情報保護學會論文誌
第13券 第3號, 2003. 6

블록 암호 구조에 대한 불능 차분 공격*

김 종 성**, 홍 석 희**, 이 상 진**, 임 종 인**, 은 희 천***

Impossible Differential Cryptanalysis for Block Cipher Structures

Jongsung Kim**, Seokhie Hong**, Sangjin Lee**, Jongin Lim**, Hichun Eun***

요 약

Biham[4]등에 의해 소개된 불능 차분 공격은 불능 차분 특성을 이용하는 공격법이다. 그러므로 블록 암호의 불능 차분 공격에 대한 안전성은 불능 차분 특성에 의해 측정된다. 본 논문에서는 라운드 함수의 구체적인 형태를 고려하지 아니한 블록 암호 구조로부터 발생할 수 있는 여러 가지 불능 차분 특성을 찾는 널리 활용 가능한 방법을 제시한다. 이 방법을 이용하여 Nyberg[12]가 제시한 일반화된 Feistel network와 일반화된 RC6 유사 구조에 대한 여러 가지 불능 차분 특성을 찾을 수 있다. 본 논문에서 다루는 모든 라운드 함수는 전단사 함수이다.

ABSTRACT

Impossible differential cryptanalysis(IDC) introduced by Biham et. al.[4] uses impossible differential characteristics. Therefore, a security of a block cipher against IDC is measured by impossible differential characteristics. In this paper, we provide a wildly applicable method to find various impossible differential characteristics of block cipher structures not using the specified form of a round function. Using this method, we can find various impossible differential characteristics for Nyberg's generalized Feistel network and a generalized RC6-like structure. Throughout the paper, we assume round functions used in block cipher structures are bijective.

Keyword :

Ⅰ. 서 론

블록 암호에 대한 가장 강력한 공격법들로서 차분 공격[2]과 선형 공격[9]이 있다. 이러한 공격법들은 기존의 여러 가지 블록 암호에 효과적으로 적용되어 왔다. 그래서 블록 암호의 차분 및 선형 공격에 대한 안전성의 평가에 많은 관심을 가지게 되었다. 1992년, Nyberg와 Knudsen은[11] 차분 공격에 대한 증명 가능한 안전성의 개념을 소개하고, Feistel 구조의 차분 공격에 대한 증명 가능한 안전성을 제시하였다. 그 후, 차분 및 선형 공격에 대한 증명 가능한 많은 블록 암호 구조들이 연구되었다[1,6,7,8,10,13,15]. 그러나 차분 및 선형 공격에 대한 안전성의 평가는 블록 암호의 안전성을 평가하는데에 한계가 있다. 왜냐하면, 차분 및 선형 공격에 취약하지 않은 블록 암호가 다른 공격법들에 취약할 수 있기 때문이다. 예를 들어, 라운드 함수가 전단사인 3 라운드 Feistel 구조는 차분 및 선형 공격에 대한 증명 가능한 안전성[1]을 가지지만, 5라운드 불능 차분 특성이 존재한다. 이러한 사실은 Nyberg[13]가 제시한 Feistel의 일반화된 구조에

* 본 연구는 고려대학교 특별연구비에 의하여 수행 되었습니다.
** 고려대학교 정보보호기술연구센터(CIST)({joshep, hsh, sangjin, jilim}@cist.korea.ac.kr)
*** 고려대학교 자연과학대학 정보수학과(hceun@tiger.korea.ac.kr)

도 적용되어진다. (이는 Nyberg의 conjecture가 옳다는 전제하에서 성립한다.[표 1])

본 논문에서는 라운드 함수가 전단사인 블록 암호 구조에서 발생할 수 있는 불능 차분 특성을 찾는 널리 활용 가능한 방법을 제시한다.

〔표 1〕 본 논문의 결과에 대한 요약
(n: 각 라운드에 존재하는 함수 F의 개수, p: 함수 F에 대한 최대 평균 차분 확률, A: 최대 평균 차분 확률이 p^{2n}으로 유계할 라운드 수 r, B: 불능 차분 특성의 라운드 수 r)

블록암호구조	차분공격(A)	불능차분공격(B)
일반화된 Feistel network	$r \geq 3n, (n \geq 1)$	$r=3n+2$, $r=7, (n=2)$
comment	conjecture[11]	성질 1 (Ⅳ장)
일반화된 RC6 유사 구조		$r=4n+1$
comment		성질 2 (Ⅳ장)

Ⅱ. 불능 차분 공격에 대한 새로운 기본적인 개념

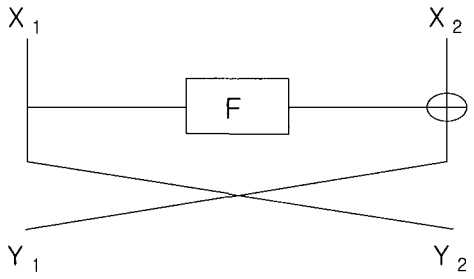
본 절에서는 불능 차분 공격에 대한 여러 가지 새로운 기호와 정의들을 소개한다. 블록 암호 구조 S는 전단사인 라운드 함수 F를 가지며, n개의 입/출력 블록을(예를 들어 Feistel 구조는 2개의 입/출력 블록을 가진다.) 가진다고 가정하자. 즉, S의 한 라운드에 대한 입력과 출력을 각각 $(Y_1, Y_2, \cdots, Y_n)$와 $(X_1, X_2, \cdots, X_n)$라 가정하자.

정의 1

블록 암호 구조 S에 대한 $n \times n$ 암호화 특성 행렬 E와 $n \times n$ 복호화 특성 행렬 D는 다음과 같이 정의한다. 만약 Y_j가 X_i에 영향을 받는다면, E의 (i,j) 성분을 1로 정의하며, 영향을 받지 않는다면, (i,j) 성분을 0으로 정의한다. 특히, Y_j가 $F(X_i)$에 영향을 받는다면, E의 (i,j)성분을 1 대신 1_F로 정의한다. 거꾸로, 만약 X_j가 Y_i에 영향을 받는다면, D의 (i,j)성분을 1로 정의하며, 영향을 받지 않는다면, (i,j)성분을 0으로 정의한다. 특히, X_j가 $F(Y_i)$ 또는 $F^{-1}(Y_i)$에 영향을 받는다면, D의 (i,j)성분을 1 대신 1_F로 정의한다.

[그림 1]과 같은 Feistel 구조의 암/복호화 특성 행렬은 정의 1에 의하여 다음과 같이 된다.

$$E=\begin{pmatrix} 1_F & 1 \\ 1 & 0 \end{pmatrix}, \quad D=\begin{pmatrix} 0 & 1 \\ 1 & 1_F \end{pmatrix}$$



〔그림 1〕 Festel 구조에 대한 한 라운드

만약 블록 암호 구조 S의 암/복호화 특성 행렬 E와 D의 각 열의 성분 $1(\neq 1_F)$의 개수가 한개 이하라면, 다음장에서 제시될 알고리즘을 이용하여 S에 대한 불능 차분 특성의 길이를 쉽게 구할 수 있다. 이러한 행렬을 1-property 행렬이라 부르기로 하자. 본 논문에서는 E와 D 모두 1-property 행렬인 S에 대해서만 고려한다.

정의 2

고정된 입력 차분 $\alpha=(\alpha_1, \alpha_2, \cdots, \alpha_n)$에 대응하는 차분 벡터 $\vec{a}=(a_1, a_2, \cdots, a_n)$은 다음과 같이 정의한다.

$$a_i=\begin{cases} 0 & \text{if } \alpha_i=0 \\ 1^* & otherwise \end{cases}$$

고정된 입력 차분 α에 대한 r 라운드 후의 가능한 출력 차분(한 블록에 대한 출력 차분)은 5가지로 표현 될 수 있다. 0 차분, 0이 아니면서 고정되지 않은 차분 , 0이 아닌 고정된 차분, 0이 아닌 고정된 차분과 0이 아니면서 고정되지 않은 차분의 exor, 그리고 고정되지 않은 차분으로 표현 되어진다. 입력 차분 α에 대한 r 라운드 후의 출력 차분에 대응하는 벡터를 $\vec{a_r}$로 표기하고, 벡터 $\vec{a_r}$의 i번째 성분을 $a_{r,i}$로 표기한다면, 성분 $a_{r,i}$에 대응하는 차분은 표 2와 같이 정의한다. (위와 같은 작업을 복호화 과정에 적용할 때에는, $\vec{a_r}$ 대신에 $\vec{b_r}$을 $a_{r,i}$ 대신에 $b_{r,i}$을 사용한다.)

〔표 2〕 차분 벡터의 성분과 대응하는 차분

성 분	대응하는 차분
0	0 차분
1	0이 아니면서 고정되지 않은 차분
1^*	0이 아닌 고정된 차분
2^*	0이 아닌 고정된 차분과 0이 아니면서 고정되지 않은 차분의 exor
$t(\geq 2)$	고정되지 않은 차분

[표 2]에 의하면, 성분 $t(\geq 2)$에 대한 대응하는 차분은 성분 t로부터 알 수 없다. 다시 말해, 성분 t에 대응하지 않는 차분을 알 수 없다. 반면, 성분 0, 1, $1^*, 2^*$에 대한 대응하지 않는 차분은 각 성분들로부터 알 수 있다. 예를 들어, 성분 2^*가 차분 $\alpha_i \oplus \delta_j$에 대응된다면,(α_i: 0이 아닌 고정된 차분, δ_j: 0이 아니면서 고정되지 않은 차분) 성분 2^*는 결코 차분 α_i를 나타낼 수 없다. (앞으로 사용되는 차분의 기호 $\alpha_i, \alpha_j, \alpha_k$는 0이 아닌 고정된 차분을 $\delta_i, \delta_j, \delta_k$는 0이 아니면서 고정되지 않은 차분을, x_i, x_j, x_k는 고정되지 않은 차분을 나타내기로 하자.) 이러한 사실은 블록 암호 구조 S에 대한 불능 차분 특성을 찾는데 유용하게 이용된다.

차분 벡터 $\overrightarrow{a_r}$ 또는 $\overrightarrow{b_r}$을 계산하기 위해서는 차분 벡터와 특성 행렬 사이의 연산을 정의해야한다. 차분 벡터 $\overrightarrow{a_r}$과 $\overrightarrow{b_r}$은 각각 다음과 같이 계산되어진다.

$$\begin{aligned}\overrightarrow{a_r} = \overrightarrow{a_{r-1}} \cdot E &= (a_{r-1,i}) \cdot (E_{i,j})) \\ &= (\sum_i a_{r-1,i} \cdot E_{i,j}), \\ \overrightarrow{b_r} = \overrightarrow{b_{r-1}} \cdot D &= (b_{r-1,i}) \cdot (D_{i,j}) \\ &= (\sum_i b_{r-1,i} \cdot D_{i,j})\end{aligned}$$

먼저, 곱 $a_{r-1,i} \cdot E_{i,j}$에 대해서는 [표 3]와 같이 정의한다. (복호화 과정의 계산도 암호화 과정의 계산과 동일하다.)

그리고 두 성분 사이의 덧셈 $a_{r-1,i_1} \cdot E_{i_1,j} + a_{r-1,i_2} \cdot E_{i_2,j}, (i_1 \neq i_2)$은 대응하는 두 차분에 대한 exor을 나타내므로, 다음과 같이 자연스럽게 정의 할 수 있다.

1. *을 가지고 있지 않은 두 성분의 덧셈은 정수 위에서의 덧셈 연산과 동일하다.
2. 두 성분 중 하나의 성분만이 *을 가질 때, 다음과 같이 정의한다.
   - 만약 성분 k가 0 또는 1이면, $1^* + k = (1+k)^*$이 되고, k가 2 이상의 성분이라면, $1^* + k = 1 + k$가 된다.
   - 만약 성분 k가 0이면, $2^* + k = (2+k)^*$이 되고, k가 1 이상의 성분이라면, $2^* + k = 2 + k$이 된다.

〔표 3〕 곱 $a_{r-1,i} \cdot E_{i,j}$에 대한 정의 및 의미
(k: 벡터에 대한 임의의 성분값)

$a_{r-1,i} \cdot E_{i,j}$	의 미
$k \cdot 0 = 0$	i번째 입력 블록은 j번째 출력 블록에 아무런 영향을 주지 않는다.
$k \cdot 1 = k$	i번째 입력 블록은 j번째 출력 블록에 F 함수를 거치지 않고 직접 영향을 준다.
$k \cdot 1_F$	i번째 입력 블록은 F 함수를 거친 후에도 j번째 출력 블록에 영향을 준다.
$0 \cdot 1_F = 0$	0 차분에 대한 F 함수 후의 출력 차분은 0이 된다.
$1 \cdot 1_F = 1$	δ_i에 대한 F 함수 후의 출력 차분은 δ_j가 된다.
$1^* \cdot 1_F = 1$	α_i에 대한 F 함수 후의 출력 차분은 δ_j가 된다.
$2^* \cdot 1_F = 2$	$\alpha_i \oplus \delta_j$에 대한 F 함수 후의 출력 차분은 x_i가 된다.
$t \cdot 1_F = t$	x_i에 대한 F 함수 후의 출력 차분은 x_j가 된다.

블록 암호 구조 S의 암/복호화 특성 행렬이 1-property 행렬이므로, [표 3]의 곱 연산에 의한 성분 $a_{r-1,i} \cdot E_{i,j}$은 모든 i에 대하여 1개 이하의 *을 갖는다. 따라서 더하여지는 두 성분이 모두 *을 가질 수는 없다. [표 4]은 두 성분의 덧셈 연산에 대응하는 두 차분의 exor을 나타낸 것이다.

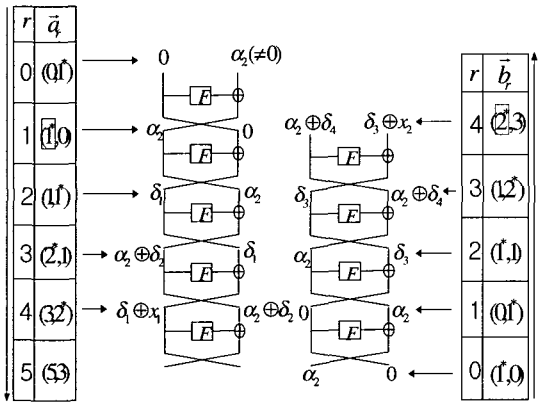
〔표 4〕 두 성분의 덧셈 연산에 대응하는 두 벡터의 exor
(γ_i: 임의의 성분 k에 대응하는 차분, t_i, t_j: 2이상의 성분)

두 성분의 덧셈	대응하는 두 벡터의 exor
$0 + k = k$	$0 \oplus \gamma_i = \gamma_i$
$1 + 1 = 2$	$\delta_i \oplus \delta_j = x_k$
$1 + 1^* = 2^*$	$\delta_i \oplus \alpha_j = \delta_i \oplus \alpha_j$
$1 + 2^* = 3$	$\delta_i \oplus (\delta_j \oplus \alpha_k) = x_i$
$1 + t = 1 + t$	$\delta_i \oplus x_j = x_k$
$1^* + t = 1 + t$	$\alpha_i \oplus x_j = x_k$
$2^* + t = 2 + t$	$(\alpha_i \oplus \delta_j) \oplus x_k = x_i$
$t_i + t_j = t_i + t_j$	$x_i \oplus x_j = x_k$

위와 같이 정의된 곱셈과 덧셈 연산은 논리적으로 ([표 2]의 관점에서) 잘 정의 되어진다.

새롭게 정의된 연산의 이해를 돕기 위해 라운드 함수가 전단사인 Feistel 구조를 살펴보자. 입력 차분 벡터 $\vec{a}=(0,1^*)$에 대한 r라운드 후의 출력 차분 벡터 $\vec{a_r}$은 위에서 정의된 연산에 의하여 다음과 같이 계산 되어진다. ([그림 2]의 왼쪽 그림 참조)

- $\vec{a_1}=\vec{a}\cdot E=(0\cdot 1_F+1^*\cdot 1,\ 0\cdot 1+1^*\cdot 0)=$
$(0+1^*,\ 0+0)=(1^*,\ 0).$
- $\vec{a_2}=\vec{a_1}\cdot E=(1^*\cdot 1_F+0\cdot 1,\ 1^*\cdot 1+0\cdot 0)=$
$(1+0,\ 1^*+0)=(1,\ 1^*).$
- $\vec{a_3}=\vec{a_2}\cdot E=(1\cdot 1_F+1^*\cdot 1,\ 1\cdot 1+1^*\cdot 0)=$
$(1+1^*,\ 1+0)=(2^*,\ 1).$
- $\vec{a_4}=\vec{a_3}\cdot E=(2^*\cdot 1_F+1\cdot 1,\ 2^*\cdot 1+1\cdot 0)=$
$(2+1,\ 2^*+0)=(3,\ 2^*).$
- $\vec{a_5}=\vec{a_4}\cdot E=(3\cdot 1_F+2^*\cdot 1,\ 3\cdot 1+2^*\cdot 0)=$
$(3+2^*,\ 3+0)=(5,\ 3).$



[그림 2] 차분 벡터 $\vec{a}=(0,1^*)$와 $\vec{b}=(1^*,0)$에 대한 $\vec{a_r}$와 $\vec{b_r}$의 대응되는 차분

($\delta_1,\delta_2,\delta_3,\delta_4$: 0 아니면서 고정되지 않은 차분, x_1,x_2 : 고정되지 않은 차분)

이제, 차분 벡터의 성분을 이용하여 블록 암호 구조 S에 대한 불능 차분 특성을 찾아보자. 입력 차분과 출력 차분이 각각 α(차분 벡터 $\vec{a}$에 대응되는 차분)와 β인 불능 차분 특성을 $\alpha\nrightarrow\beta$로 표기한다면, 다음과 같은 성질을 갖는다.

- 만약 $a_{r,i}=0$이면, $\beta_i\neq 0$인 r 라운드 불능 차분 특성 $\alpha\nrightarrow\beta$이 존재한다.
- 만약 $a_{r,i}=1$이면, $\beta_i=0$인 r 라운드 불능 차분 특성 $\alpha\nrightarrow\beta$이 존재한다.
- 만약 $a_{r,i}=1^*$(대응하는 차분: α_i)이면, $\beta_i\neq\alpha_i$인 r 라운드 불능 차분 특성 $\alpha\nrightarrow\beta$이 존재한다.
- 만약 $a_{r,i}=2^*$(대응하는 차분: $\alpha_i\oplus\delta_j$)이면, $\beta_i=\alpha_i$인 r 라운드 불능 차분 특성 $\alpha\nrightarrow\beta$이 존재한다.

만약 $a_{r,i}>2$이면, 성분 $a_{r,i}$로부터 대응되는 차분을 추측할 수 없다. 이것은 2이상의 성분을 이용한 불능 차분 특성이 존재하는지 여부를 정확히 알 수 없음을 의미한다. 그러나 불능 차분 공격의 관점에서 성분 $0,1,1^*,2^*$은 유용하게 이용된다. 이러한 성분의 집합을 $U=\{0,1,1^*,2^*\}$로 표기하고, 이제부터 집합 U에 속하지 않는 성분은 고려하지 않는다.

$a_{r,i}\in U$인 경우, r 라운드 불능 차분 특성은 위와 같이 항상 존재하며, 또한 r 라운드 이상의 불능 차분 특성도 존재 할 수 있다. r 라운드 이상의 불능 차분 특성을 찾기 위해 $m\in U$의 보조 성분 집합인 $\overline{m}$을 정의하자. $\overline{m}$는 다음과 같은 성질을 갖는다. 첫째, $\overline{m}$는 U의 부분 집합이다. 둘째, $\overline{m}$의 원소들은 m에 대응하지 않는 모든 차분들을 나타낸다. 예를 들어, $\overline{1^*}$를 살펴보자. 1^*는 0이 아닌 고정된 차분 α_i을 나타내므로, 1^*는 U의 원소들에 대응하는 차분들 중 0, $\alpha_j(\neq\alpha_i)$ 또는 $\alpha_i\oplus\delta_j$ 차분과는 대응될 수 없다. 따라서, $\overline{1^*}=\{0,1^*,2^*\}$이 된다. 비슷한 방법으로 $m\in U$에 대한 $\overline{m}$를 [표 5]와 같이 얻을 수 있다.

[표 5] 성분 $m\in U$와 집합 $\overline{m}$에 대응하는 차분

m	차분	$\overline{m}$	차분
0	0	$\overline{0}=\{1,1^*\}$	δ_j,α_i
1	δ_i	$\overline{1}=\{0\}$	0
1^*	α_i	$\overline{1^*}=\{0,1^*,2^*\}$	$0,\alpha_j,\alpha_i\oplus\delta_j$
2^*	$\alpha_i\oplus\delta_j$	$\overline{2^*}=\{1^*\}$	α_i

$\overline{m}$의 정의에 의하여, $a_{r,i}\in U$일 때 다음과 같은 r라운드 이상의 불능 차분 특성이 존재한다.

- 만약 $a_{r,i}=m$이고 $b_{r,i}\in\overline{m}$이면, $(r+r')$라운드

불능 차분 특성 $\alpha \nrightarrow \beta$이 존재한다.
- 만약 $a_{r,i} \in \overline{m}$이고 $b_{r',i} = m$이면, $(r+r')$라운드 불능 차분 특성 $\alpha \nrightarrow \beta$이 존재한다.

정의 3

고정된 입력 차분 벡터 $\vec{a}$에 대해서, $\vec{a}$와 성분 $m \in U$ (또는 집합 $\overline{m}$)에 따른 최대 암호화 라운드 수는 다음과 같이 정의한다.

$$ME_i(\vec{a}, m) = \max_r \{r \mid a_{r,i} = m\},$$
$$ME_i(\vec{a}, \overline{m}) = \max_{l \in \overline{m}} \{ME_i(\vec{a}, l)\}.$$

또한, 성분 $m \in U$ (또는 집합 $\overline{m}$)에 따른 최대 암호화 라운드 수는 다음과 같이 정의한다.

$$ME_i(m) = \max_{\vec{a} \neq 0} \{ME_i(\vec{a}, m)\},$$
$$ME_i(\overline{m}) = \max_{\vec{a} \neq 0} \{ME_i(\vec{a}, \overline{m})\}.$$

동일한 방법으로, 각각의 최대 복호화 라운드 수는 다음과 같이 정의한다.

$$MD_i(\vec{b}, m) = \max_r \{r \mid b_{r,i} = m\},$$
$$MD_i(\vec{b}, \overline{m}) = \max_{l \in \overline{m}} \{MD_i(\vec{b}, l)\},$$
$$MD_i(m) = \max_{\vec{b} \neq 0} \{MD_i(\vec{b}, m)\},$$
$$MD_i(\overline{m}) = \max_{\vec{b} \neq 0} \{MD_i(\vec{b}, \overline{m})\}.$$

정의 3에 의하면, 블록 암호 구조 S는 $(ME_i(\vec{a}, m) + MD_i(\vec{b}, \overline{m}))$ 라운드 또는 $(ME_i(\vec{a}, \overline{m}) + MD_i(\vec{b}, m))$ 라운드의 불능 차분 특성을 갖는다. 만약 $M(\vec{a}, \vec{b}) = \max_{i,m} \{ME_i(\vec{a}, m) + MD_i(\vec{b}, \overline{m})\} = \max_{i,m} \{ME_i(\vec{a}, \overline{m}) + MD_i(\vec{b}, m)\}$, $M = \max_{\vec{a} \neq 0, \vec{b} \neq 0} M(\vec{a}, \vec{b})$라 정의한다면, 블록 암호 구조 S는 $M(\vec{a}, \vec{b})$ 라운드 또는 M 라운드의 불능 차분 특성 또한 갖는다. 한편, $M = \max_{i,m} \{ME_i(m) + MD_i(\overline{m})\} = \max_{i,m} \{ME_i(m) + MD_i(\overline{m})\}$이(이 식은 다음 장에서 제시되는 알고리즘에 유용하게 사용된다.) 성립하며, 위의 수식들로부터 다음과 같은 정리를 이끌어 낼 수 있다.

정리 1

라운드 함수가 전단사이고 암/복호화 특성 행렬이 1-property 행렬인 블록 암호 구조 S에 대해서 집합 U를 이용하여 찾을 수 있는 최대 불능 차분 특성의 라운드 수는 M이다.

다음은 Feistel 구조에 대한 M 라운드 불능 차분 특성을 찾는 과정을 보여준다.

• 라운드 함수가 전단사인 Feistel 구조는 5 라운드 불능 차분 특성을 갖는다.

먼저, i, m에 따른 $ME_i((0,1^*), m)$와 $MD_i((1^*, 0), \overline{m})$의 값을 구해 보자. [그림 2]에 의하여 $ME_i((0,1^*), m)$와 $MD_i((1^*,0), \overline{m})$의 값은 쉽게 체크할 수 있다. 특히 [그림 2]의 박스 부분에 의하여 $M((0,1^*),(1^*,0)) = 5$ 가 됨을 알 수 있다. 이와 동일한 방법으로 다른 입력 차분 벡터들에 대한 다음의 식들을 얻을 수 있다.

$M((0,1^*),(0,1^*)) = 4$, $M((0,1^*),(1^*,1^*)) = 4$,
$M((1^*,0),(0,1^*)) = 3$, $M((1^*,0),(1^*,0)) = 4$,
$M((1^*,0),(1^*,1^*)) = 3$, $M((1^*,1^*),(0,1^*)) = 3$,
$M((1^*,1^*),(1^*,0)) = 4$, $M((1^*,1^*),(1^*,1^*)) = 2$.

따라서 $M = \max_{\vec{a} \neq 0, \vec{b} \neq 0} M(\vec{a}, \vec{b}) = 5$이 된다.

그러므로 라운드 함수가 전단사인 Feistel 구조는 5라운드 불능 차분 특성 $(0, \alpha_2) \nrightarrow (\alpha_2, 0)$을 갖는다.

Ⅲ. 라운드 수 M을 구하는 알고리즘

본 장에서는 앞장에서 소개한 정의와 기호들을 이용하여 불능 차분 특성의 길이 M을 구하는 알고리즘을 제시한다. 이 알고리즘은 블록 암호 구조 S의 암/복호화 특성 행렬이 1-property 행렬일 때 유용하게 이용된다. 알고리즘은 다음과 같이 크게 4단계의 과정을 수행한다.

Step 1. 암/복호화 특성 행렬 $E = (E_{i,j})_{n \times n}$와 $D = (D_{i,j})_{n \times n}$를 입력한다.
Step 2. 최대 암호화 라운드 수 $ME_i(m)$을 계산한다. $(1 \le i \le n,\ m \in U)$
Step 3. 최대 복호화 라운드 수 $MD_i(\overline{m})$을 계산한다.
Step 4. U을 이용한 불능 차분 특성의 최대 길이 $M = \max_{i,m} \{ME_i(m) + MD_i(\overline{m})\}$을 출력한다.

[표 6]은 위의 단계들의 수행 과정상 필요한 저장 공간에 대한 설명이다. 알고리즘에서 가장 중요한 부분은 차분 벡터의 성분들중 *을 가지는 성분을 구분해 내는 것이다. [표 6]은 성분 y와 y^*을 구분하기 위한 변수 tt_i에 대한 설명이다. [표 6]에서 출력 차분 벡터에 대한 j번째 성분이 *을 가질 필요충분 조건이 $tt_1+tt_2+\cdots+tt_n=-1$이 된다. 왜냐하면 암/복호화 특성 행렬 E와 D가 1-property 행렬이기 때문이다.

〔표 6〕 알고리즘에 사용되는 저장 공간의 값에 대한 의미 ($y=0,1,2,\cdots.$)

저장 공간	의 미
$e_{i,j}=0$	$E_{i,j}=0$
$e_{i,j}=1$	$E_{i,j}=1$ or 1_F
$\widehat{e_{i,j}}=0$	$E_{i,j}=1$ ($y^*\cdot E_{i,j}=y^*$로서 * 을 보존한다.)
$\widehat{e_{i,j}}=1$	$E_{i,j}=0$ or 1_F ($y^*\cdot E_{i,j}=0$ or y 로서 *을 보존하지 못한다.)
$a_{r,i}=y$	차분 벡터 $\overrightarrow{a_r}$의 i번째 성분이 y 또는 y^* 이다.
$\widehat{a_{r,i}}=0$	차분 벡터 $\overrightarrow{a_r}$의 i번째 성분이 * 을 가지지 않는다.
$\widehat{a_{r,i}}=-1$	차분 벡터 $\overrightarrow{a_r}$의 i번째 성분이 * 을 갖는다.
$ME_i(\overrightarrow{a},k)=r$	$ME_i(\overrightarrow{a},m)=r$ ($m=0$이면 $k=1$, $m=1$이면 $k=2$, $m=1^*$이면 $k=3$, $m=2^*$이면 $k=4$이다.)
$ME_i(k)=r$	$ME_i(m)=r$ (m,k: 위와동일)
$MD_i(k)=r$	$MD_i(m)=r$ (m,k: 위와동일)
$\overline{MD_i}(k)=r$	$MD_i(\overline{m})=r$ (m,k: 위와동일)

〔표 7〕 알고리즘 안에서의 차분 벡터와 행렬의 곱

차분벡터의 성분 $c,(\widehat{a_i})$	E or D의성분 $d,(\widehat{e_{i,j}})$	$c\cdot d$	$\widehat{a_i}+\widehat{e_{i,j}}=tt_i$ if$(tt_i=1)tt_i\leftarrow 0$
$y^*,(-1)$	$0,(1)$	0	0
$y^*,(-1)$	$1_F,(1)$	y	0
$y^*,(-1)$	$1,(0)$	y^*	-1
$y,(0)$	$0,(1)$	0	0
$y,(0)$	$1_F,(1)$	y	0
$y,(0)$	$1,(0)$	y	0

불능 차분 특성의 길이 M을 구하는 알고리즘

Step 1 :
if $E_{i,j}=0$, then $e_{i,j}\leftarrow 0$, $\widehat{e_{i,j}}\leftarrow 1$
if $E_{i,j}=1$, then $e_{i,j}\leftarrow 1$, $\widehat{e_{i,j}}\leftarrow 0$
if $E_{i,j}=1_F$, then $e_{i,j}\leftarrow 1$, $\widehat{e_{i,j}}\leftarrow 1$

Step 2 :
$ME_i(k)\leftarrow 0$, for $1\le i\le n$, $1\le k\le 4$
For each input difference vector $\overrightarrow{a}$
if($a_{0,i}=0$) $\widehat{a_{0,i}}\leftarrow 0$, for $1\le i\le n$
if($a_{0,i}=1$) $\widehat{a_{0,i}}\leftarrow -1$, for $1\le i\le n$
$ME_i(\overrightarrow{a},k)\leftarrow 0$, for $1\le i\le n$, $1\le k\le 4$
$r\leftarrow 0$
while(there exists $l,(1\le l\le n)$ such that $a_l\le 2.$)
for $i=1$ to n
$t_i\leftarrow 0$, $\widehat{t_i}\leftarrow 0$
for $j=1$ to n
$t_i\leftarrow t_i+a_{r,j}\cdot e_{j,i}$
$tt_j\leftarrow \widehat{a_{r,j}}+\widehat{e_{j,i}}$
if($tt_j=1$) $tt_j\leftarrow 0$
$\widehat{t_i}\leftarrow \widehat{t_i}+tt_j$
$r\leftarrow r+1$
$a_{r,i}\leftarrow t_i$, $\widehat{a_{r,i}}\leftarrow \widehat{t_i}$, for $1\le i\le n$
for $i=1$ to n
if($a_{r,i}=0$) $ME_i(\overrightarrow{a},1)\leftarrow r$
if($a_{r,i}=1$, $\widehat{a_{r,i}}=0$) $ME_i(\overrightarrow{a},2)\leftarrow r$
if($a_{r,i}=1$, $\widehat{a_{r,i}}=-1$) $ME_i(\overrightarrow{a},3)\leftarrow r$
if($a_{r,i}=2$, $\widehat{a_{r,i}}=-1$) $ME_i(\overrightarrow{a},4)\leftarrow r$
for $i=1$ to n
for $k=1$ to 4
if($ME_i(k)\le ME_i(\overrightarrow{a},k)$)
$ME_i(k)\leftarrow ME_i(\overrightarrow{a},k)$

Step 3: Step 1과 2에서 행렬 E대신 D를 적용하여 $MD_i(k)$를 구한다.
for $i=1$ to n
$\overline{MD_i}(1)\leftarrow \max\{MD_i(2),MD_i(3)\}$
$\overline{MD_i}(2)\leftarrow MD_i(1)$
$\overline{MD_i}(3)\leftarrow \max\{MD_i(1),MD_i(3),MD_i(4)\}$
$\overline{MD_i}(4)\leftarrow MD_i(3)$

Step 4 :
$M=\max_{1\le i\le n,1\le k\le 4}\{ME_i(k)+\overline{MD_i}(k)\}$을 출력한다.

Ⅳ. 블록 암호 구조에의 적용

본장에서는 Ⅲ장에서 제시한 알고리즘을 이용하여

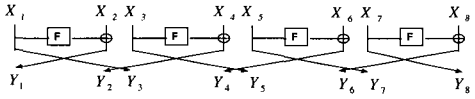
Nyberg의 일반화된 Feistel network와 일반화된 RC6 유사 구조에 대한 여러 가지 불능 차분 특성을 찾는다. 본장의 결과들은 각 입/출력 블록의 개수가 작은 경우의 (32개 이하) 프로그래밍에 기초한 것이다. 하지만, 일반화된 구조는 일정한 구조적 특성을 가지고 있기 때문에, 프로그래밍의 결과들을 입/출력 블록의 개수에 따른 일반화가 가능하다.

4.1 일반화된 Feistel Network에의 적용

일반화된 Feistel network는 Nyberg[12]에 의해 제안된 블록 암호 구조이다. 간단하게 그 구조를 살펴보면 다음과 같다. 한 라운드에 대한 입력값을 $(X_1, X_2, \cdots, X_{2n})$라 하자. 주어진 n개의 라운드 함수 $F_1, F_2, \cdots, F_n$과 n개의 라운드 키 $K_1, K_2, \cdots, K_n$에 대해서, 출력값 $(Y_1, Y_2, \cdots, Y_{2n})$은 다음과 같이 계산되어진다.

$$Y_{2j} = F_{j+1}(X_{2j+1} \oplus K_{j+1}) \oplus X_{2j+2},$$
$$Y_{2j+1} = X_{2j-1}, \quad (j = 1, \cdots, n-1),$$
$$Y_1 = F_1(X_1 \oplus K_1) \oplus X_2, \quad Y_{2n} = X_{2n-1}$$

만약 F_j를 키가 사용된 함수 F로 간주하고, $n=4$라면, 일반화된 Feistel network은 다음과 같이 묘사된다.



〔그림 3〕 일반화된 Feistel network에 대한 한 라운드

이제 일반화된 Feistel network에 대한 불능 차분 특성을 찾아보자. 일반화된 Feistel network는 1-property 행렬 E와 D를 갖는다. 그러므로 앞장에서 제시한 알고리즘을 이 network에 직접 적용할 수 있다. 이 network에 대한 알고리즘의 수행 시간은 대략 $2 \cdot 2^n$번의 Step 2의 과정이 요구된다. 하지만 일반화된 Feistel network의 암호화 함수와 복호화 함수가 거의 동일하다는 사실을 이용하여 알고리즘의 수행 시간을 1/2으로 줄일 수 있다. 즉, Step 3의 과정에서 필요한 최대 복호화 라운드 수 $MD_i(k)$은 Step 2에서 계산된 $ME_i(k)$로부터 쉽게 구할 수 있다. 성질 1은 일반화된 Feistel network에 대한 알고리즘의 적용 결과를 일반화 시킨 결과이다.

성질 1

· 각 라운드마다 2개의 전단사 함수 F를 가지고 있는 일반화된 Feistel network는 7 라운드의 불능 차분 특성을 갖는다. 또한, 각 라운드마다 3개 이상의 전단사 함수 F를 가지고 있는 일반화된 Feisztel network는 $(3n+2)$ 라운드의 불능 차분 특성을 갖는다.

또한 Ⅲ장에서 제시한 알고리즘을 약간 변형하여 성질 1에서 언급된 최대 불능 차분 특성의 구체적인 모양을 찾을 수 있다. (표 8).

표 8. 일반화된 Feistel Network의 최대 길이의 불능 차분 특성 ($\alpha_1, \alpha_2, \alpha_3, \beta_1$: 0이 아닌 고정된 차분, $(\gamma_1, \gamma_2) \neq (0,0)$)

7 라운드 불능 차분 특성 $(n=2)$
$(0,0,0,\alpha_1) \nrightarrow (\gamma_1,0,\gamma_2,0)$
$(0,0,\alpha_1,0) \nrightarrow (\gamma_1,0,\gamma_2,0)$
$(0,0,\alpha_1,\alpha_2) \nrightarrow (\beta_1,0,0,0)$
$(0,0,\alpha_1,\alpha_2) \nrightarrow (0,0,\beta_1,0)$
$(0,\alpha_1,\alpha_2,0) \nrightarrow (\alpha_2,0,0,0)$
$(0,\alpha_1,\alpha_2,\alpha_3) \nrightarrow (\alpha_2,0,0,0)$
$(3n+2)$ 라운드 불능 차분 특성 $(3 \le n \le 20)$
$(0,0,\cdots,0,\alpha_1) \nrightarrow (\gamma_1,0,\gamma_2,0,\cdots,0)$
$(0,\cdots,0,\alpha_1,0) \nrightarrow (\beta_1,0,0,\cdots,0,0)$
$(0,\cdots,0,\alpha_1,\alpha_2) \nrightarrow (\gamma_1,0,\gamma_2,0,\cdots 0)$

4.2 일반화된 RC6 유사 구조에의 적용

일반화된 RC6 유사 구조는 Moriai등[11]에 의해 제시된 블록 암호 구조로서 다음과 같이 묘사된다.

$$\begin{aligned} Y_{2i} &= X_{2i-1} && (1 \le i \le n) \\ Y_{2j+1} &= F(X_{2j-1}) \oplus X_{2j} && (1 \le j \le n-1) \\ Y_1 &= F(X_{2n-1}) \oplus X_{2n} \end{aligned}$$

성질 2는 일반화된 RC6 유사 구조에 대한 알고리즘의 적용 결과를 일반화 시킨 결과이다.

성질 2

각 라운드마다 n개의 전단사 함수 F를 가지고 있

는 일반화된 RC6 유사 구조는 $(4n+1)$ 라운드 불능 차분 특성 $(0,0,\cdots,0,\alpha_1)\nrightarrow(0,0,\cdots,0,\alpha_1)$을 갖는다.

Ⅳ. 결 론

본 논문에서는 라운드 함수가 전단사인 블록 암호 구조에서 발생할 수 있는 불능 차분 특성을 찾는 널리 활용 가능한 방법을 제시하였다. 이 방법을 이용하여, 일반화된 Feistel network의 $(3n+2)$라운드의 불능 차분 특성과 일반화된 RC6 유사 구조의 $(4n+1)$ 라운드의 불능 차분 특성을 찾을 수 있었다.

참 고 문 헌

[1] K. Aoki, K. Ohta, "Strict evaluation of the maximum average of differential probability and the maximem average of linear probability", IEICE Transactions fundamentals of Electronics, Communications and Computer Sciences, No.1, 1997, pp.2~8.

[2] E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", Advances in Cryptology-CRYPTO'90, LNCS 537, Springer-Verlag, 1991, pp.2~21.

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

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

[5] J. H. Cheon, M. J. Kim, K. J. Kim, J. Y. Lee, "Improved Impossible Differential Cryptanalysis of Rijndael and Crypton", ICISC'01, LNCS 2288, Springer-verlag, 2001, pp.39~49.

[6] S. H. Hong, S. J. Lee, J. I. Lim, J. C. Sung, D. Y. Choen, I. H. Cho, "Provable Security against Differential and Linear Cryptanalysis for the SPN structure", FSE'00, Springer-Verlag, 2000, pp.273~283.

[7] S. H. Hong, J. C. Sung, S. J. Lee, J. I. Lim, J. S. Kim, "Provable Security for 13 round Skipjack-like Structure", IPL, vol 82, 2002, pp.243~246.

[8] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, K. Ohta, "A strategy for constructing fast functions with practical security against differential and linear cryptanalysis", SAC'99, LNCS 1556, 1999, pp. 264~279.

[9] M. Matsui, "Linear cryptanalysis method for DES cipher", Advances in Cryptology - EUROCRYPT'93, LNCS 765, Springer-Verlag, 1994, pp.386~397.

[10] M. Matsui, "New structure of block ciphers with provable security against differential and linear cryptanalysis", FSE'96, 1996, pp.205~218.

[11] S. Moriai, S. Vaudenay, "On the Pseudorandomness of Top-Level Schemes of Block Ciphers", Advances in Cryptology - ASIACRYPT'00, LNCS 1976, Springer-Verlag, 2000, pp.289~302.

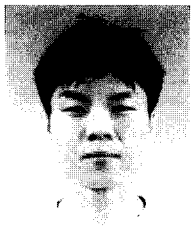
[12] K. Nyberg, L. R. Knudsen, "Provable security against differential cryptanalysis", Advances in Cryptology - CRYPTO'92, LNCS 740, Springer-Verlag, 1992, pp.566~574.

[13] K. Nyberg, "Generalized Feistel Networks", Advances in Cryptology - ASIACRYPT'96, LNCS 1163, 1996, pp.91~104.

[14] M. Sugita, K. Kobara, H. Imai, "Security of Reduced Version of the Block Cipher Camellia against Truncated and Impossible Differential Cryptanalysis", Advances in Cryptology - ASIACRYPT'01, LNCS 2248, 2001, pp.193~207.

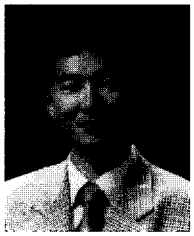
[15] J. C. Sung, S. J. Lee, J. I. Lim, S. H. Hong, S. J. Park, "Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis", Advances in Cryptology - ASIACRYPT'00, LNCS 1976, 2000, pp.274~288.

〈著者紹介〉



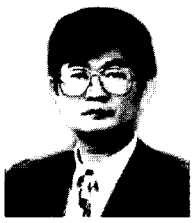
김 종 성 (Jong-Sung Kim)
2000년 8월 : 고려대학교 수학과 학사
2002년 8월 : 고려대학교 수학과 석사
2002년 8월~현재 : 고려대학교 정보보호대학원 박사 과정
<관심분야> 블록 암호 및 스트림 암호의 분석과 설계

홍 석 희 (Seok-Hie Hong)
1995년 2월 : 고려대학교 수학과 학사
1997년 2월 : 고려대학교 수학과 석사
2001년 2월 : 고려대학교 수학과 박사
2001년 3월~현재 : 고려대학교 정보보호기술연구센터 선임 연구원
<관심분야> 블록 암호 및 스트림 암호의 분석과 설계



이 상 진 (Sang-Jin Lee)
1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 8월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구소 선임 연구원
1999년 3월~현재 : 고려대학교 자연과학대학 부교수, 고려대학교 정보보호대학원 겸임교수, 고려대학교 정보 보호기술연구센터 연구실장
<관심분야> 블록 암호 및 스트림 암호의 분석과 설계, 암호 프로토콜, 공개키 암호 알고리즘 분석

임 종 인 (Jong-in Lim)
1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1999년 2월~현재 : 고려대학교 자연과학대학 정교수, 한국통신정보보호학회 편집위원장, 고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
<관심분야> 블록 암호 및 스트림 암호의 분석 및 설계. 암호 프로토콜, 공개키 암호 알고리즘의 분석, 정보보호 정책



은 희 천 (Hi-Chun Eun)
1969년 2월 : 고려대학교 수학과 학사
1974년 2월 : 고려대학교 수학과 석사
1982년 2월 : 고려대학교 수학과 박사
1982년 3월~현재 : 고려대학교 자연과학대학 수학과 교수