通信情報保護學會誌
第2卷 第4號, 1992.12

FEAL의 Differential 암호분석†

성 수 학*

1. 서 론

FEAL(Fast data Encipherment ALgorithm)은 1987년 일본 NTT에서 개발한 64비트 블럭암호로 DES보다 처리속도가 빠르고 소프트웨어 실현이 쉽다. 암호 알고리즘의 구성은 블럭암호에서 주로 채택하는 Feistel 알고리즘에 근간을 두었으며 DES에서와 같이 많은 논란이 있는 table look-up방식을 채택하지 않았다. 처음에 FEAL은 라운드 수가 4인 알고리즘이었으나, 약점이 발견되어 라운드 수를 2배로 증가한 FEAL-8을 표준알고리즘으로 채택하였다.

1988년 Den Boer는 10,000개의 chosen plaintext를 사용하여 FEAL-4 알고리즘의 키를 찾았다. 1990년 Murphy는 20개의 chosen plaintext를 이용하여 FEAL-4를 분석했다. 1991년 Tardy Corfdir와 Gilbert는 선형함수의 상관관계를 이용하여 1,000개의 평문을 사용하여 FEAL-4를 분석하였다. 1990년 Gilbert와 Guy Chasse는 differential cryptanalysis와 비슷한 방법을 사용하여 20,000개의 chosen plaintext로 FEAL-8을 분석하였다. 1991년 differential cryptanalysis의 제안자인 Biham과 Shamir는 4개의 chosen plaintext를 사용하여 FEAL-4, 2,000개의 chosen plaintext를 사용하여 FEAL-8을 분석하였고, 이 방법을 이용하면 라운드 수가 31이하인 FEAL-N은 exhaustive search보다 더 빨리 분석할 수 있다.

Differential cryptanalysis의 핵심은 확률이 큰 characteristic을 찾는 것이다. 이 문제를 해결하기 위해, FEAL의 S-box의 XOR확률 분포를 빨리 구하는 방법을 제시하였다. 또한, 확률이 큰 반복가능한 characteristic을 어떻게 찾는지를 제안하였다.

2. FEAL 알고리즘의 구조

FEAL은 2개의 처리부로 구성된다. 하나는 64비트 비밀키를 (2N+16)×8비트의 확장키로 생성하는 키생성부와, 다른 하나는 데이타를 랜덤화하는 부분이다. 64비트의 비밀키가 2N+16개의 바이트 K(0), K(1), …, K(2N+15)의 확장키로 나누어지는데, 상세한 것은 Shimizu-Miyaguchi 또는 현대암호학을 참조하기 바라며 여기서는 더 이상 언급하지 않겠다. 데이타를 랜덤화하는 부분은 3단계로 나눌 수 있다.

1) 1단계

64비트 평문의 왼쪽반을 I^0, 오른쪽 반을 I^1이라하고, X^0과 X^1은 다음과 같이 정의한다.

(I^0, I^1)=평문

† 본 연구는 한국전자통신연구소의 지원금에 의해 이루어졌습니다.

* 배재대학교 응용수학과 조교수

$X^0=I^0 \oplus \big(K(2N), K(2N+1), K(2N+2), K(2N+3)\big)$
$X^1=X^0 \oplus I^1 \oplus \big(K(2N+4),\ K(2N+5),\ K(2N+6),\ K(2N+7)\big)$

2) 2단계

64비트(X^0, X^1)은 N라운드 Feistel 알고리즘의 입력이 되며, 라운드 수를 0에서 N-1까지 움직이는 것으로 생각하자. i라운드에서 X^{i+2}는 다음과 같이 계산된다.

$$X^{i+2} = f_i(X^{i+1}) \oplus X^i$$

단, f_i는 입력값과 출력값이 32비트로 아래의 조건을 만족하는 함수이다.

$$f_i : \{0,1\}^{32} \rightarrow \{0,1\}^{32}$$
$$(X_0, X_1, X_2, X_3) \mapsto (Y_0, Y_1, Y_2, Y_3)$$
$$Y_0 = S_1\big(X_0 \oplus X_1 \oplus K(2i), X_2 \oplus X_3 \oplus K(2i+1)\big)$$
$$Y_1 = S_0(X_0, Y_1)$$
$$Y_2 = S_0\big(Y_1, X_2 \oplus X_3 \oplus K(2i+1)\big)$$
$$Y_3 = S_1(Y_2, X_3)$$
$$S_i(B_1, B_2) = Rot_2\big(B_1 + B_2 + i (mod\ 256)\big)$$

X_i, Y_i, B_i는 1바이트이고, $Rot_2(B)$는 1바이트 길이의 데이타 B를 왼쪽으로 2비트 쉬프트하는 연산이다. 함수 f_i는 1-1함수이고 2개의 확장된 키 바이트 $K(2i)$와 $K(2i+1)$에 의해 결정된다.

3) 3단계

(X^N, X^{N+1})은 마지막 라운드의 입력이고 64비트 암호문 (O^0, O^1)은 다음과 같이 계산된다.

$$O^0 = X^{N+1} \oplus \big(K(2N+8),\ K(2N+9),\ K(2N+10),\ K(2N+11)\big)$$
$$O^1 = X^N \oplus X^{N+1} \oplus \big(K(2N+12),\ K(2N+13),\ K(2N+14),\ K(2N+15)\big)$$

3. FEAL-N의 Differential 암호분석

3.1. S-box의 확률 분포

$S_i(x,y) = Rot_2(x+y+i(mod256))$(i=0 또는 1)이므로, $x+y+i(mod256)$을 계산하여 왼쪽으로 2비트 이동하면 된다. $x=(x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0)$, $y=(y_7, y_6, y_5, y_4, y_3, y_2, y_1, y_0)$을 임의의 2개의 바이트라고 하자. 그리고 $c=(c_7, c_6, c_5, c_4, c_3, c_2, c_1, c_0)$을 $x+y+i(mod256)$의 캐리라고 하자. 즉, $x+y+i(mod256) = x \oplus y \oplus c$이다. 그러면, $S_i(x,y) = Rot_2(x_7 \oplus y_7 \oplus c_7,\ x_6 \oplus y_6 \oplus c_6,\ \cdots,\ x_0 \oplus y_0 \oplus c_0) = (x_5 \oplus y_5 \oplus c_5,\ \cdots,\ x_0 \oplus y_0 \oplus c_0,\ x_7 \oplus y_7 \oplus c_7,\ x_6 \oplus y_6 \oplus c_6)$이다.

$$c_0 = 0 (x+y+0\text{일때}),\ c_0 = 1 (x+y+1\text{일때})$$
$$c_i = \begin{cases} 0, & x_{i-1} + y_{i-1} + c_{i-1} \le 1 \\ 1, & x_{i-1} + y_{i-1} + c_{i-1} \ge 2. \end{cases}$$

$\{c_i, 0 \le i \le 7\}$는 마르코프 연쇄이며, 1단계 전이확률은 다음과 같다.

정리 3.1. $\{c_i, 0 \le i \le 7\}$의 1단계 전이확률은

$$\begin{pmatrix} P(c_{i+1}=0 \mid c_i=0) & P(c_{i+1}=1 \mid c_i=0) \\ P(c_{i+1}=0 \mid c_i=1) & P(c_{i+1}=1 \mid c_i=1) \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}$$

이다. 단, $i=1, 2, \cdots, 6$이다.

증명.

$$P(c_{i+1}=0 \mid c_i=0) = \frac{P(c_i=0,\ c_{i+1}=0)}{P(c_i=0)}$$
$$= \frac{P(c_i=0,\ x_i+y_i+c_i \le 1)}{P(c_i=0)} = \frac{P(c_i=0,\ x_i+y_i \le 1)}{P(c_i=0)}$$

그런데, c_i와 $\{x_i, y_i\}$는 독립이므로,

$$\frac{P(c_i=0,\ x_i+y_i \le 1)}{P(c_i=0)} = \frac{P(c_i=0)\ P(x_i+y_i \le 1)}{P(c_i=0)}$$
$$= P(x_i+y_i \le 1) = P(x_i=0,\ y_i=0) + P(x_i=0, y_i=1)$$
$$+ P(x_i=1,\ y_i=0) = \frac{3}{4}$$

이다. 같은 방법으로 나머지 것들도 증명할 수 있다.

이젠, c_0의 분포와 $\{c_i\}$의 1단계 전이확률을 이용하여 c_i의 확률분포를 구하여 보자.

1) $x+y+0(mod256)$에서의 캐리의 확률분포
(이 경우 $c_0=0$)

$$\begin{pmatrix} P(c_1=0) \\ P(c_1=1) \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix}$$

$$\begin{pmatrix} P(c_2=0) \\ P(c_2=1) \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}^2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{10}{16} \\ \frac{6}{16} \end{pmatrix}$$

$$\begin{pmatrix} P(c_3=0) \\ P(c_3=1) \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}^3 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{36}{64} \\ \frac{28}{64} \end{pmatrix}$$

$$\begin{pmatrix} P(c_4=0) \\ P(c_4=1) \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}^4 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{136}{256} \\ \frac{120}{256} \end{pmatrix}$$

$$\begin{pmatrix} P(c_5=0) \\ P(c_5=1) \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}^5 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{528}{1024} \\ \frac{496}{1024} \end{pmatrix}$$

$$\begin{pmatrix} P(c_6=0) \\ P(c_6=1) \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}^6 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{2080}{4096} \\ \frac{2016}{4096} \end{pmatrix}$$

$$\begin{pmatrix} P(c_7=0) \\ P(c_7=1) \end{pmatrix} = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}^7 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{8256}{16384} \\ \frac{8126}{16384} \end{pmatrix}$$

2) $x+y+1(mod256)$에서의 캐리의 확률분포

이 경우는 c_0은 1만 취하고 $\{c_i\}$의 1단계 전이확률은 $x+y+0(mod256)$인 경우와 같기 때문에 $c_i=0$의 확률은 앞의 경우의 $c_i=1$의 확률과 같고, $c_i=1$의 확률은 앞의 경우의 $c_i=0$의 확률과 같다. 두 경우에서 i가 증가하면서 c_i는 일양분포에 접근함을 알 수 있다.

예 1. 2개의 랜덤한 바이트 $x=(x_7,\cdots,x_0)$, $y=(y_7,\cdots,y_0)$에 대해 다음 식이 성립한다.

(1) $x+y(mod256)=x\oplus y$ 확률 $(\frac{3}{4})^7$

(2) $x+y+1(mod256)=x\oplus y\oplus 1_x\oplus FE_x$ 확률 $(\frac{3}{4})^7$

풀이. (1) $x+y(mod256)=x\oplus y\oplus c=x\oplus y$ 이므로 $c=0$이 될 확률을 구하면 된다. c는 $x+y(mod256)$의 캐리이므로, $P(c=0)=P(c_0=0,\ \cdots,c_7=0)=P(c_0=0)\{P(c_{i+1}=0|c_i=0)\}^7=(3/4)^7$이다.

(2) $x+y+1(mod256)=x\oplus y\oplus c=x\oplus y\oplus 1_x\oplus FE_x=x\oplus y\oplus(1111\ 1111)_2$이므로, $c=(1111\ 1111)_2$가 될 확률을 구하면 된다. c는 $x+y(mod256)$의 캐리이므로, $P(c_0=1,\ \cdots,c_7=1)=P(c_0=1)\{P(c_{i+1}=1|c_i=1)\}^7=(3/4)^7$이다.

3.2. S-box의 XOR확률분포

$x=(x_7,x_6,x_5,x_4,x_3,x_2,x_1,x_0)$, $y=(y_7,y_6,y_5,y_4,y_3,y_2,y_1,y_0)$을 S-box의 입력벡터, $x^*=(x_7^*,x_6^*,x_5^*,x_4^*,x_3^*,x_2^*,x_1^*,x_0^*)$, $y^*=(y_7^*,y_6^*,y_5^*,y_4^*,y_3^*,y_2^*,y_1^*,y_0^*)$는 다른 S-box의 입력벡터, c와 c^*는 각각 $x+y+i$와 x^*+y^*+i의 캐리 벡터, $x'=x\oplus x^*$, $y'=y\oplus y^*$, $c'=c\oplus c^*$라고 하자. 그러면,

$$\begin{aligned} &S_i(x,y)\oplus S_i(x^*,y^*) \\ &= Rot_2\big(x+y+i(mod256)\oplus x^*+y^*+i(mod256)\big) \\ &= Rot_2(x\oplus y\oplus c\oplus x^*\oplus y^*\oplus c^*) \\ &= Rot_2(x'\oplus y'\oplus c') \end{aligned}$$

이다. $S_i(x,y)\oplus S_i(x^*,y^*)=S_i(x',y')$로 두면,

$$\begin{aligned} S_i(x',y') &= Rot_2(x'\oplus y'\oplus c') \\ &= (x'_5\oplus y'_5\oplus c'_5,\ \cdots,\ x'_0\oplus y'_0\oplus c'_0, \\ &\qquad x'_7\oplus y'_7\oplus c'_7,\ x'_6\oplus y'_6\oplus c'_6) \end{aligned}$$

이다. $i=0$인 경우 $c_0=c_0^*=0$이므로 $c'_0=0\oplus 0=0$이다. 또한, $i=1$인 경우도 $c_0=c_0^*=1$이므로 $c'_0=1\oplus 1=0$이다. c'_i의 확률분포는 다음과 같이 8가지 경우를 고려하여 구할 수 있다.

(1) $x'_i=0$, $y'_i=0$, $c'_i=0$ (즉, $x_i=x_i^*, y_i=y_i^*, c_i=c_i^*$)인 경우

$$c_{i+1}=\begin{cases}0, & x_i+y_i+c_i\le 1\\ 1, & x_i+y_i+c_i\ge 2\end{cases}$$

$$c^*_{i+1}=\begin{cases}0, & x_i^*+y_i^*+c_i^*\le 1\\ 1, & x_i^*+y_i^*+c_i^*\ge 2\end{cases}$$

이므로 $c_{i+1}=c^*_{i+1}$이다. 따라서, $c'_{i+1}=c_{i+1}\oplus c^*_{i+1}=0$이다.

(2) $x'_i=0$, $y'_i=0$, $c'_i=1$(즉, $x_i=x_i^*$, $y_i=y_i^*$, $c_i\neq c_i^*$)인 경우

$$P(c'_{i+1}=0|x'_i=0,\ y'_i=0,\ c'_i=1)$$

$$=\frac{P(c'_{i+1}=0,\ x'_i=0,\ y'_i=0,\ c'_i=1)}{P(x'_i=0,\ y'_i=0,\ c'_i=1)}$$

$$=\frac{P(c_{i+1}=0,\ c'_{i+1}=0,\ x'_i=0,\ y'_i=0,\ c'_i=1)}{P(x'_i=0,\ y'_i=0,\ c'_i=1)}$$

$$+\frac{P(c_{i+1}=1,\ c'_{i+1}=0,\ x'_i=0,\ y'_i=0,\ c'_i=1)}{P(x'_i=0,\ y'_i=0,\ c'_i=1)}$$

$$=\frac{P(x_i=x_i^*=0,\ y_i=y_i^*=0,\ c'_i=1)}{P(x'_i=0,\ y'_i=0,\ c'_i=1)}$$

$$+\frac{P(x_i=x_i^*=1,\ y_i=y_i^*=1,\ c'_i=1)}{P(x'_i=0,\ y'_i=0,\ c'_i=1)}$$

$$=\frac{P(x_i=x_i^*=0,\ y_i=y_i^*=0)\ P(c'_i=1)}{P(x'_i=0,\ y'_i=0)\ P(c'_i=1)}$$

$$+\frac{P(x_i=x_i^*=1,\ y_i=y_i^*=1)\ P(c'_i=1)}{P(x'_i=0,\ y'_i=0)\ P(c'_i=1)}$$

$$=\frac{1/16}{1/4}+\frac{1/16}{1/4}=\frac{1}{2}$$

따라서, $x'_i=0$, $y'_i=0$, $c'_i=1$일때, $P(c'_{i+1}=0)=P(c'_{i+1}=1)=1/2$이다.

(3) $x'_i=0$, $y'_i=1$, $c'_i=0$ (즉, $x_i=x_i^*, y_i\neq y_i^*, c_i=c_i^*$) 인 경우

(2)의 경우와 같이 계산할 수 있으며, $P(c'_{i+1}=0)=P(c'_{i+1}=1)=1/2$이다.

(4) $x'_i=1$, $y'_i=0$, $c'_i=0$ (즉, $x_i\neq x_i^*, y_i=y_i^*, c_i=c_i^*$) 인 경우

(2)의 경우와 같이 계산할 수 있으며, $P(c'_{i+1}=0)=P(c'_{i+1}=1)=1/2$이다.

(5) $x'_i=0$, $y'_i=1$, $c'_i=1$ (즉, $x_i=x_i^*, y_i\neq y_i^*, c_i\neq c_i^*$) 인 경우

$$P(c'_{i+1}=0\mid x'_i=0,\ y'_i=1,\ c'_i=1)$$

$$=\frac{P(c'_{i+1}=0,\ x'_i=0,\ y'_i=1,\ c'_i=1)}{P(x'_i=0,\ y'_i=1,\ c'_i=1)}$$

$$=\frac{P(c_{i+1}=0,\ c'_{i+1}=0,\ x'_i=0,\ y'_i=1,\ c'_i=1)}{P(x'_i=0,\ y'_i=1,\ c'_i=1)}$$

$$+\frac{P(c_{i+1}=1,\ c'_{i+1}=0,\ x'_i=0,\ y'_i=1,\ c'_i=1)}{P(x'_i=0,\ y'_i=1,\ c'_i=1)}$$

$$=\frac{P(x_i=x_i^*=0,\ y_i=0, y_i^*=1,\ c_i=1, c_i^*=0)}{P(x'_i=0,\ y'_i=1,\ c'_i=1)}$$

$$+\frac{P(x_i=x_i^*=0,\ y_i=1,\ y_i^*=0,\ c_i=0,\ c_i^*=1)}{P(x'_i=0,\ y'_i=0,\ c'_i=1)}$$

$$+\frac{P(x_i=x_i^*=1,\ y_i=0,\ y_i^*=1,\ c_i=1,\ c_i^*=0)}{P(x'_i=0,\ y'_i=1,\ c'_i=1)}$$

$$+\frac{P(x_i=x_i^*=1,\ y_i=1,\ y_i^*=0,\ c_i=0,\ c_i^*=1)}{P(x'_i=0,\ y'_i=0,\ c'_i=1)}$$

$$=2\left\{\frac{1/16\ P(c_i=1,\ c_i^*=0)}{1/4\ P(c'_i=1)}+\frac{1/16\ P(c_i=0,\ c_i^*=1)}{1/4\ P(c'_i=1)}\right\}=\frac{1}{2}$$

따라서, $x'_i=0$, $y'_i=1$, $c'_i=1$이면, $P(c'_{i+1}=0)=P(c'_{i+1}=1)=1/2$이다.

(6) $x'_i=1$, $y'_i=1$, $c'_i=0$ (즉, $x_i\neq x_i^*, y_i\neq y_i^*, c_i=c_i^*$) 인 경우

(5)의 경우와 같이, $P(c'_{i+1}=0)=P(c'_{i+1}=1)=1/2$이다.

(7) $x'_i=1$, $y'_i=0$, $c'_i=1$(즉, $x_i\neq x_i^*$, $y_i=y_i^*$, $c_i\neq c_i^*$) 인 경우

(5)의 경우와 같이, $P(c'_{i+1}=0)=P(c'_{i+1}=1)=1/2$이다.

(8) $x'_i=1$, $y'_i=1$, $c'_i=1$(즉, $x_i\neq x_i^*$, $y_i\neq y_i^*$, $c_i\neq c_i^*$) 인 경우

$$\begin{aligned}P(c'_{i+1}=0)&=P(c_{i+1}\oplus c_{i+1}^*=0)\\&=P(c_{i+1}=c_{i+1}^*=0)+P(c_{i+1}=c_{i+1}^*=1)\\&=P(c_i=0,\ c_{i+1}=c_{i+1}^*=0)\\&\quad+P(c_i=1,\ c_{i+1}=c_{i+1}^*=0)\\&\quad+P(c_i=0,\ c_{i+1}=c_{i+1}^*=1)\\&\quad+P(c_i=1,\ c_{i+1}=c_{i+1}^*=1)\\&=0\end{aligned}$$

따라서, $c'_{i+1}=1$이다.

위의 8개의 경우를 요약하면 다음표와 같다. 이 표를 이용하여 S-box의 XOR 확률분포를 쉽게 구할 수 있다.

x_i'	y_i'	c_i'	c_{i+1}'
0	0	0	0 (확률 1)
0	0	1	0 또는 1 (확률 $\frac{1}{2}$)
0	1	0	0 또는 1 (확률 $\frac{1}{2}$)
0	1	1	0 또는 1 (확률 $\frac{1}{2}$)
1	0	0	0 또는 1 (확률 $\frac{1}{2}$)
1	0	1	0 또는 1 (확률 $\frac{1}{2}$)
1	1	0	0 또는 1 (확률 $\frac{1}{2}$)
1	1	1	1 (확률 1)

예 2. $x'=80_x$, $y'=80_x$이면, $x_7'=y_7'=1$, $x_6'=y_6'=\cdots=x_0'=y_0'=0$이다. 따라서, $c_0'=c_1'=\cdots=c_7'=0$이고, $S_i(80',80')=Rot_2(x_7'\oplus y_7'\oplus c_7',\cdots,x_0'\oplus y_0'\oplus c_0')=Rot_2(0,\cdots,0)=00_x$ 이다.

예 3. $x'=01_x$, $y'=01_x$이면, $x_0'=y_0'=1$, $x_1'=y_1'=\cdots x_7'=y_7'=0$이다. $x_0'=y_0'=1$, $c_0'=0$이므로, c_1'은 0과 1이 될 확률은 각각 1/2이다. $c_1'=0$이면, $c_2'=\cdots=c_7'=0$이다. $c_1'=1$이면, c_2'는 0과 1이 될 확률은 각각 1/2이다. 계속하여 $c_3',\cdots,c_7'$을 구할 수 있다.

$$c'=(c_7',\cdots,c_0')=\begin{cases}(0000\ 0000) & \text{확률 } \frac{1}{2}\\ (0000\ 0010) & \text{확률 } \frac{1}{2^2}\\ (0000\ 0110) & \text{확률 } \frac{1}{2^3}\\ (0000\ 1110) & \text{확률 } \frac{1}{2^4}\\ (0001\ 1110) & \text{확률 } \frac{1}{2^5}\\ (0011\ 1110) & \text{확률 } \frac{1}{2^6}\\ (0111\ 1110) & \text{확률 } \frac{1}{2^7}\\ (1111\ 1110) & \text{확률 } \frac{1}{2^7}\end{cases}$$

따라서,

$$S_i(01_x',01_x')=Rot_2(x'\oplus y'\oplus c')=Rot_2(c')$$

$$=\begin{cases}00_x & \text{확률 } \frac{1}{2}\\ 08_x & \text{확률 } \frac{1}{2^2}\\ 18_x & \text{확률 } \frac{1}{2^3}\\ 38_x & \text{확률 } \frac{1}{2^4}\\ 78_x & \text{확률 } \frac{1}{2^5}\\ F8_x & \text{확률 } \frac{1}{2^6}\\ F9_x & \text{확률 } \frac{1}{2^7}\\ FB_x & \text{확률 } \frac{1}{2^7}\end{cases}$$

위의 두 예에서와 같이 S-box의 XOR 확률분포는 쉽게 구할 수 있다. Differential cryptanalysis에서 관심의 대상이 되는 것은 확률이 큰 S-box의 XOR 확률 분포를 구하는 것이다. 확률 1인 S-box의 XOR 분포는 4개 뿐이다.

정리 3.2. 확률 1인 S-box의 XOR분포는 다음과 같다.

$(i)S_i(00_x',00_x')=00_x'$, $(ii)S_i(00_x',80_x')=02_x'$
$(iii)S_i(80_x',00_x')=02_x'$, $(iv)S_i(80_x',80_x')=00_x'$

증명. $S_i(x',y')=Rot_2(x'\oplus y'\oplus c')$에서 c'이 확률 1을 가질 조건을 찾으면 된다. $c_0'=0$이므로 c_1'이 고정된 값(확률 1)을 가지기 위해서는 $x_0'=y_0'=0$이 되어야 한다. 이때, $c_1'=0$이다. 같은 방법으로 $x_1'=y_1'=0$, $\cdots$, $x_6'=y_6'=0$이 되어야 하며, 이때 $c_2'=\cdots=c_7'=0$이다. 따라서, $x'=(x_7000\ 0000)$, $y'=(y_7000\ 0000)$이고, $S_i(x',y')=Rot_2(x'\oplus y'\oplus c')=Rot_2(x'\oplus y')$이다.

3.3. 반복 가능한 Characteristic

라운드 수가 크면 확률이 큰 characteristic을 찾기가 힘든다. 이 때는 라운드가 작은 반복 가능한 characteristic을 이용하여 라운드가 큰 characteristic을 만들 수 있다.

1) 2-라운드 반복 가능한 Characteristic

2-라운드 반복 가능한 characteristic이 존재할

필요 충분조건은 적당한 α', β'에 대해 $\beta' \oplus f(\alpha') = \beta'$, $f(\beta' \oplus f(\alpha')) = 0$이다. 이 식을 정리하면, $f(\alpha') = 0$, $f(\beta') = 0$이다. 그런데, $f(\alpha') = 0$이 되는 것은 $\alpha' = 0$ 일때다. 따라서, $\alpha' = 0$, $\beta' = 0$이 되어, 2-라운드 반복가능한 characteristic(입력벡터가 0인 것은 제외)은 존재하지 않는다.

2) 3-라운드 반복 가능한 Characteristic

정리 3.3. 3-라운드 반복 가능한 characteristic이 존재할 필요충분조건은 적당한 α', β'에 대해 다음 두 식을 만족한다.

(*i*) $f(\beta' \oplus f(\alpha')) = \alpha' \oplus \beta'$

(*ii*) $\alpha' \oplus f(\alpha') = \beta' \oplus f(\beta')$

4. 결 론

FEAL의 f함수는 4개의 S-box로 구성되어 있다. 따라서, f함수의 XOR 확률 분포는 S-box의 확률 분포를 이용하여 쉽게 구할 수 있다. 확률이 큰 f 함수의 XOR 확률 분포를 이용하여 확률이 큰 반복 가능한 characteristic을 얻을 수 있다. 이것을 이용하여 N-라운드 FEAL의 복잡도를 계산할 수 있을 뿐만 아니라 differential cryptanalysis에 견디기 위한 라운드의 수 N을 결정할 수도 있다.

참 고 문 헌

1. E. Biham, A. Shamir, Differential cryptanalysis of FEAL and N-Hash, Proceedings of EUROCRYPT '91, pp.1-16, 1991.

2. B. Den-Boer, Cryptanalysis of FEAL, Proceedings of EUROCRYPT '88, pp. 293-299, 1988.

3. H. Gilbert, G. Chasse, A statistical attack of the FEAL-8 cryptosystem, Proceedings of CRYPTO '90, pp.21-32, 1990.

4. S. Murphy, The cryptanalysis of FEAL-4 with 20 chosen plaintext, Journal of Cryptography, Vol. 12, No.3, pp.145-154, 1990.

5. A. Shimizu, S. Miyaguchi, Fast data encipherment algorithm FEAL, Proceedings of EUROCRYPT '87, pp.267-278, 1987.

6. A. Tardy-Corfdir, H. Gilbert, A known plaintext attack of FEAL-4 and FEAL-6, Proceedings of CRYPTO '91, 1991.

7. 한국전자통신연구소, 현대암호학, 1991.

□ 著者紹介

成 洙 學(正會員)

1982年 慶北大學校 數學科(學士)
1985年 KAIST 應用數學科(碩士)
1988年 KAIST 應用數學科(博士)
1988年～1991年 韓國電子通信研究所 先任研究員
1991年～현재 培材大學校 應用數學科 助敎授