차 차분 공격(higher order DC) 관점의 안전성을 분석하고자 한다.

고차 차분 공격법은 Lai[7]에 의해서 제안된 블록 암호의 분석 기법으로 차분(differen-tial)의 차수를 높여서 특성을 조사하는 선택평문 공격의 일종이다. 직관적으로 고차 차분 공격법은 DC를 일반화한 분석법으로 볼 수 있으며, 적은 라운드 수를 갖는 블록 암호 공격에 효과적인 것으로 알려져 있다. 이 공격법은 벡터 부울 함수의 대수적 차수(algebraic deg-ree)와 밀접한 관계가 있어서 일반적으로 암호 함수의 대수적 차수가 높을 때 고차 차분 공격에 대한 내성이 우수하다.

고차 차분 공격을 실제로 블록 알고리즘 공격에 적용한 예는 Knudsen[6]이 처음으로, 특정한 라운드 함수를 갖는 5 라운드 Feistel 구조에 대한 고차 차분 공격을 실시하는 방법을 보여 주었다. Jakobsen과 Knudsen[4]은 DC에 대하여 증명 가능한 안전성을 제공하는 원형(prototype)으로 Nyberg와 Knud-sen[14]이 제안한 *KN* 암호에 대한 고차 차분 공격을 실시하였다. 그 결과 Feistel 구조 6 라운드로 구성된 *KN* 암호에 대한 고차 차분 공격의 공격 복잡도는 DC 및 LC의 공격 복잡도 보다 상당히 낮다는 사실을 밝혔으며, Shimoyama 등[15]은 올바른 키를 찾아내는 판별식을 개선함으로써 Jakobsen과 Knud-sen 공격의 공격 복잡도를 낮추었다. 한편, Nyberg와 Knudsen[14]이 제안한 DC 및 LC에 대하여 증명 가능한 안전성 개념을 바탕으로 Matsui[10]는 Feistel 구조와 다른 새로운 구조를 제안하였으며, 이 구조를 기본으로 하여 블록 암호 MISTY[11]를 설계하였다. MISTY에 대한 고차 차분 공격은 Sugita [16]에 의해서 발표되었는데 그는 이 공격에 의해서 MISTY가 더이상 암호로서 안전하지 않음을 주장하였다.

본 논문에서는 DC 및 LC에 대하여 증명 가능한 안전성을 제공하는 세가지 서로 다른 2-블록 구조에 대한 고차 차분 공격 관점의 라운드별 안전성을 비교 분석한다. 3 라운드 이후에 DC 및 LC에 대한 증명 가능 안전성을 제공하는 세가지 2-블록 구조가 4 라운드 이후에는 고차 차분 공격 관점의 안전성 강도가 동일하다는 사실을 밝힌다. 그리고 5 라운드 이후에 라운드 수 증가에 따른 고차 차분 공격 관점의 안전성을 일반적으로 평가할 수 있는 관계식을 이끌어내어 세가지 2-블록 구조를 비교 가능하게 한다. 세가지 구조 중에서 두가지는 이미 고차 차분 공격에 관한 연구가 발표된 것들로 각각 Feistel과 Matsui가 제안한 구조이다. 나머지 하나는 Skipjack[12]에 원용된 구조로 이에 대한 고차 차분 공격 관점의 안전성 분석은 아직까지 발표되지 않고 있다. 그러므로 이 구조에 대한 본 논문의 결과는 새로운 것으로 볼 수 있다.

본 논문은 서론을 포함하여 총 5개의 절로 구성된다. 2절에서는 DC 및 LC에 대하여 증명 가능한 2-블록 구조를 설명하고, 3절에서는 부울 함수의 대수적 차수와 고차 차분 공격을 기술한다. 4절에서는 세가지 2-블록 구조에 대한 고차 차분 공격 관점의 안전성을 진단하고 비교 분석하며, 5절은 결론부이다.

II. DC 및 LC에 대하여 증명 가능한 2-블록 구조

입력과 출력의 크기가 각각 n 비트인 암호 함수를 F라 하자. 즉, $F: Z_2^n \rightarrow Z_2^n$으로 표현할 수 있으며, F는 블록 암호 알고리즘의 라운드 함수로 작용한다고 하자. 임의의 $\Delta x, \Delta y, a, b \in Z_2^n$에 대하여, F의 차분(differential) 확률과 선형(linear) 확률은 각각

$$DP^F(\Delta x \rightarrow \Delta y) = \frac{\#\{x \in Z_2^n : F(x) \oplus F(x \oplus \Delta x) = \Delta y\}}{2^n}$$

와

$$LP^F(a \rightarrow b) = \left(\frac{\#\{x \in Z_2^n : \langle a, x\rangle = \langle b, F(x)\rangle\}}{2^{n-1}} - 1\right)^2$$

으로 정의된다. 여기에서 $\langle \alpha, \beta\rangle$는 벡터 α와 β를 비트별 AND한 후 각각을 비트별 EXOR함으로써 구해지는 값이다. DC와 LC에 강한 함수 F는 임의의 $\Delta x \neq 0$와 $b \neq 0$에 대해서 DP^F와 LP^F 값이 각각 작아야 하므로 DC와 LC에 대한 함수 F의 내성(immunity)을 측정하는 도구로서

$$DP^F_{\max} = \max_{\Delta x \neq 0, \Delta y} DP^F(\Delta x \rightarrow \Delta y)$$

와

$$LP^F_{\max} = \max_{a, b \neq 0} LP^F(a \rightarrow b)$$

가 사용된다.

이제 E를 2-블록 구조의 암호화 함수, 즉, 입출력 크기가 $2n$ 비트인 키 종속 암호화 함수라 하고, K는 가능한 모든 키들의 집합이라 하자. 임의의 고정된 $k \in K$에 대하여 $E^{(k)}$를 Z_2^{2n}에서 Z_2^{2n}으로 가는 $2n$ 변수 함수라 놓으면, $DP^{E^{(k)}}(\Delta x \rightarrow \Delta y)$와 $LP^{E^{(k)}}(a \rightarrow b)$는 $DP^F(\Delta x \rightarrow \Delta y)$ 및 $LP^F(a \rightarrow b)$와 같이 정의된다. 단지 여기에서는 $\Delta x, \Delta y, a, b$가 모두 Z_2^{2n} 안의 원소라는 사실만 함수 F에 대한 정의에서와 다를 뿐이다. 암호화 함수 E에 대한 차분 확률과 선형 확률은 키 값에 따른 $DP^{E^{(k)}}$와 $LP^{E^{(k)}}$들의 평균(average)으로 정의된다. 즉,

$$DP^E(\Delta x \rightarrow \Delta y) = \frac{1}{\#K} \sum_{k \in K} DP^{E^{(k)}}(\Delta x \rightarrow \Delta y)$$

이고,

$$LP^E(a \rightarrow b) = \frac{1}{\#K} \sum_{k \in K} LP^{E^{(k)}}(a \rightarrow b)$$

이다. DP^E와 LP^E가 $\Delta x \neq 0$과 $b \neq 0$인 모든 $\Delta x, \Delta y, a, b \in Z_2^{2n}$에 대하여 충분히 작은 값일 때, 우리는 E가 DC와 LC에 대하여 증명 가능한 구조를 갖는다고 말한다. 달리 표현하면, E가 DC와 LC에 대하여 증명 가능한 구조라는 뜻은

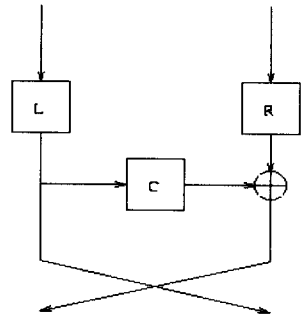
$$DP^E{}_{\max} = \max_{\Delta x \neq 0, \Delta y} DP^E(\Delta x \rightarrow \Delta y)$$

와

$$LP^E{}_{\max} = \max_{a, b \neq 0} LP^E(a \rightarrow b)$$

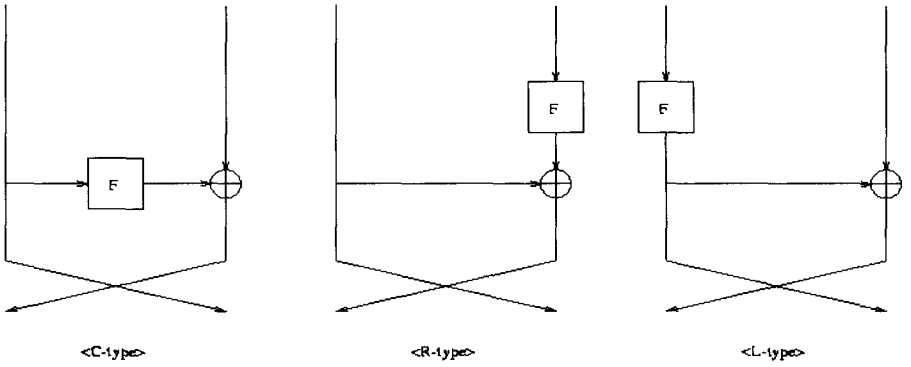
가 충분히 작은 값을 갖는다는 것을 의미한다.

DC와 LC에 대하여 증명 가능한 안전성을 제공하는 2-블록 구조 블록 암호는 라운드 함수 F의 위치에 따라서 세가지로 대별할 수 있다. 그림 1에는 라운드 함수 F가 놓일 수 있는 위치가 표현되어 있다.



(그림 1) 2-블록 구조에서 라운드 함수의 위치

편의상 본 논문에서는 왼편에만 라운드 함수



(그림 2) 세가지 2-블록 구조

가 위치한 구조를 L-형(Left-type), 가운데만 위치한 구조를 C-형(Center-type), 그리고 오른편에만 위치한 구조를 R-형(Right-type)으로 각각 부르기로 한다. L-형 구조인 경우 C와 R에 위치한 라운드 함수를, C-형 구조인 경우 L과 R에 위치한 라운드 함수를, 그리고 R-형인 경우 L과 C에 놓인 라운드 함수를 각각 항등 함수로 간주하는 것이다(그림 2).

C-형 구조는 Feistel 구조로 널리 알려진 것으로서 DES 알고리즘의 기본 구조로 사용되었다. $DP^F_{\max} \le p$ 이고 $LP^F_{\max} \le q$ 인 경우 Nyberg와 Knudsen[14]은 라운드 수가 4 이상인 C-형 구조의 $DP^E_{\max}$ 상한은 $2p^2$, $LP^E_{\max}$ 상한은 $2q^2$임을 보였으며, F 함수가 전단사일 때는 3 라운드 이상이면 이 상한들을 갖는다는 사실을 증명하였다. 그리고 Aoki와 Ohta[1]는 F가 전단사 함수일 때, 라운드 수가 3 이상이면 $DP^E_{\max}$와 $LP^E_{\max}$의 상한이 각각 p^2과 q^2임을 증명하여 Nyberg와 Knudsen의 결과를 개선하였다.

Matsui[10]는 병렬 연산이 가능하고 DC와 LC에 대하여 증명 가능한 안전성을 제공하는 블록 암호 알고리즘의 구조를 제안하였으며, 이 구조를 기본으로 하여 MISTY[11]라는 블록 암호 알고리즘을 설계하였다. Matsui가 제안한 구조는 R-형 구조이며, Feistel 구조와는 다르게 복호화 과정을 위해서는 라운드 함수 F가 반드시 전단사 함수라야 한다. 라운드 함수가 모두 전단사 함수라는 조건 하에서 Matsui는 R-형 구조가 3 라운드 이상일 때, $DP^E_{\max}$와 $LP^E_{\max}$의 상한이 각각 p^2과 q^2이 되어 Feistel 구조와 같은 증명 가능한 안전성을 소유하고 있음을 밝혔다[10].

한편, L-형 구조는 C-형과 R-형 구조와는 달리 이를 기본 구조로 하여 설계된 블록 암호는 아직까지 발표되지 않고 있다. 다만 F 함수의 출력이 다른 블록의 입력과 EXOR되는 논리가 Skipjack[12]에 사용되었다. Skipjack은 4-블록 구조이므로 증명 가능한 안전성 측면에서 2-블록 구조에 대한 안전성 분석과는 다르지만 기본적인 논리는 L-형 구조와 차이가 없을 것이라 예상된다. 이 L-형 구조의 증명 가능한 안전성 역시 C-형과 R-형 구조와 같다는 사실이 알려져 있다. Kaneko 등[5]은 L-형의 DC는 R-형의 LC에, L-형의 LC는 R-형의 DC에 각각 대응된다는 쌍대성(duality)을 이용하여 증명 가능한 안전성 측면에서 L-형과 R-형이 동등한 안전성을 갖고 있음을 증명하였다.

본 논문에서는 위에서 언급한 증명 가능한 안전성을 제공하는 세가지 2-블록 구조에 대한 고차 차분 공격(higher order DC) 관점의 안전성을 분석하고자 한다. 지금부터는 편의상 R-형과 L-형의 라운드 함수는 모두 전단사 함수라 가정한다.

III. 대수적 차수와 고차 차분 공격

$x=(x_1, \ldots, x_n) \in Z_2^n$을 임의의 n 차원 이진

벡터라 하고, $f(x)$를 x의 성분들의 부울 함수라 하자. 그러면 다음과 같이 $f(x)$를 대수적 정규 표현(algebraic normal form)으로 나타낼 수 있다. 즉,

$$\begin{aligned} f(x) = {} & a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n \\ & \oplus a_{12}x_1x_2 \oplus \cdots \oplus a_{n-1,n}x_{n-1}x_n \\ & \vdots \\ & \oplus a_{12\cdots n}x_1x_2\cdots x_n \ . \end{aligned}$$

대수적 정규 표현에서 거듭 제곱 항이 없는 이유는 0 또는 1의 모든 거듭 제곱은 항상 0 또는 1이기 때문이다. i개 변수의 곱을 i차 곱이라 하고, 함수 f의 대수적 차수(algebraic degree)는 최고차의 곱으로 정의된다. 예를 들면, $x=(x_1,x_2,x_3,x_4,x_5)$이고,

$$f(x)=1+x_5+x_1x_3+x_2x_4x_5$$

라 할 때, 함수 f의 대수적 차수는 3이 된다. 함수 f의 대수적 차수를 간단히 $\deg(f)$로 나타내기로 한다.

함수 f가 $f: Z_2^n \to Z_2^m$인 벡터 부울 함수일 때는 각 성분 함수의 대수적 차수 중 최대값을 함수 f의 대수적 차수로 정의한다. 즉, $f=(f_1,\cdots,f_m)$일 때,

$$\deg(f)=\max_{1\le i\le m}\deg(f_i)$$

이다.

한편, Lai[7]는 고차 도함수(higher order derivative)를 다음 정의와 같이 소개하였다.

정의 1. *$f: Z_2^n \to Z_2^m$을 임의의 벡터 부울 함수라 하자. 그러면 함수 f의 점 $a \in Z_2^n$에서의 도함수(derivative)는*

$$\Delta_a f(x)=f(x \oplus a) \oplus f(x)$$

로 정의되고, 점 $a_1,\cdots,a_i \in Z_2^n$에서 함수 f의 i차 도함수(i-th derivative)는

$$\Delta^{(i)}_{a_1,\cdots,a_i} f(x)=\Delta_{a_i}\left(\Delta^{(i-1)}_{a_1,\cdots,a_{i-1}} f(x)\right)$$

로 정의된다. 여기에서 임의의 $a, b \in Z_2^n$에 대하여, $a \oplus b$는 비트별 EXOR을 의미한다.

DC를 실시할 때, 특성(characteristic)과 이 특성들의 집합으로 볼 수 있는 차분(differ-ential)이란 개념이 이용되었다. 이와 비슷하게 고차 도함수(higher order derivative)로부터 고차 차분(higher order differential)을 정의 할 수 있다.

정의 2. *$f: Z_2^n \to Z_2^m$을 임의의 벡터 부울 함수라 하자. 그러면 함수 f의 i차 차분(i-th order differential)은*

$$\Delta^{(i)}_{a_1,\cdots,a_i} f(x)=b, \quad x \in Z_2^n$$

을 만족하는 $(i+1)$-순서쌍 $(a_1,\cdots,a_i,b) \in (Z_2^n)^i \times Z_2^m$으로 정의된다.

Lai[7]는 고차 도함수에 대하여 여러가지 성질을 증명하였는데 여기에서는 논리 전개에 필요한 부분만을 기술하기로 한다.

정리 1(Lai[7]). *함수 f의 대수적 차수와 $\Delta_a f$의 대수적 차수 사이에는 다음과 같은 관계가 성립한다.*

$$\deg(\Delta_a f(x)) \le \deg(f(x))-1.$$

정리 2(Lai[7]). *$L[a_1,\cdots,a_i]$를 벡터 $a_1, \cdots, a_i$들의 2^i개 일차 결합들 전체로 이루어진 공간이라 놓으면,*

$$\Delta^{(i)}_{a_1,\cdots,a_i} f(x)=\sum_{c \in L[a_1,\cdots,a_i]} f(x \oplus c)$$

가 된다.

정리 3(Lai[7]). *함수 $f: Z_2^n \to Z_2^m$과 Z_2^n*

상의 일차 독립인 벡터들 $a_1, \cdots, a_i$, 그리고 임의의 벡터 $b \in Z_2^n$에 대하여, x가 일양분포(uniform distribution)를 한다면, $P(\Delta^{(i)}_{a_1,\cdots,a_i} f(x) = b)$의 값은 0이거나 적어도 2^{i-n}이다.

정리 4(Lai[7]). *만일 a_i가 $a_1, \cdots, a_{i-1}$과 일차 종속인 벡터라면, $\Delta^{(i)}_{a_1,\cdots,a_i} f(x) = 0$이 된다.*

정리 5(Lai[7]). *임의의 벡터 부울 함수 $f: Z_2^n \to Z_2^m$에 대하여 함수 f의 n차 도함수는 상수이다. 만일 함수 f가 $f: Z_2^n \to Z_2^n$인 가역 함수(invertible function)라면, f의 $n-1$차 도함수는 상수이다.*

우리는 정리 4로부터 고차 도함수를 구하는 점들인 $a_1, \cdots, a_i$들은 반드시 일차 독립이어야 한다는 것을 알 수 있다. 그리고 정리 5의 내용은 함수 f의 대수적 차수는 정의역의 차원을 넘지 못한다는 사실과 가역 함수인 경우는 대수적 차수가 정의역의 차원에서 1을 뺀 것보다 크지 못하다는 사실을 상기하면 정리 1로부터 자연스럽게 유추할 수 있는 내용이다.

Lai가 제안한 고차 차분 공격을 실제로 블록 암호 공격에 가장 먼저 적용한 사람은 Knudsen[6]이다. 그는 특정한 라운드 함수를 갖는 5 라운드 Feistel 구조에 대한 고차 차분 공격을 실시하는 과정을 구체적으로 묘사하였다. 임의의 고정된 라운드 키에 대해서 $F: Z_2^{2n} \to Z_2^{2n}$을 1 라운드 암호화 함수라 하고, $F^{(j)}$를 함수 F의 j 라운드 반복 암호화 함수라 하자. 그리고 암호 알고리즘의 총 라운드 수는 r이며, $F^{(r-1)}$의 대수적 차수는 d라고 가정하자. 그러면 정리 1로부터 임의의 일차 독립인 벡터들 $a_1, \cdots, a_d, a_{d+1} \in Z_2^{2n}$에 대하여,

$$\Delta^{(d+1)}_{a_1,\cdots,a_d,a_{d+1}} F^{(r-1)}(x) = 0, \quad \forall x \in Z_2^{2n} \quad (1)$$

이 성립한다. 라운드 키를 n 비트라고 할 때, Knudsen은 식 (1)을 토대로 하여 2^{d+1}개의 평문과 암호문 쌍을 가지고 $2^{d+1} \cdot 2^n$의 계산량으로 고차 차분 공격이 가능함을 보인 것이다. 그런데 식 (1)은 다른 수식으로 표현 가능하다. 정리 1에 의하면 임의의 일차 독립인 벡터들 $a_1, \cdots, a_d \in Z_2^{2n}$과 적당한 상수 C에 대하여,

$$\Delta^{(d)}_{a_1,\cdots,a_d} F^{(r-1)}(x) = C \quad \forall x \in Z_2^{2n} \quad (2)$$

이 성립하는 것이다. Shimoyama 등[15]은 식 (2)가 평문 뿐만 아니라 라운드 키 값에 대해서 독립적으로 성립한다는 사실에 주목하여 라운드 키와 평문이 모두 0인 값을 사용하여 상수 C값을 결정하였다. 이를 이용하여 그들은 고차 차분 공격에 필요한 평문과 암호문 쌍의 개수를 2^d으로, 계산량을 $2^d \cdot 2^n$으로 각각 낮춤으로써 Knudsen의 결과를 개선하였다.

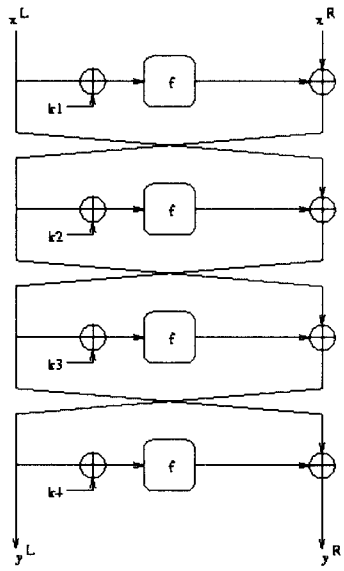
우리는 다음 절에서 Knudsen과 Shimoyama 등이 실시한 고차 차분 공격 방법을 근간으로 세가지 2-블록 구조인 C-형, R-형, L-형에 대한 공격 방식을 서술하고, 라운드별 안전성 강도를 비교 분석한다.

IV. 2-블록 구조의 고차 차분 공격에 대한 내성

세가지 2-블록 구조가 모두 3 라운드 이상일 때 DC 및 LC에 대하여 증명 가능한 안전성을 제공하고, 일반적으로 4 라운드 이상인 2-블록 구조에 대해서 고차 차분 공격이 의미를 갖기 때문에 먼저 각 구조들의 총 라운드 수는 4 라운드로 고정한다. 그리고 $x=(x^L, x^R)$이 평문 좌우측 블록일 때, 대응하는 암호문은

$$E(x) = y = (y^L, y^R) = (E^L(x), E^R(x))$$

로 표현하고, $x_i=(x_i^L, x_i^R)$은 i 라운드 후의 암호문 좌우측 블록을 나타낸다고 하며, 편의상 마지막 라운드에서의 swapping은 없다고 가정하자. 각 라운드에 작용하는 라운드 함수는 모두 $f: Z_2^n \to Z_2^n$이라 하고, R-형과 L-형에



(그림 3) C-형 구조 4 라운드

서는 f가 전단사 함수라 하자. f의 대수적 차수는 d라 하고, 일차 독립인 벡터들을 충분히 잡기 위한 조건으로 $d \le n$을 만족한다고 하며, k_i는 i번째 라운드 키로 n 비트라 하자. 그리고 라운드 키는 모두 각 라운드 함수 직전에서 EXOR된다고 가정하며,

$$f_{k_i}(x) = f(x \oplus k_i)$$

로 정의한다.

C-형 구조를 갖는 4 라운드 블록 암호는 그림 3에 나타나 있다. 그림 3으로부터 우리는

$$\begin{aligned} x_3^L &= x^R \oplus f_{k_1}(x^L) \oplus \\ &\quad f_{k_3}(x^L \oplus f_{k_2}(x^R \oplus f_{k_1}(x^L))), \\ x_3^R &= x^L \oplus f_{k_2}(x^R \oplus f_{k_1}(x^L)) \end{aligned} \quad (3)$$

임을 알 수 있다. x_3을 유추해내기 위해서 x_3^R만 알아내면 된다. $x_3^L = y^L$이므로 x_3^L은 쉽게 얻어낼 수 있기 때문이다. 식 (3)에서 보는 바와 같이 x_3^R은 k_1과 k_2에 의존하므로

$$x_3^R = T^C{}_{[k_1,k_2]}(x) = x^L \oplus f_{k_2}(x^R \oplus f_{k_1}(x^L))$$

이라 하자. 그러면 정리 1과 2로부터 Z_2^{2n} 상의 임의의 벡터 중에서 $a_j = (0, a_j^R) \in Z_2^n \times Z_2^n$, $\forall\ 1 \le j \le d$를 만족하는 d개의 일차 독립인 벡터들 $a_1, \cdots, a_d$와 적당한 상수 c에 대해서

$$\begin{aligned} &\Delta^{(d)}_{a_1,\cdots,a_d} T^C{}_{[k_1,k_2]}(x) \\ &= \sum_{v \in L[a_1,\cdots,a_i]} T^C{}_{[k_1,k_2]}(x \oplus v) \\ &= c \end{aligned} \quad (4)$$

가 임의의 $x \in Z_2^{2n}$과 임의의 키 값 k_1, k_2와는 독립적으로 성립한다. 그러므로 평문과 라운드 키 값이 모두 0인 경우를 고려하면

$$c = \sum_{v \in L[a_1,\cdots,a_i]} T^C{}_{[0,0]}(v) \quad (5)$$

임을 알 수 있다. 한편, C-형 구조에서는

$$x_3^R = f_{k_4}(y^L) \oplus y^R$$

이 성립하므로

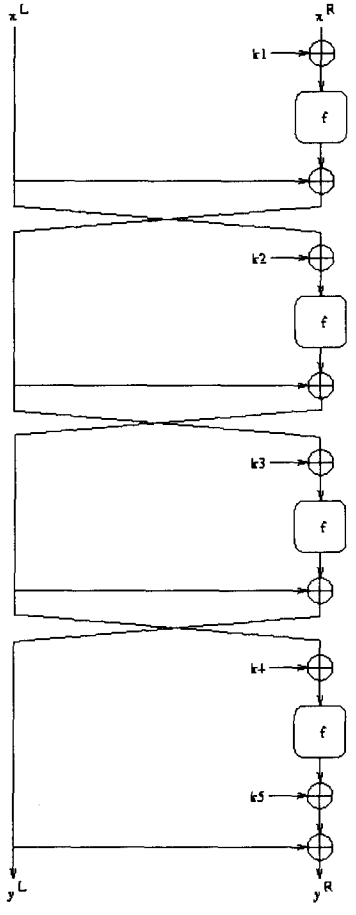
$$T^C{}_{[k_1,k_2]}(x) = f_{k_4}(E^L(x)) \oplus E^R(x) \quad (6)$$

로 쓸 수 있다. 결과적으로 식 (4), (5), (6)을 종합하면 마지막 라운드 키 k_4에 대한 판별식으로

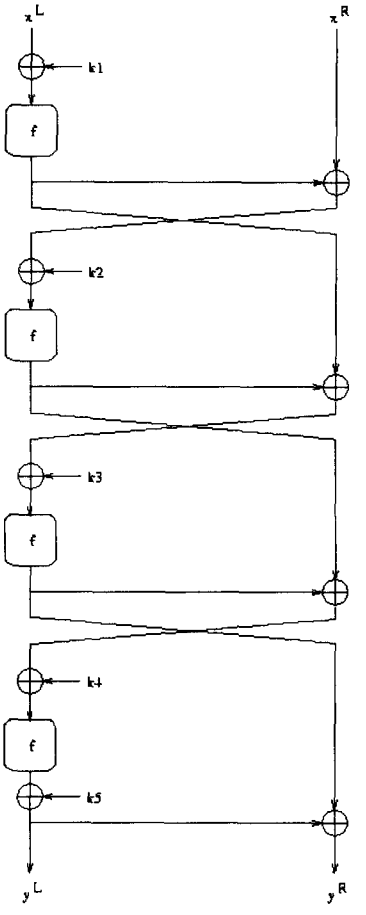
$$\begin{aligned} &\sum_{v \in L[a_1,\cdots,a_d]} f_{k_4}(E^L(v)) \oplus E^R(v) \\ &= \sum_{v \in L[a_1,\cdots,a_d]} T^C{}_{[0,0]}(v) \end{aligned} \quad (7)$$

을 얻을 수 있다. 마지막 라운드 키에 대한 판별식 (7)을 이용하여 k_4를 찾아내는 과정은 다음과 같다.

1. Z_2^{2n} 상에서
   $a_j = (0, a_j^R) \in Z_2^n \times Z_2^n$, $\forall 1 \le j \le d$
   를 만족하는 d개의 일차 독립인 벡터들 $a_1, \cdots, a_d$를 선택한다.
2. 마지막 라운드 키 k_4의 값을 가정한다.
3. $L[a_1, \cdots, a_d]$에 속하는 2^d개 벡터 v



(그림 4) R-형 구조 4 라운드



(그림 5) L-형 구조 4 라운드

각각에 대하여 다음을 계산한다.

- $E^L(v)$, $E^R(v)$를 얻는다.
- $T^C{}_{[0,0]}(v)$를 계산한다.
- $f_{k_4}(E^L(v))$를 계산한다.

4. 판별식 (7)이 성립하는지 판단한다.
5. 판별식이 성립하면 k_4를 올바른 키로 판정하고, 성립하지 않으면 두번째 단계로 돌아가서 과정을 반복한다.

우리는 위 과정을 수행하기 위해서 필요한 평문과 암호문 쌍의 개수는 2^d개 이고, 최대 $4 \cdot 2^d + 2^{d+n}$번의 라운드 함수 계산량이 필요하다는 사실을 얻을 수 있다. 그리고 마지막 라운드 키가 결정되면 유사한 공격을 반복함으로써 축차적으로 이전 라운드의 키를 결정할 수 있으므로 전체 라운드 키를 찾아낼 수 있다.

R-형과 L-형 구조는 각각 그림 4와 5에 표현되어 있다. 구조적 특성상 R-형과 L-형에서는 복호화 과정을 감안하여 라운드 함수 f가 가역(invertible)이어야 하며, 마지막 라운드의 함수 f가 암호적 의미를 갖기 위해서 라운드 함수 이후에 라운드 키를 한번 더 EXOR해 주는 단계가 필요하다. 마지막의 키 EXOR 단계가 추가되지 않는다면 암호문으로부터 키 요소의 가정 없이 단순히 f^{-1}을 계산함으로써 마지막 라운드 함수 직전의 입력을 얻을 수 있

으므로 공격 관점에서 마지막 라운드 함수의 암호적 의미가 사라지기 때문이다. 그리고 라운드 키를 마지막에 한번 더 EXOR해주는 단계는 계산 복잡도가 라운드 함수 계산에 비해서 상대적으로 매우 작은 정도이므로 별도의 라운드로 생각할 필요는 없다. 이러한 이유로 R-형과 L-형 구조에서는 마지막 라운드 함수 직후에 한 번의 라운드 키 EXOR 단계가 추가된 것으로 약속한다.

그림 4로부터 우리는 R-형 구조에 대해서

$$\begin{aligned} x_3^L &= x^L \oplus f_{k_1}(x^R) \oplus f_{k_2}(x^L) \\ &\quad \oplus f_{k_3}(x^L \oplus f_{k_1}(x^R)) \\ x_3^R &= x^L \oplus f_{k_1}(x^R) \oplus f_{k_2}(x^L) \end{aligned} \tag{8}$$

이라는 관계식을 얻을 수 있다. 4 라운드 f 함수의 입력을 $\widehat{x_3^R} = x_3^R \oplus k_4$라 하면, 식 (8)로부터

$$\begin{aligned} \widehat{x_3^R} &= T^R{}_{[k_1,k_2,k_4]}(x) \\ &= x^L \oplus f_{k_1}(x^R) \oplus f_{k_2}(x^L) \oplus k_4 \end{aligned}$$

로 표현됨을 알 수 있다. R-형 구조 마지막 라운드를 보면 $\widehat{x_3^R} = f_{k_5}^{-1}(y^L \oplus y^R)$가 성립되므로 C-형 구조에서와 비슷하게 마지막 라운드 키 k_5에 대한 판별식

$$\sum_{v \in L[a_1,\cdots,a_d]} f^{-1}{}_{k_5}(E^L(v) \oplus E^R(v)) = \sum_{v \in L[a_1,\cdots,a_d]} T^R{}_{[0,0,0]}(v) \tag{9}$$

를 얻을 수 있다. 그러므로 4 라운드 R-형 구조에 대한 고차 차분 공격에 필요한 평문과 암호문 쌍의 개수와 계산량은 C-형 구조와 같다는 사실을 알 수 있다.

L-형 구조 4 라운드 암호를 표현한 그림 5로부터 우리는

$$\begin{aligned} x_3^L &= f_{k_2}(x^R \oplus f_{k_1}(x^L)) \oplus f_{k_3}(f_1(x^L) \\ &\quad \oplus f_{k_2}(x^R \oplus f_{k_1}(x^L))) , \\ x_3^R &= f_{k_3}(f_{k_1}(x^L) \\ &\quad \oplus f_{k_2}(x^R \oplus f_{k_1}(x^L))) \end{aligned} \tag{10}$$

임을 알 수 있다. 여기에서 x_3의 올바른 값을 얻어내기 위해서는 x_3^L을 유추해내야만 한다. $x_3^R = y^L \oplus y^R$에 의해서 x_3^R은 쉽게 계산해낼 수 있기 때문이다. 언뜻 보면 식 (10)으로부터 우리는 일차 독립인 벡터들 $a_1, \cdots, a_d \in Z_2^{2n}$을 아무리 잘 선택한다 할지라도 x_3을 표현하는 함수의 대수적 차수는 적어도 d^2이 된다고 생각하기 쉽다. 그런데 이 L-형 구조의 특성상 (x_3^L, x_3^R)을 알 수 있다면, $x_2^R = x_3^L \oplus x_3^R$이므로 x_2^R까지 얻을 수 있다. 공격자는 대수적 방정식이 복잡한 x_3^L 보다는 x_2^R에 대한 대수적 방정식을 이용함으로써 공격 복잡도를 낮출 수 있다.

$$x_2^R = f_{k_2}(x^R \oplus f_{k_1}(x^L)) \tag{11}$$

이 성립하므로 공격자는 식 (10)을 이용하는 것이 아니라 식 (11)을 이용하여 공격에 필요한 평문과 암호문 쌍의 개수를 줄일 수 있는 것이다. R-형에서와 비슷하게 $\widehat{x_3^L} = x_3^L \oplus k_4$라 하고, $\widehat{x_2^R} = \widehat{x_3^L} \oplus x_3^R$이라 하며,

$$\begin{aligned} \widehat{x_2^R} &= T^L{}_{[k_1,k_2,k_4]}(x) \\ &= f_{k_2}(x^R \oplus f_{k_1}(x^L)) \oplus k_4 \end{aligned}$$

로 놓자. 그러면

$$\widehat{x_2^R} = f^{-1}{}_{k_5}(y^L) \oplus y^L \oplus y^R$$

이므로 $a_1, \cdots, a_d$가 일차 독립이고 각각의 좌측 블록 $a_j^L = 0$인 d개의 벡터들을 선택하므로써 식 (7), (9)와 유사한 판별식

$$\sum_{v \in L[a_1,\cdots,a_d]} f_{k_5}^{-1}(E^L(v)) \oplus E^L(v) \oplus E^R(v) = \sum_{v \in L[a_1,\cdots,a_d]} T^L{}_{[0,0,0]}(v)$$

를 얻을 수 있다. 이로부터 4 라운드 L-형 구조의 고차 차분 공격에 필요한 평문과 암호문 쌍의 개수 및 계산량은 C-형 및 R-형과 같다는 사실을 알 수 있다.

지금까지 분석한 DC 및 LC에 대하여 증명 가능한 2-블록 구조 4 라운드의 고차 차분 공격에 대한 안전성 분석 내용을 종합하면 다음 정리와 같다.

정리 6. *라운드 함수 f의 대수적 차수를 d라 할 때, 세가지 2-블록 구조 C-형, R-형, L-형 각각의 4 라운드 고차 차분 공격에 필요한 평문과 암호문 쌍의 개수와 라운드 함수 최대 계산량은 각각 2^d, $4\cdot 2^d + 2^{d+n}$으로 모두 같다.*

이제 5 라운드 암호화 함수에 대한 대수적 차수를 비교해 보자. 마지막 라운드인 5 라운드에서만 swapping이 없다고 가정한 기호를 사용하기로 한다. C-형과 R-형 구조 5 라운드에 대한 고차 차분 공격에서는 x_4^R의 대수적 방정식을, 그리고 L-형인 경우는 x_3^R의 대수적 방정식을 주목함으로써 공격에 필요한 평문 및 암호문의 개수를 예측할 수 있다. 각각의 대수적 방정식을 나타내면 다음과 같다.

$$C-\text{형}: \quad x_4^R = x^R \oplus f_{k_1}(x^L) \oplus f_{k_3}(x^L \oplus f_{k_2}(x^R \oplus f_{k_1}(x^L)))$$

$$R-\text{형}: \quad x_4^R = x^L \oplus f_{k_1}(x^R) \oplus f_{k_2}(x^L) \oplus f_{k_3}(x^L \oplus f_{k_1}(x^R))$$

$$L-\text{형}: \quad x_3^R = f_{k_3}(f_{k_1}(x^L) \oplus f_{k_2}(x^R \oplus f_{k_1}(x^L)))$$

고차 차분 값을 구하는 점인 일차 독립인 벡터들을 무엇으로 택하든지 C-형과 L-형은 x_4^R과 x_3^R이 표현되는 함수의 대수적 차수가 최소 d^2인 반면, R-형의 경우는 x_4^R을 나타내는 함수의 대수적 차수를 d로 낮출 수 있음을 발견할 수 있다. R-형의 x_4^R을 나타내는 함수에서 공격자가 오른쪽 n 비트 성분이 모두 0이고, 일차 독립인 벡터들 $a_1,\cdots,a_d$에서의 d차 도함수를 계산하면 그 값은 상수가 된다. 그러므로 이 d차 차분을 이용하여 고차 차분 공격을 실시할 경우 필요로 하는 평문 및 암호문 쌍은 2^d개로 C-형과 L-형의 2^{d^2}개에 비해서 적다는 것을 알 수 있다. 이렇게 R-형의 대수적 차수가 작은 이유는 구조적인 특이성 때문이다. 고차 차분 공격 관점에서 보았을 때, 라운드별 최소의 대수적 차수는 C-형과 L-형이 4 라운드 공격시 d가 되고, 5 라운드 이후에는 라운드 수 증가에 따라서 d의 거듭 제곱으로 증가한다. 반면, R-형은 4 라운드 공격시 d가 된 이후로는 라운드 수가 두개 증가함에 따라 대수적 차수는 d의 거듭 제곱이 되는 구조를 갖고 있다. 이러한 점을 고려하여 고차 차분 공격에 대한 내성과 라운드 수에 대한 관계를 종합해서 나타낸 것이 다음 정리 7이다.

정리 7. *블록 암호의 총 라운드 수를 r이라 하고, $r \geq 4$이며, 라운드 함수 f의 대수적 차수를 d라 하자. 그러면 세가지 2-블록 구조 C-형, R-형, L-형 각각의 r 라운드 고차 차분 공격에 필요한 평문과 암호문 쌍의 개수 및 계산량은 다음 표 1과 같다.*

〈표 2〉 고차 차분 공격에 필요한 선택평문의 개수와 계산량

구조	선택 평문 개수	계산량
C-형	$2^{d^{r-3}}$	$r\cdot 2^{d^{r-3}} + 2^{d^{r-3}+n}$
R-형	$2^{d^{\lceil (r-3)/2 \rceil}}$	$r\cdot 2^{d^{\lceil (r-3)/2 \rceil}} + 2^{d^{\lceil (r-3)/2 \rceil}+n}$
L-형	$2^{d^{r-3}}$	$r\cdot 2^{d^{r-3}} + 2^{d^{r-3}+n}$

표에서 $\lceil x \rceil$은 x 보다 크거나 같고 x와 가장 가까운 정수를 의미하고, 계산량은 한 라운드 키를 결정하기 위해서 최대로 수행하는 라운드 함수의 계산 회수를 나타낸다.

정리 7을 보면 4 라운드 암호 함수에 대해서는 세가지 2-블록 구조가 고차 차분 공격 측면에서 동일한 안전성을 제공하지만, 5 라운드 이후에는 C-형과 L-형에 비해서 R-형의 안전성이 떨어진다는 사실을 알 수 있다. 정리 7에 제시된 계산량은 라운드 함수의 구체적인 모양에 의존하여 키에 대한 선형 함수로 구성된 판별식을 유도함으로써 계산 회수를 낮출 수 있

는 여지가 있다. 실제로 Shimoyama 등[15]은 라운드 함수의 대수적 차수가 2인 KN 암호에 대한 고차 차분 공격의 판별식으로 키에 대하여 선형인 수식을 이끌어 냄으로써 계산량을 낮추는 결과를 얻었다.

Matsui가 R-형을 블록 암호 MISTY[11]에 적용했을 때 장점으로 내세운 것이 병렬성이었다. R-형 구조는 C-형이나 L-형과 달리 두개의 라운드를 동시에 계산하는 것이 가능한 구조로 되어있다. 그러므로 병렬 연산이 가능한 환경에서는 R-형 구조가 속도면에서 우수하다고 볼 수 있다. 본 절에서 분석한 고차 차분 공격 관점의 안전성 측면에서는 R-형이 C-형과 L-형에 비해서 약한 것으로 판단되기 때문에 여기에서 우리는 안전성과 효율성은 양립하기 힘든 개념이란 사실을 다시한번 깨닫게 된다.

V. 결 론

우리는 본 논문에서 DC 및 LC에 증명 가능한 안전성을 제공하는 세가지 서로 다른 2-블록 구조에 대한 고차 차분 공격 관점의 안전성을 이론적으로 비교 분석하였다. 특히, L-형 구조에 대한 고차 차분 공격은 본 논문에서 처음으로 수행한 것으로 마지막 r 라운드 키를 결정하기 위해서 $r-1$ 라운드 후의 암호문을 이용한 C-형 및 R-형과 달리 $r-2$ 라운드 후의 암호문을 이용할 수 있음을 보였다.

라운드 함수의 대수적 차수와 고차 차분 공격의 관계를 토대로 한 안전성 분석 결과로서 4 라운드 암호화 함수의 경우 세가지 2-블록 구조가 고차 차분 공격 관점에서 동일한 안전성을 제공한다는 사실을 증명하였으며, 5 라운드 이후의 암호화 함수에 있어서는 병렬 연산이 가능한 R-형 구조가 C-형과 L-형에 비해서 효율성은 높지만 고차 차분 공격 관점의 안전성은 떨어진다는 사실을 밝혔다.

참 고 문 헌

[1] K. Aoki and K. Ohta, "Strict evaluation of the maximum average of differential probability and the maximum average of linear probability", *IEICE TRANS. FUNDAMENTALS*, No. 1, 1997, pp. 2-8.

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

[3] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like Cryptosystems", *Journal of Crypto logy*, 1991, No. 4, (1), pp. 3-72.

[4] T. Jakobsen and L. R. Knudsen, "The interpolation attack on block ciphers", *Fast Software Encryption'97*, LNCS 1267, Springer- Verlag, 1997, pp. 28-40.

[5] Y. Kaneko, F. Sano, and K. Sakurai, "On provable security against differential and linear cryptanalysis in generalized Feistel ciphers with multiple random functions", *Proceedings of SAC'97*, 1997, pp. 185-199.

[6] L. R. Knudsen, "Truncated and higher order differentials", *Fast Software Encryption'95, LNCS 1008*, Springer-Verlag, 1995, pp. 196-211.

[7] X. Lai, "Higher order derivatives and differential cryptanalysis", *Communications and Cryptography*, Kluwer Academic Press, 1994, pp. 227-233.

[8] X. Lai, J. Massey, and S.Murphy, "Markov Ciphers and Differential Cryptanalysis", *Advances in Cryptology - Eurocrypt'91*, LNCS 547, Springer-Verlag, 1991, pp. 17-38.

[9] M. Matsui, "Linear cryptanalysis method for DES cipher", *Advances in Cryptology - Eurocrypt'93*, LNCS 765, Springer-Verlag,

1993, pp. 386-397.

[10] M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptalaysis", *Fast Software Encryption*, LNCS 1039, Springer-Verlag, 1996, pp. 205-218.

[11] M. Matsui, "New Block Encryption Algorithm MISTY", *Fast Software Encryption'97*, LNCS 1267, Springer-Verlag, 1997, pp. 54-68.

[12] National Institute of Standards and Technology, "Skipjack and KEA Algorithm Specifications", http://csrc.nist.gov/encryption/skipjack-jea.htm, 1998.

[13] K. Nyberg, "Linear Approximation of Block Ciphers", *Advances in Cryptology - Eurocrypt'94*, LNCS 950, Springer-Verlag, 1994, pp. 439-444.

[14] K. Nyberg and L. R. Knudsen, "Provable Security against Differential Cryptanalysis", *Journal of Cryptology*, 1995, No. 8, (1), pp. 27-37.

[15] T. Shimoyama, S. Moriai, and T. Kaneko, Improving the higher order differential attack and cryptanalysis of the KN Cipher", *Information Security Workshop, Preproceedings*, 1997, pp. 1-8.

[16] M. Sugita, Higher order differen- tial attack of block ciphers MISTY1,2", *Technical Report of IEICE*, ISEC 98-4, 1998, pp. 31-40.

著者紹介----------

강 주 성 (Ju-Sung Kang)

1989년 2월 : 고려대학교 수학과 졸업
1991년 2월 : 고려대학교 수학과 석사
1996년 2월 : 고려대학교 수학과 박사
1997년 12월 ~ 현재 : 한국전자통신연구원 선임연구원

박 상 우 (Sangwoo Park)

1989년 2월 : 고려대학교 수학교육과 졸업
1991년 8월 : 고려대학교 수학과 석사
1991년 8월 ~ 현재 : 한국전자통신연구원 선임연구원

이 상 진 (Sangjin Lee)

1987년 2월 : 고려대학교 수학과 졸업
1989년 2월 : 고려대학교 수학과 석사
1994년 8월 : 고려대학교 수학과 박사
1989년 10월 ~ 1999년 2월 : 한국전자통신연구원 선임연구원
1999년 3월 ~ 현재 : 고려대학교 자연과학대학 수학과 조교수