일반화된 Feistel 구조와 Nyberg의 가설

요 약

Nyberg는 Asiacrypt'96에서 한 라운드에 여러 개의 S-box가 작용하는 일반화된 Feistel 구조를 제안하였으나, 안전성에 대해서는 정확한 증명없이 추측만을 제시하였다. 본 논문에서는 한 라운드에 2개의 S-box가 작용하는 일반화된 Feistel 구조의 안전성을 증명한다. 또 Nyberg의 추측이 틀리다는 것도 증명한다.

Abstract

In Asiacrypt'96, Nyberg obtained an upper bound of the maximum average of differential probability for a generalized Feistel network. In this paper, we prove a counterexample to Nyberg's result is given.

1 서론

Feistel 구조를 이용하여 DES(1977) 암호가 개발된 이후, 20 여년간 Feistel 구조는 여러 사람들에 의해 연구되었으나 아직까지 구조의 취약점이 발견되지 않았다. Feistel 구조는 아주 간단하며, F 함수에 관계없이 복호화가 가능하며, S/W 및 H/W 구현이 간단하며, 처리속도가 빠르며, diffusion이 좋기 때문에 블록암호 설계시 가장 많이 사용되는 구조이다. 최근에 Feistel 구조와 유사한 구조가 많이 개발되고 있다. Matsui(1996)는 차분해독 및 선형해독 관점에서 Feistel 구조와 같은 안전성을 지니면서 병렬처리 했을 때 처리속도가 2배 빠른 유사 Feistel 구조를 개발하였다. 위에서 언급한 유사 Feistel 구조는 한 라운드에 1개의 S-box가 작용한다.

Nyberg(1996)는 한 라운드에 여러 개의 S-box가 작용하는 일반화된 Feistel 구조를 제안하였으나, 안전성에 대해서는 정확한 증명없이 추측만을 제시하였다.

본 논문에서는 Feistel 구조, Matsui의 구조에 대한 안전성을 간단히 살펴본다. 그리고 한 라운드에 2개의 S-box가 작용하는 일반화된 Feistel 구조의 안전성을 증명하며, Nyberg의 추측이 틀리다는 것도 증명한다.

2 차분해독과 선형해독

차분해독(Differential Cryptanalysis)은 Biham-Shamir(1990)에 의해 개발된 공격법이며, 선형해독(Linear Cryptanalysis)은 Matsui(1993)에 의해 개발된 공격법으로, 모두 블록암호에 적용가능한 공격법이다. 차분해독에 대한 암호 알고리즘의 안전도는 알고리즘의 최대차분확률에 의해 결정되며, 선형해독에 대한 암호 알고리즘의 안전도는 알고리즘의 최대선형확률에 의해 결정된다.

정의 1 *$F : \{0,1\}^n \to \{0,1\}^m$가 부울함수일 때 $DP^F(a \to b)$는 다음과 같이 정의한다.*

$$DP^F(a \to b) = \sharp\{x | F(x) \oplus F(x \oplus a) = b\}$$

$DP^F(a \to b)$를 입력 XOR가 a 출력 XOR가 b인 차분확률이라고 한다. 그리고 $\max_{a \neq 0, b} DP^F(a \to b)$를 간단히 $DP^F_{\max}$라고 쓰며, $DP^F_{\max}$를 F의 최대차분확률이라고 정의한다.

차분해독법을 수행하는데 필요한 복잡도(키를 찾을 때 까지의 암호화 수행 횟수)는 최대차분확률의 역수 정도이다. Feistel 형태 구조는 반복블록암호로 각 라운드에 작용하는 서브키가 독립이고 일양분포를 가지면 반복블록암호의 차분확률은 각 라운드 차분확률 곱의 합으로 쓸 수 있다.

아래 보조정리는 본 논문의 정리를 증명하는데 사용된다. 상세한 증명은 참고문헌을 참조하기 바란다[5].

보조정리 1 *$F : \{0,1\}^n \to \{0,1\}^m$가 부울함수일 때 다음이 성립한다.*

$$\sum_b DP^F(a \to b) = 1$$

특히 F가 치환이면 임의 $a(\neq 0)$에 대해 $DP^F(a \to 0) = 0$이다.

정의 2 *$F : \{0,1\}^n \to \{0,1\}^m$가 부울함수일 때 $LP^F(a \to b)$는 다음과 같이 정의한다.*

$$LP^F(a \to b) = (\frac{\#\{x|a \cdot x = b \cdot F(x)\}}{2^{n-1}} - 1)^2$$

$LP^F(a \to b)$를 선형근사확률이라고 한다. 그리고 $\max_{a,b\neq 0} LP^F(a \to b)$를 간단히 $LP^F_{\max}$라고 쓰며, $LP^F_{\max}$를 F의 최대선형근사확률이라고 정의한다.

차분특성과 선형근사는 Feistel 형태 구조에서 대칭적인 성질을 가지므로 본 논문에서는 차분해독에 대해서만 살펴보기로 한다. 본 논문을 통해 라운드에 작용하는 서브키는 독립이고 일양분포를 가지며, 그리고 각 라운드에 같은 S-box가 작용한다고 가정한다. 또 p를 S-box의 최대차분확률로 정의한다. 즉 한 라운드에 작용하는 S-box를 $F_1, \cdots, F_n$이라고 할 때

$$p = \max_{1\leq j\leq n} \max_{a\neq 0,b} DP^{F_j}(a \to b)$$

이다.

3 유사 Feistel 구조

각 라운드가 같은 구조로 이루어진 블록암호를 반복블록암호(Iterated Block Cipher)라고 한다. 대표적인 반복블록암호인 Feistel 구조의 i번째 라운드는 그림1과 같다.
i 번째 라운드의 입력을 X_1, X_2, 서브키를 K_i라고 할 때 라운드의 출력 Y_1', Y_2'은 다음과 같다.

$$Y_1 = X_1 \oplus F(X_2 \oplus K_i), \quad Y_2 = X_2$$
$$Y_1' = Y_2, \quad Y_2' = Y_1$$

Feistel 구조는 한 라운드에 작용하는 S-box인 F가 1개이다. Nyberg-Knudsen(1995)은 라운드의 수가 4 이상인 Feistel 구조의 $DP_{\max}$ 상한은 $2p^2$, 특히 F가 치환일 때 3 라운드 이상이면 $DP_{\max}$ 상한은 $2p^2$임을 증명하였다. Aoki-Ohta(1996)는 F가 치환일 때 3 라운드 이상이면 $DP_{\max}$ 상한은 p^2임을 증명하여, Nyberg-Knudsen(1995)의 결과를 개선하였다.

1996년 Matsui는 병렬로 처리했을 때 Feistel 구조보다 속도가 2배 빠른 유사 Feistel 구조를 제안하였으며, 이것을 이용하여 MISTY라는 블록암호를 설계하였다. Matsui 구조의 i 번째 라운드는 그림2와 같다.

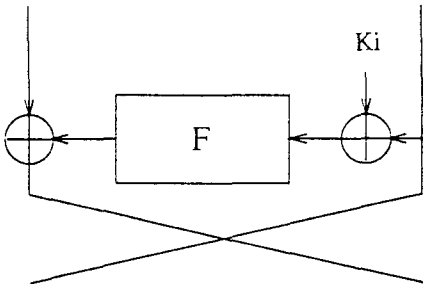

그림 1: Feistel 구조의 i번째 라운드

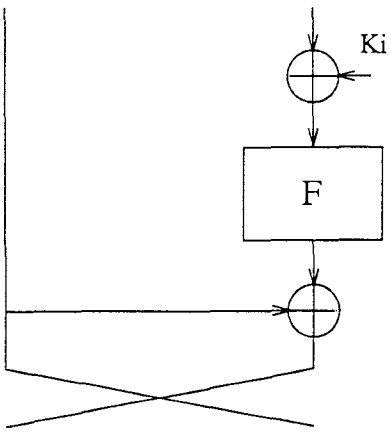

그림 2: Matsui 구조의 i 번째 라운드

Feistel 구조에서 S-box는 반드시 치환일 필요가 없으나 Matsui 구조에서는 S-box가 치환이여야 한다. 그렇치 않으면 차분해독법에 취약점이 드러날 수 있다. F가 치환일 때 3 라운드 Matsui 구조의 $DP_{\max}$ 상한은 p^2이다[5].

이제까지 살펴본 유사 Feistel 구조는 한 라운드에 작용하는 S-box의 갯수가 1개이다. 다음 절에서는 한 라운드에 작용하는 S-box의 갯수가 여러 개인 일반화된 Feistel 구조에 대해 살펴본다.

4 일반화된 Feistel 구조

한 라운드에 작용하는 F 함수가 여러 개인 구조를 일반화된 Feistel 구조(GFN, Generalized Feistel Network)라고 한다. 1996년 Nyberg는 한 라운드에 작용하는 F 함수의 갯수가 n인 일반화된 Feistel 구조를 제안하였다. i번째 라운드의 구체적인 형태를 살펴보자.

블록의 크기가 d인 $2n$개의 블록 $X_1, \cdots, X_{2n}$을 i번째 라운드의 입력이라고 하자 (알고리즘의 입력블록 크기는 $2n * d$이다). n개의 $d \times d$인 S-box를 $F_1, \cdots, F_n$이라고 하며, n개의 라운드 키를 $K_{i1}, \cdots, K_{in}$이라고 하자. 그러면 i번째 라운드의 출력 $Y'_1, \cdots, Y'_{2n}$은 다음과 같이 정의한다.

$$
\begin{aligned}
Y_{n+1-j} &= X_{n+1-j} \oplus F_j(X_{j+n} \oplus K_{ij}),\ j = 1, 2, \cdots, n \\
Y_j &= X_j,\ j = n+1, \cdots, 2n \\
Y'_1 &= Y_{2n}, \\
Y'_j &= Y_{j-1},\ j = 2, \cdots, 2n
\end{aligned}
$$

$n = 1$일 때가 바로 Feistel 구조이다. $n = 2$일 때 일반화된 Feistel 구조의 i번째 라운드는 그림4와 같다. 그리고 $n = 2$일 때 6 라운드 일반화된 Feistel 구조는 그림 5와 같다.

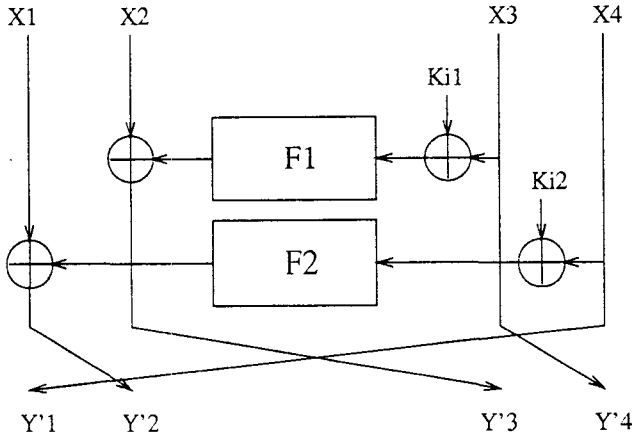

그림 3: $n = 2$일 때 일반화된 Feistel 구조의 i 번째 라운드

이젠 $n = 2$일 때 6 라운드 일반화된 Feistel 구조의 최대차분확률의 상한을 구해보자. 즉 6 라운드의 일반화된 Feistel 구조를 G라고 할 때, $DP^G_{\max} = \max_{\alpha \neq 0, \beta} DP^G(\alpha \to \beta)$의 상한을 구하기로 한다. 2절에서도 언급하였드시 라운드 키 K_{ij}는 서로 독립이고 일양분포를 갖는다. 또 일반화된 Feistel 구조에 작용하는 S-box인 F_1, F_2는 치환이라고 가정하며, S-box에 대한 최대

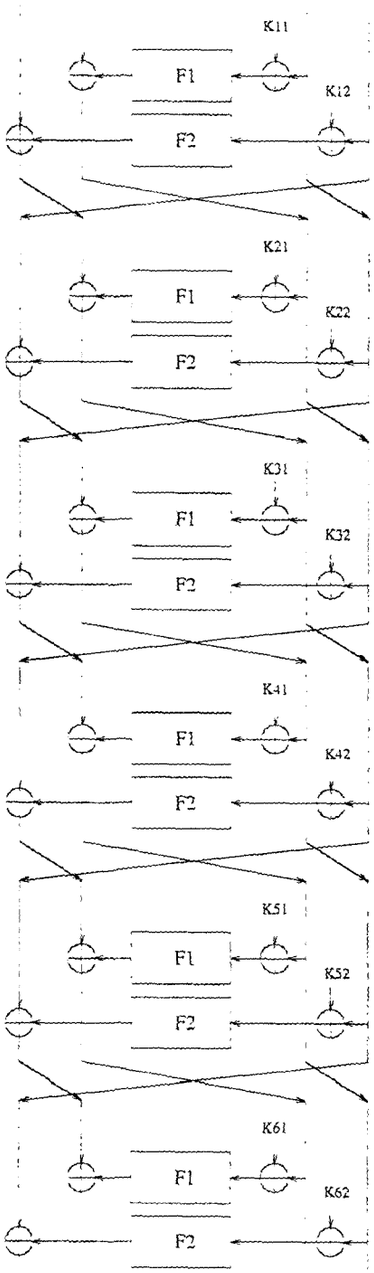

그림 4: $n = 2$일 때 6라운드 일반화된 Feistel 구조

차분확률을 p라고 쓴다. 즉

$$p = \max_{1 \le j \le 2} \max_{a \neq 0, b} DP^{F_j}(a \to b)$$

S-box인 F_1, F_2가 치환이므로 임의 $b \neq 0$에 대해 $DP^{F_i}(0 \to b) = 0$이며, 임의 $a \neq 0$에 대해 $DP^{F_i}(a \to 0) = 0$이다(보조정리 1 참조).

입력 XOR가 $\alpha = (a_1, a_2, a_3, a_4)$, 출력 XOR가 $\beta = (b_1, b_2, b_3, b_4)$인 6 라운드 일반화된 Feistel 구조 G의 차분(differential)은 다음과 같다.

a_1	a_2	a_3	a_4
c_{12}	c_{11}	a_3	a_4
a_4	c_{12}	c_{11}	a_3
c_{22}	c_{21}	c_{11}	a_3
a_3	c_{22}	c_{21}	c_{11}
c_{32}	c_{31}	c_{21}	c_{11}
c_{11}	c_{32}	c_{31}	c_{21}
c_{42}	c_{41}	c_{31}	c_{21}
c_{21}	c_{42}	c_{41}	c_{31}
c_{52}	b_3	b_4	c_{31}
c_{31}	c_{52}	b_3	b_4
b_1	b_2	b_3	b_4

첫째 행벡터 $\alpha = (a_1, a_2, a_3, a_4)$는 G의 입력 XOR이고, 마지막 행벡터 $\beta = (b_1, b_2, b_3, b_4)$는 출력 XOR이다. 직선은 블록치환을 나타내며, 두 직선 사이의 첫째 행은 그 라운드의 입력 XOR이고, 둘째 행은 블록치환 이전의 출력 XOR이다. 변수 c_{ij}는 i번째 라운드의 F_j의 출력에 의존한다. c_{ij}가 변함에 따라 입력 XOR가 α, 출력 XOR가 β인 특성(characteristic)이 되며, 가능한 c_{ij}를 모두 고려한 특성이 바로 차분이다.

위에서 구한 G의 차분을 이용하면 차분확률 $DP^G(\alpha \to \beta)$는 다음과 같다. G의 입력 XOR인 α는 0벡터가 아니라는 사실에 유의하기 바란다.

$$\begin{aligned} DP^G(\alpha \to \beta) = \sum [& DP^{F_1}(a_3 \to a_2 \oplus c_{11}) DP^{F_2}(a_4 \to a_1 \oplus c_{12}) \\ & DP^{F_1}(c_{11} \to c_{12} \oplus c_{21}) DP^{F_2}(a_3 \to a_4 \oplus c_{22}) \\ & DP^{F_1}(c_{21} \to c_{22} \oplus c_{31}) DP^{F_2}(c_{11} \to a_3 \oplus c_{32}) \\ & DP^{F_1}(c_{31} \to c_{32} \oplus b_4) DP^{F_2}(c_{21} \to c_{11} \oplus c_{42}) \\ & DP^{F_1}(b_4 \to c_{42} \oplus b_3) DP^{F_2}(c_{31} \to c_{21} \oplus c_{52}) \\ & DP^{F_1}(b_3 \to c_{52} \oplus b_2) DP^{F_2}(b_4 \to c_{31} \oplus b_1)] \end{aligned}$$

위에서 $\sum$은 변수 $c_{11}, c_{12}, c_{21}, c_{22}, c_{31}, c_{32}, c_{42}, c_{52}$의 가능한 모든 값에 대해 한 것이다. 이젠 $DP^G(\alpha \to \beta)$의 상한을 $b_3 \neq 0, b_4 \neq 0$일 때, $b_3 = b_4 = 0$일 때, $b_3 = 0, b_4 \neq 0$일 때, $b_3 \neq 0, b_4 = 0$일 때로 나누어 구해 보자.

먼저 $b_3 \neq 0, b_4 \neq 0$이라고 가정하자. $b_3 \neq 0, b_4 \neq 0$이므로

$$\begin{aligned} DP^G(\alpha \to \beta) \leq p^3 \sum [&DP^{F_1}(a_3 \to a_2 \ominus c_{11}) DP^{F_2}(a_4 \to a_1 \oplus c_{12}) \\ &DP^{F_1}(c_{11} \to c_{12} \ominus c_{21}) DP^{F_2}(a_3 \to a_4 \oplus c_{22}) \\ &DP^{F_1}(c_{21} \to c_{22} \oplus c_{31}) DP^{F_2}(c_{11} \to a_3 \oplus c_{32}) \\ &DP^{F_1}(c_{31} \to c_{32} \ominus b_4) DP^{F_2}(c_{21} \to c_{11} \oplus c_{42}) \\ &DP^{F_2}(c_{31} \to c_{21} \oplus c_{52})] \end{aligned}$$

이다. 위에서도 $\sum$은 변수 $c_{11}, c_{12}, c_{21}, c_{22}, c_{31}, c_{32}, c_{42}, c_{52}$의 가능한 모든 값에 대해 한 것이다. 이젠 위의 식에서 $\sum$ 항의 상한을 계산해 보자. 먼저 $DP^{F_1}(c_{21} \to c_{22} \oplus c_{31}) \leq 1$이라는 사실을 적용하자. 다음에 $\sum$에 변수 c_{52}을 작용하면 보조정리 1에 의해서

$$\sum_{c_{52}} DP^{F_2}(c_{31} \to c_{21} \ominus c_{52}) = 1$$

이다. 다음에 $\sum$에 변수 c_{42}을 작용하면 보조정리 1에 의해서

$$\sum_{c_{42}} DP^{F_2}(c_{21} \to c_{11} \ominus c_{42}) = 1$$

이다. 다음에 $\sum$에 변수 c_{21}을 작용하면 보조정리 1에 의해서

$$\sum_{c_{21}} DP^{F_1}(c_{11} \to c_{12} \ominus c_{21}) = 1$$

이다. 다음에 $\sum$에 변수 c_{31}을 작용하면 보조정리 1에 의해서

$$\sum_{c_{31}} DP^{F_1}(c_{31} \to c_{32} \ominus b_4) = 1$$

이다. 다음에 $\sum$에 변수 c_{32}을 작용하면 보조정리 1에 의해서

$$\sum_{c_{31}}) DP^{F_2}(c_{11} \to a_3 \ominus c_{32}) = 1$$

이다. 이젠 남은 변수 c_{11}, c_{12}, c_{22}에 대해 $\sum$을 하면 보조정리 1에 의해서

$$\sum_{c_{11}, c_{12}, c_{22}} [DP^{F_1}(a_3 \to a_2 \oplus c_{11}) DP^{F_2}(a_4 \to a_1 \oplus c_{12}) DP^{F_2}(a_3 \to a_4 \oplus c_{22})] = 1$$

이다. 따라서 $\sum$ 항은 1 이하이므로 $DP^G(\alpha \to \beta) \leq p^3$이다.

$b_3 = b_4 = 0$인 경우, $b_3 = 0, b_4 \neq 0$인 경우, $b_3 \neq 0, b_4 = 0$인 경우도 위의 경우와 같은 방법으로 증명하면 $DP^G(\alpha \to \beta) \leq p^3$이다. 여기서 상세한 증명을 생략하기로 한다.

이상의 사실을 요약하면 다음 정리를 얻을 수 있다.

정리 1 *한 라운드에 2개의 치환인 S-box가 작용하는 6 라운드 일반화된 Feistel 구조 G의 $DP^G_{\max}$의 상한은 p^3이다.*

위의 정리 1에서 $DP^G_{\max}$의 상한이 최적인지를 보기 위해 특정한 입력 XOR인 α와 출력 XOR인 β에 대해 $DP^G(\alpha \to \beta)$를 구해 보자. $\alpha = (0, a, 0, a), \beta = (a, 0, a, 0)$일 때 G의 차분은 다음과 같다.

0	a	0	a
c_{12}	a	0	a
a	c_{12}	a	0
a	0	a	0
0	a	0	a
c_{32}	a	0	a
a	c_{32}	a	0
a	0	a	0
0	a	0	a
c_{52}	a	0	a
a	c_{52}	a	0
a	0	a	0

따라서 G의 차분확률 $DP^G(\alpha \to \beta)$는 다음과 같이 계산된다.

$$DP^G(\alpha \to \beta) = \sum_{c_{12}, c_{32}, c_{52}} [DP^{F_1}(a \to c_{12}) DP^{F_2}(a \to c_{12}) \\ DP^{F_1}(a \to c_{32}) DP^{F_2}(a \to c_{32}) \\ DP^{F_1}(a \to c_{52}) DP^{F_2}(a \to c_{52})]$$

특히 S-box를 같은 것으로 사용했을 때, 즉 $F_1 = F_2 = S$일 때 $DP^G(\alpha \to \beta)$는 다음과 같다.

$$DP^G(\alpha \to \beta) = \{\sum_c (DP^S(a \to c))^2\}^3$$

이젠 구체적인 S-box에 대해 고려해 보자. 기약다항식 $x^3 + x + 1$을 갖는 Galois 체 $GF(2^3)$ 상의 S-box를 $S(x) = x^5$로 정의하자. 그러면 S-box의 XOR 분포는 다음과 같다.

입력 XOR	출력 XOR 0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	2	0	2	0	2	0	2
2	0	0	2	2	0	0	2	2
3	0	2	2	0	0	2	2	0
4	0	0	2	2	2	2	0	0
5	0	2	2	0	2	0	0	2
6	0	0	0	0	2	2	2	2
7	0	2	0	2	2	0	2	0

S-box의 XOR 분포로부터 $p = \max_{a \neq 0, b} DP^S(a \to b) = 1/4$이다. 위의 S-box를 이용하여 만든 6 라운드 일반화된 Feistel 구조 G의 차분확률 $DP^G(\alpha \to \beta)$은 다음과 같다.

$$DP^G(\alpha \to \beta) = \{\sum_{c=0}^{7} (DP^S(a \to c))^2\}^3 = (\frac{1}{4})^3 = p^3$$

따라서 이 경우 $DP^G_{\max} = \max_{\alpha \neq o, \beta} DP^G(\alpha \to \beta) = p^3$이므로 정리 1에서 구한 $DP^G_{\max}$의 상한 p^3은 최적이다.

[주] Nyberg(1996)는 한 라운드에 n개의 치환인 S-box가 작용하는 $3n$ 라운드의 일반화된 Feistel 구조의 $DP_{\max}$ 상한은 p^{2n}이라고 추측하였다. 그러나 $n = 2$일 때 $DP_{\max}$가 p^3인 6 라운드 일반화된 Feistel 구조를 위에서 설계하였으므로 Nyberg(1996)의 추측은 틀리며, 대신 다음과 같은 새로운 추측을 할 수 있다.

한 라운드에 n개의 치환인 S-box가 작용하는 $3n$ 라운드의 일반화된 Feistel 구조의 $DP_{\max}$ 상한은 p^{n+1}일 것으로 예측된다.
$n = 1, 2$일 때 위의 추측은 옳다. $n = 1$에 해당되는 것이 Aoki-Ohta(1996)의 결과이며, $n = 2$에 해당되는 것이 본 논문의 정리 1이다.

5 결론

Feistel 구조는 볼록 암호알고리즘에서 설계시 가장 많이 사용한다. Nyberg(1996)는 안전성과 효율성을 높이기 위해 한 라운드에 여러 개의 S-box가 작용하는 일반화된 Feistel 구조를 제안하였다. 그런데 Nyberg는 일반화된 Feistel 구조의 안전성에 대해 명확한 증명을 하지 않고 추측만을 제시하였다. 본 논문에서는 한 라운드에 2개의 S-box가 작용하는 일반화된 Feistel 구조의 안전성을 증명하였으며, Nyberg의 추측이 틀린다는 것도 지적하였다.

참고문헌

[1] K. Aoki and K. Ohta, Strict evaluation for the maximum average of differential probability and the maximum average of linear probability, in Proceedings of SCIS'96, SCIS96-4A, 1996.

[2] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, in Advances in Cryptology - Crypto'90(Springer, Berlin, 1991) 1-21.

[3] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, in Advances in Cryptology - Eurocrypt'94(Springer, Berlin, 1995) 356-365.

[4] M. Matsui, Linear cryptanalysis method for DES cipher, Eurocrypt'93.

[5] M. Matsui, New structure of block ciphers with provable security against differentail and linear cryptanalysis, in Fast Software Encryption(Springer, Berlin, 1996) 205-218.

[6] M. Matsui, New block encryption algorithm MISTY, 4th international workshop, Fast Software Encryption, 1997.

[7] K. Nyberg, Differentially uniform mappings for cryptography, in Advances in Cryptology - Eurocrypt'93(Springer, Berlin, 1994) 55-64.

[8] K. Nyberg, Generalized Feistel networks, in Advances in Cryptology - Asiacrypt'96(Springer, Berlin, 1996) 91-104.

[9] K. Nyberg and L. Knudsen, Provable security against a differential attack, J. Cryptology 8(1995) 27-37.