情報保護學會論文誌
第11券 第3號, 2001. 6

SPN 구조 블록 암호의 차분 공격 및 선형 공격에 대한 안전성을 측정하는 고속 알고리즘

박 상 우*, 지 성 택*, 박 춘 식*, 성 수 학**

A Fast Algorithm for evaluating the Security of Substitution and Permutation Networks against Differential attack and Linear attack

Sangwoo Park*, Seongtaek Chee*, Choonsik Park*, Soo Hak Sung**

요 약

본 논문에서는 SPN 구조 블록 암호의 안전성을 평가하는 알고리즘을 제안한다. 먼저, practical security를 이용하여 차분 공격과 선형 공격에 대한 안전성을 측정하는데 문제점이 있는 SPN 구조 블록 암호의 예를 제시한다. 다음으로, SPN 구조 블록 암호의 최대 차분 확률(maximum differential probability)과 linear hull의 최대 선형 확률(maximum linear hull probability)을 측정하는 알고리즘을 제안하고, 이 알고리즘의 수행 효율성을 높이는 가속화 방법을 제안한다. 마지막으로, 제안한 알고리즘을 사용하여 블록 암호 E2의 라운드 함수 F의 최대 차분 확률 및 linear hull의 최대 선형 확률을 계산한다.

ABSTRACT

In this paper, we examine the method for evaluating the security of SPN structures against differential cryptanalysis and linear cryptanalysis. We present an example of SPN structures in which there is a considerable difference between the differential probabilities and the characteristic probabilities. Then we propose an algorithm for estimating the maximum differential probabilities and the maximum linear hull probabilities of SPN structures and an useful method for accelerating the proposed algorithm. By using this method, we obtain the maximum differential probabilities and the maximum linear probabilities of the round function F of block cipher E2.

keyword : *블록 암호(Block ciphers), 차분 공격(Differential Cryptanalysis), 선형 공격(Linear Cryptanalysis)*

Ⅰ. 서 론

SPN(Substitution and Permutation Networks) 구조 블록 암호의 차분 공격(differential cryptanaylsis)[1~2]과 선형 공격(linear cryptanalysis)[3]에 대한 안전성은 각각 최대 차분 확률(maximum differential probability)과 linear hull의 최대 선형 확률(maximum linear probability of linear hull)을 기반으로 한다. 그러나, 일반적으로 이들 확률을 계산하는 것은 매우 어렵다. 따라서, 최대 차분 확률 대신에 최대 특성 확률(maximum characteristic probability)의 상한을 이용하며, 또한, linear hull의 최대 선형 확률 대신에 선형 근사 확률(linear approximation probability)의 상한을 이용한다. 그러나, SPN 구조 블록 암호에서는 차분 확률과 특성 확률이 크게 다를

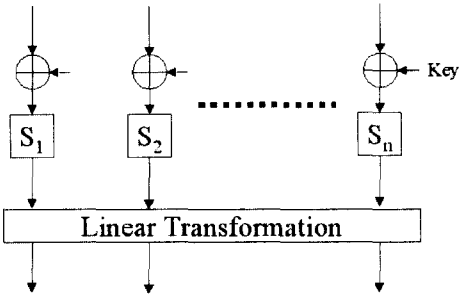
* 국가보안기술연구소((psw, chee, cspark)@etri.re.kr)
** 배재대학교 전산정보수학과(sungsh@paichai.ac.kr)

수 있으며, 또한, linear hull의 최대 선형 확률과 선형 근사 확률 역시 큰 차이를 보일 수 있다.

본 논문에서는 SPN 구조 블록 암호의 안전성을 측정하는 알고리즘을 제안한다. 먼저, 차분 확률과 특성 확률이 크게 다른 SPN 구조 블록 암호의 예를 제시한다. 이는 practical security[4~5~6~7] 관점에서 SPN 구조 블록 암호의 안전성을 평가할 때 문제점이 있을 수 있음을 시사한다. 다음으로 SPN 구조 블록 암호의 안전성을 측정하는 알고리즘을 제안한다. 제안 알고리즘에서, 차분 확률은 동일한 입력 difference와 출력 difference를 가지는 특성 확률들의 합이 된다. 또한, linear hull의 선형 확률은 동일한 입력 mask와 출력 mask를 가지는 선형 근사 확률들의 합이 된다. 그리고, 이 알고리즘의 효율성을 크게 높일 수 있는 가속화 방법을 제안한다. 마지막으로 가속화 방법을 사용한 제안 알고리즘을 이용하여 블록 암호 E2[8]의 최대 차분 확률과 최대 선형 확률을 구한다.

II. SPN 구조 블록 암호의 차분 공격 및 선형 공격에 대한 특성

SPN 구조 블록 암호의 한 라운드는 키 덧셈(key addition), 대치(substitution), 선형 변환(linear transformation)의 3 단계로 구성된다. 키 덧셈 단계는 일반적으로 라운드 키와 라운드 입력의 배타적 논리합(exclusive-or)이다. 대치 단계는 입력을 몇 개의 작은 블록으로 구분한 후에 각각의 소 블록들에 S-box라 부르는 비선형 변환을 적용하여 출력값을 얻는 과정으로 혼동(confusion) 효과를 주기 위한 단계이다. 선형 변환 단계는 대치 단계의 암호적 특성을 확산하는 단계이다. 전형적인 SPN 구조 블록 암호의 한 라운드는 (그림 1)과 같다.



(그림 1) SPN 구조 블록 암호의 한 라운드

S-box와 선형 변환은 복호화를 위하여 가역(invertible)이어야 한다. 그래서, 본 논문에서는 모든 S-box를 정의역과 공변역을 $\{0,1\}^m$으로 하는 전단사 함수로 가정한다.

S를 m 비트 입력과 출력을 가지는 S-box라 하자. S의 차분 확률 및 선형 확률은 다음으로 정의된다.

정의 1. 임의의 $a',b',a,b\in\{0,1\}^m$에 대하여 S의 차분 확률 $DP^S(a'\rightarrow b')$과 선형 확률 $LP^S(a\rightarrow b)$은 다음으로 정의된다.

$$DP^S(a'\rightarrow b')=\frac{\delta_S(a',b')}{2^m}=\frac{\#\{x\in\{0,1\}^m: S(x)\oplus S(x\oplus a')=b'\}}{2^m},$$

$$LP^S(a\rightarrow b)=\left(\frac{\lambda_S(a,b)}{2^{m-1}}\right)^2=\left(\frac{\#\{x\in\{0,1\}^m: a\cdot x=b\cdot S(x)\}}{2^{m-1}}-1\right)^2.$$

여기서, $x\cdot y$는 x와 y의 비트별 곱의 패리티(0 또는 1)을 의미한다.

a'과 b'을 각각 입력 difference와 출력 difference라 한다. 또한, a와 b를 각각 입력 mask와 출력 mask라 한다.

암호학적으로 안전한 S-box의 DP^S와 LP^S는 임의의 입력 difference $a'\neq 0$와 임의의 출력 mask $b\neq 0$에 대해 작아야 한다.

정의 2. S의 최대 차분 확률 $DP^S_{\max}$와 최대 선형 확률 $LP^S_{\max}$는 다음으로 정의된다.

$$DP^S_{max}=\max_{a'\neq 0,b'} DP^S(a'\rightarrow b')$$
$$LP^S_{max}=\max_{a,b\neq 0} LP^S(a\rightarrow b).$$

Practical measure[4~5~6~7] 관점에서 SPN 구조 블록 암호의 안전성을 측정하는 것은 기본적으로 active S-box의 개념으로부터 시작한다.

정의 3. 어떤 S-box에 임의의 0이 아닌 입력 difference가 주어졌을 때 그 S-box를 differentially active S-box라 한다. 그리고,

어떤 S-box에 임의의 0이 아닌 출력 mask 값이 주어졌을 때 그 S-box를 linearly active S-box라 한다.

대치 단계에서 사용되는 모든 S-box들은 전단사 함수이므로 S-box가 differentially active S-box이면 0이 아닌 출력 difference를 가지며, S-box가 linearly active S-box이면 0이 아닌 입력 mask 값을 가진다.

블록 암호에서 active S-box의 최소 개수를 계산하여 이로부터 차분 및 선형 확률의 상한 값을 구하는 것이 practical security 관점에서 블록 암호의 안전성을 평가하는 것이다.

다음으로 SPN 구조 블록 암호의 차분 확률 및 선형 확률을 고려한다. 우선, i번째 라운드의 선형 변환 단계 $L_i(x)$를 다음으로 표현하기로 한다.

$$L_i(x) = C_i \cdot \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix}$$

여기서, C_i는 $n \times n$ 정칙 행렬(non-singular matrix)이다. 즉, $det(C_i) \neq 0$ 이다. $L_i(x) \oplus L_i(x^*) = L_i(x \oplus x^*)$이므로 SPN 구조 블록 암호의 한 라운드의 차분 확률은 $a' = (a_1', \cdots, a_n')$와 $b' = (b_1', \cdots, b_n')$에 대해 다음으로 정의된다.

$$DP(a' \rightarrow L_i(b')) = \prod_{i=1}^{n} DP^{S_i}(a_i' \rightarrow b_i').$$

이 차분 특성(differential characteristic)을 $a' \rightarrow b' \rightarrow L_i(b')$ 으로 표기하기로 한다. r 라운드 차분 특성은 다음 집합으로 정의된다.

$$A_i' \rightarrow B_i' \rightarrow L_i(B_i') : L_i(B_i') = A_{i+1}', \quad 1 \leq i \leq r-1$$

그리고, 특성 확률은 다음과 같다.

$$\prod_{i=1}^{r} DP(A_i' \rightarrow L_i(B_i'))$$

A_1'과 $L_r(B_r')$을 각각 r 라운드 차분 특성에서의 입력과 출력이라 한다. 동일한 입력과 출력을 가지는 모든 특성들의 집합을 r라운드 차분이라 하며, 차분 확률은 동일한 입력과 출력을 가지는 특성 확률 등의 합이 된다. 즉, 차분은 특성들의 모임이라 할 수 있다.

SPN 구조 블록 암호의 선형 확률 역시 차분 확률과 유사하게 정의된다. L_i에 대응하는 선형 변환 L_i'을 다음으로 정의하자.

$$L_i'(x) = (C_i^{-1})^t \cdot \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix}$$

그러면, $LP^L(b \rightarrow L_i'(b)) = 1$이므로 한 라운드 SPN 구조 블록 암호의 선형 근사 확률은 다음으로 정의된다.

$$LP(a \rightarrow L_i'(b)) = \prod_{i=1}^{n} LP^{S_i}(a_i \rightarrow b_i).$$

이 선형 근사를 $a \rightarrow b \rightarrow L_i'(b)$로 표기하자. r라운드 선형 근사는 다음 집합으로 정의된다.

$$\{A_i \rightarrow B_i \rightarrow L_i'(B_i) : L_i'(B_i) = A_{i+1}, \ 1 \leq i \leq r-1\}.$$

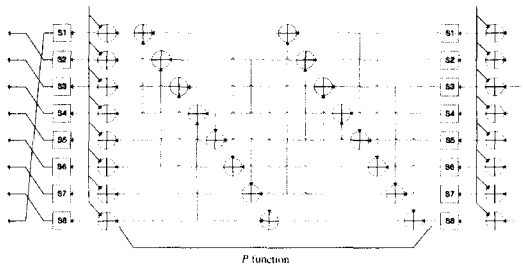
그리고, 선형 근사 확률은 다음과 같다.

$$\prod_{i=1}^{r} LP(A_i \rightarrow L_i'(B_i))$$

A_1과 $L_r'(B_r)$을 각각 r라운드 선형 근사의 입력 mask와 출력 mask라 한다. 동일한 입력 mask와 출력 mask를 가지는 모든 선형 근사들의 집합을 r라운드 linear hull이라 하며, linear hull의 선형 확률은 동일한 입력 mask와 출력 mask를 가지는 선형 근사 확률들의 합이 된다. 즉, linear hull은 선형 근사들의 집합이다.

Ⅲ. SPN 구조 안전성 평가 알고리즘

본 장에서는 SPN 구조 블록 암호의 최대 차분 확률과 linear hull의 최대 선형 확률을 평가하는 알고리즘을 제안한다. 먼저 차분 확률과 특성 확률이 큰 차이를 보이는 SPN 구조 블록 암호의 예를 제시한다. 예로서 블록 암호 E2의 라운드 함수 F를 고려한다. 단, 사용되는 S-box는 $GF(2^3)$상의 x^5로 설정한다. $GF(2^3)$상의 x^5의 difference distribution table은 [표 1]과 같다.



(그림 2) E2의 라운드 함수 F

P 함수의 입력을 $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$라 하자. 그러면, P 함수의 출력 $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8$은 다음과 같다.

〔표 1〕 $GF(2^3)$의 x^5의 difference distribution table

		b′							
		0	1	2	3	4	5	6	7
a′	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	0	2	2
	7	0	2	0	2	2	2	2	0

$$
\begin{aligned}
y_1 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \\
y_2 &= x_1 \oplus x_3 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_8 \\
y_3 &= x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_7 \oplus x_8 \\
y_4 &= x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_8 \\
y_5 &= x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6 \\
y_6 &= x_1 \oplus x_2 \oplus x_3 \oplus x_6 \oplus x_7 \\
y_7 &= x_2 \oplus x_3 \oplus x_4 \oplus x_7 \oplus x_8 \\
y_8 &= x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_8
\end{aligned}
$$

이제 라운드 함수 F의 차분 확률을 계산하자. F의 입력 difference를 (4,4,4,0,0,0,0,0), 출력 difference를 (0,0,2,0,2,0,0,0)라 하자. 〔표 1〕에서 출력 difference가 2가 되는 입력 difference는 2,3,4,5의 4 가지이다. P 함수의 입력 difference가 $(x_1, x_2, x_3, 0, 0, 0, 0, 0)$, 출력 difference가 $(0, 0, 0, y_4, 0, y_6, 0, 0)$ 이므로 $x_1 = x_2 = x_3$과 $y_4 = y_6 = x_1 \oplus x_2 \oplus x_3$이 된다. 즉, 라운드 함수 F의 차분 확률은

$$\sum_{x=2}^{5} (DP^S(4 \rightarrow x))^3 (DP^S(x \rightarrow 2))^2 = (1/4)^4$$

이 된다. 다음으로 라운드 함수 F의 특성 확률의 상한을 계산하자. 참고 문헌[9~10]에 의하면 라운드 함수 F의 differentially actice S-box의 최소 개수는 5 이다. 따라서, 특성 확률의 상한은 $(DP^S_{\max})^5 = (1/4)^5$이 되는데, 여기서, $DP^S_{\max}$는 우리가 제시하는 예제에서 E2에 원래 사용된 S-box 대신에 사용한 S-box의 최대 차분 확률이다.

본 예제에서 특성 확률의 상한은 차분 확률보다 작다. 이는 practical security 관점에서 SPN 구조 블록 암호의 안전성을 평가할 때 중요한 오류를 범할 수 있음을 시사한다.

이제 최대 차분 확률과 linear hull의 선형 확률을 평가하는 알고리즘을 제안한다.

〔최대 차분 확률 측정 알고리즘〕

〔단계 1〕 Differentially active S-box의 개수가 최소가 되는 특성을 찾는다.

〔단계 2〕 단계 1에서 찾은 특성과 동일한 입력 difference와 출력 difference를 가지는 모든 특성을 찾는다. 찾은 특성들에 대해서 각 라운드 별 differentially active S-box의 개수는 동일하여야 한다.

〔단계 3〕 단계 2에서 구한 특성 확률들의 합을 차분 확률로 설정한다.

참고 1. 제안 알고리즘에서 구한 차분 확률이 최대 차분 확률이 아닐 수 있다. 또한, linear hull의 최대 선형 확률 역시 제안 알고리즘과 유사한 방법으로 구할 수 있다.

제안 알고리즘을 E2의 라운드 함수 F의 최대 차분 확률을 구하는데 적용해 보자. E2의 라운드 함수 F의 active S-box의 최소 개수는 5임을 이미 알고 있다. E2의 라운드 함수 F는 처음 S-box들과 P 함수를 1 라운드, 다음 구조를 2 라운드로 구분할 수 있다(그림 1 참조). 즉, 라운드 함수 F는 2 라운드 SPN 구조 블록 암호로 볼 수 있다. 첫 번째로 1 라운드에서 S_4와 S_8의 2개 active S-box가 있고, 2 라운드에서는 S_1, S_4, S_5의 3개 active S-box가 있는 경우를 고려하자. 이 경우 입력 diffe-

rence는 $(0,0,0,a'_4,0,0,0,a'_8)$ 이며, 출력 difference는 $(0,0,b'_3,b'_4,0,0,0,b'_8)$이다. 또한, 차분 확률은

$$\sum_{x'=1}^{255} DP^{S_1}(a'_4 \rightarrow x')DP^{S_8}(a'_8 \rightarrow x')DP^{S_1}(x' \rightarrow b'_8) DP^{S_4}(x' \rightarrow b'_3)DP^{S_5}(x' \rightarrow b'_4). \quad (1)$$

이 된다.

식 (1)의 합을 계산하기 위하여 $a'_4, a'_8, b'_3, b'_4, b'_8$의 모든 가능한 경우를 고려하여야 하며 이는 $(256-1)^5 \approx 2^{40}$이다. 두 번째로 1 라운드에서 S_1, S_2, S_3의 3개 active S-box가 있고, 2 라운드에서 S_4, S_6의 2개 active S-box가 있는 경우를 고려한다. 이 경우에 입력 difference는 $(a'_1, a'_2, a'_3, 0,0,0,0,0)$출력 difference는 $(0,0,b'_3,0,b'_5,0,0,0)$이 되며, 차분 확률은

$$\sum_{x'=1}^{255} DP^{S_1}(a'_1 \rightarrow x')DP^{S_2}(a'_2 \rightarrow x')DP^{S_3}(a'_3 \rightarrow x') DP^{S_4}(x' \rightarrow b'_3)DP^{S_6}(x' \rightarrow b'_5) \quad (2)$$

이 된다. 식 (2)를 계산하기 위해서는 $a'_1, a'_2, a'_3, b'_3, b'_5$의 모든 가능한 경우를 고려하여야 하는데 이 양 역시 $(256-1)^5 \approx 2^{40}$이다. 즉, 라운드 함수 F의 최대 차분 확률을 구하기 위해서는 약 2^{40}의 계산이 필요하며 이는 현실적으로 계산하기 어려운 양이다. 이 문제를 해결하기 위하여 다음 장에서 가속화 방법을 제안한다.

Ⅳ. 가속화 방법

본 장에서는 앞장에서 제안한 알고리즘의 효율성을 높히는 유용한 방법을 제안한다.

보조정리 1. 실수 $x_i^{(j)}, 1 \le j \le m, 1 \le i \le N$ 에 대해서 다음 부등식이 성립한다.

$$\sum_{i=1}^{N}|x_i^{(1)}x_i^{(2)}\cdots x_i^{(m)}| \le \left(\sum_{i=1}^{N}|x_i^{(1)}|^m\right)^{1/m}\left(\sum_{i=1}^{N}|x_i^{(2)}|^m\right)^{1/m}\cdots\left(\sum_{i=1}^{N}|x_i^{(m)}|^m\right)^{1/m}$$

(증명) 수학적 귀납법을 이용하여 증명한다. m=1인 경우에는 부등식은 자명하게 성립한다. m에 대하여 부등식이 성립한다고 가정하고 다음의 Holder 부등식을 적용한다.

$$\sum_{i=1}^{N}|x_i^{(1)}x_i^{(2)}\cdots x_i^{(m)}x_i^{(m+1)}| \le \left(\sum_{i=1}^{N}|x_i^{(1)}x_i^{(2)}\cdots x_i^{(m)}|^{\frac{m+1}{m}}\right)^{\frac{m}{m+1}}\left(\sum_{i=1}^{N}|x_i^{(m+1)}|^{m+1}\right)^{\frac{1}{m+1}}$$

귀납법의 가정에 의하여 부등식의 좌변은 다음에 의해 유계(bounded)된다.

$$\left(\sum_{i=1}^{N}|x_i^{(1)}|^{m+1}\right)^{\frac{1}{m+1}}\cdots\left(\sum_{i=1}^{N}|x_i^{(2)}|^{m+1}\right)^{\frac{1}{m+1}} \left(\sum_{i=1}^{N}|x_i^{(m)}|^{m+1}\right)^{\frac{1}{m+1}}\left(\sum_{i=1}^{N}|x_i^{(m+1)}|^{m+1}\right)^{\frac{1}{m+1}}.$$

따라서, 부등식이 성립한다.

정리 1. 실수 $x_i^{(j)}, y_i^{(k)}, 1 \le j \le m, 1 \le k \le n, 1 \le i \le N$ 에 대하여 다음 부등식이 성립한다.

$$\sum_{i=1}^{N}|x_i^{(1)}x_i^{(2)}\cdots x_i^{(m)}y_i^{(1)}y_i^{(2)}\cdots y_i^{(n)}| \le \max\left\{\sum_{i=1}^{N}|x_i^{(1)}|^{m}|y_i^{(1)}|^{n},\cdots,\sum_{i=1}^{N}|x_i^{(m)}|^{m}|y_i^{(n)}|^{n}\right\}$$

(증명) 좌변은 다음으로 다시 표현할 수 있다.

$$\sum_{i=1}^{N}[|x_i^{(1)}|^{1/n}|y_i^{(1)}|^{1/m}|x_i^{(1)}|^{1/n}|y_i^{(2)}|^{1/m}\cdots|x_i^{(1)}|^{1/n}|y_i^{(n)}|^{1/m} |x_i^{(2)}|^{1/n}|y_i^{(1)}|^{1/m}|x_i^{(2)}|^{1/n}|y_i^{(2)}|^{1/m}\cdots|x_i^{(2)}|^{1/n}|y_i^{(n)}|^{1/m}\cdots |x_i^{(m)}|^{1/n}|y_i^{(1)}|^{1/m}|x_i^{(m)}|^{1/n}|y_i^{(2)}|^{1/m}\cdots|x_i^{(m)}|^{1/n}|y_i^{(n)}|^{1/m}$$

보조 정리 1에 의하여 위 식은 다음으로 유계된다.

$$\left[\sum_{i=1}^{N}|x_i^{(1)}|^{m}|y_i^{(1)}|^{n}\sum_{i=1}^{N}|x_i^{(1)}|^{m}|y_i^{(2)}|^{n}\cdots\sum_{i=1}^{N}|x_i^{(1)}|^{m}|y_i^{(n)}|^{n} \sum_{i=1}^{N}|x_i^{(2)}|^{m}|y_i^{(1)}|^{n}\sum_{i=1}^{N}|x_i^{(2)}|^{m}|y_i^{(2)}|^{n}\cdots\sum_{i=1}^{N}|x_i^{(2)}|^{m}|y_i^{(n)}|^{n} \sum_{i=1}^{N}|x_i^{(m)}|^{m}|y_i^{(1)}|^{n}\sum_{i=1}^{N}|x_i^{(m)}|^{m}|y_i^{(2)}|^{n}\cdots\sum_{i=1}^{N}|x_i^{(m)}|^{m}|y_i^{(n)}|^{n}\right]^{1/mn}$$

위 식은 다시 다음으로 유계된다.

$$\max \left\{ \sum_{i=1}^{N} |x_i^{(1)}|^{m} |y_i^{(1)}|^{n}, \cdots, \sum_{i=1}^{N} |x_i^{(m)}|^{m} |y_i^{(n)}|^{n} \right\}$$

이제, 정리 1을 사용하여 라운드 함수 F의 최대 차분 확률을 계산한다. 정리 1에 의하면 식 (1)의 상한은 다음이 된다.

$$\max_{a',b'} \sum_{x=1}^{255} \{DP^S(a' \rightarrow x')\}^2 \{DP^S(x' \rightarrow b')\}^3. \quad (3)$$

라운드 함수 F의 모든 S-box는 동일하므로 정리 1에 의해 구한 상한은 최대값이 된다. 그러나, 서로 다른 S-box가 사용되었다면 정리 1에 의하여 구한 상한은 일반적으로 최대값이 아닐 수 있다. 모든 가능한 경우의 a와 b에 대하여 식 (3)의 합을 구하기 위해서는 $(256-1)^2$의 경우만 고려하면 되고 이 양은 컴퓨터 계산을 이용하여 계산 가능한 양이다. 컴퓨터 시뮬레이션에 의하여 최대 차분 확률은 $a' = 84_x$과 $b' = 1b_x$일 때 $56,960/(256)^5$이다.

즉, 차분 특성

$(0,0,0,84_x,0,0,0,84_x) \rightarrow (0,0,1b_x,1b_x,0,0,0,1b_x)$

의 확률은

$(0,0,0,a'_4,0,0,0,a'_8) \rightarrow (0,0,b'_3,b'_4,0,0,0,b'_8)$

형태의 차분 특성들 중에서 $56,960/(256)^2$을 최대값으로 가진다. 이 계산은 표 2와 표 3을 이용하여 구할 수 있다. 라운드 함수 F의 모든 S-box들이 동일하므로 최대 차분 확률은 차분의 형태가 다를지라도 모두 동일하다.

〔표 2〕 $\delta_S(84_x, b'_x)$의 분포

2	1,2,9,a,b,15,1d,1e,1f,20,23,26,2b,2c,31,33,35,3a,3c,40,58,5c,5e,5f,65,66,6b,72,74,78,7a,84,85,88,91,95,96,97,9b,9c,9f,a0,a2,a8,aa,ac,ad,b0,b1,b2,b5,b7,ba,be,bf,c0,c3,c8,c9,ce,d0,db,dd,de,df,e0,e1,ee,f0,f1,f2,f6,fb,fc,fe,ff
4	d,14,16,2f,30,3b,45,56,67,6a,a4,ab,b4,d4,d6,d9,e8
6	3d,49,57
8	cf
10	f3

〔표 3〕 $\delta_S(a'_x, 1b_x)$의 분포

2	3,a,b,11,19,1c,1f,21,23,25,26,2d,30,32,34,36,3a,3d,3f,40,41,47,4b,4c,4e,4f,53,54,55,56,5b,5d,5f,62,63,64,67,6c,6d,6e,75,7b,7c,7d,7e,80,81,83,88,8a,8c,97,9b,9f,a1,a2,a3,a7,ab,b4,bd,be,bf,c1,c3,c6,c9,ca,ce,d1,e5,e7,e9, ed,ef,f5,f9,fb,fd,fe
4	1,5,18,1b,43,45,65,66,87,98,99,a4,b9,bb,cd,db,ec,f0,f8
6	20,c2
8	f3

다음으로 1 라운드에서 3개의 active S-box, 2 라운드에서 2개의 active S-box가 있는 경우의 최대 차분 확률을 계산하자. 정리 1에 의하면 식 (2)의 상한은

$$\max_{a',b'} \sum_{x=1}^{255} \{DP^S(a' \rightarrow x')\}^3 \{DP^S(x' \rightarrow b')\}^2$$

이 된다. $a' = 84_x$과 $b' = 1b_x$일 때 식 (4)는 최대값을 가진다. 따라서, 차분 특성

$$(84_x, 84_x, 84_x, 0,0,0,0,0) \rightarrow (0,0,1b_x,0,1b_x,0,0,0)$$

은 최대 차분 확률 69,760/(256)5을 가진다.

이상에서 E2의 라운드 함수 F의 최대 차분 확률은 $69,760/(256)^5$임을 계산하였다. 유사하게, 선형 변환을 L 대신에 L'을 사용하여 linear hull의 최대 선형 확률을 구할 수 있다. 1 라운드에서 2개의 active S-box, 2 라운드에서 3개의 active S-box가 있는 경우에는 최대 선형 확률은

$$\sum_{x=1}^{255} (LP^S(b_x \rightarrow x))^2 (LP^S(x \rightarrow 56_x))^3 \approx 190,827/(256)^5$$

이 된다. 1 라운드에서 3개의 active S-box, 2 라운드에서 2개의 active S-box가 있는 경우에는 최대 선형 확률은

$$\sum_{x=1}^{255} (LP^S(b_x \rightarrow x))^3 (LP^S(x \rightarrow 56_x))^2 \approx 218,225/(256)^5$$

이 된다. 따라서, 최대 선형 확률은 $218,225/(256)^5$

이 된다.

참고 2. E2의 설계자들은 컴퓨터 시뮬레이션을 통하여 라운드 함수 F의 최대 차분 확률의 근사값이 $2^{-23.91}$이고 최대 선형 확률의 근사값이 $2^{-22.26}$ 임을 제시한 바 있다.

V. 결 론

본 논문에서는 최대 차분 확률과 linear hull의 최대 선형 확률을 평가하는 알고리즘을 제안하였다. 최대 차분 확률을 계산하기 위하여 첫번째로 differentially active S-box의 개수가 최소인 특성을 찾고 찾은 특성과 동일한 입력 difference와 출력 difference를 가지는 모든 특성을 찾는다. 다음으로, 찾은 특성들의 합으로 최대 차분 확률을 계산한다. 이 과정의 효율성을 높히는 가속화 방법을 제안하였다. 유사한 방법으로 linear hull의 최대 선형 확률을 구할 수 있다. 가속화 방법을 적용한 제안 알고리즘을 사용하여 블록 암호 E2의 라운드 함수 F의 최대 차분 확률과 최대 선형 확률을 구하였다.

참 고 문 헌

[1] Eli Biham and Adi Shamir. Differential cryptanalysis of {DES}-like cryptosystem. In Alfred J. Menezes and Scott A. Vanstone, editors, Advances in Cryptology - Crypto'90, volume 537 of Lecture Notes in Computer Science, pages 2--21. Springer-Verlag, Berlin, 1991.

[2] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, volume 4, number 1, pages 3--72, 1991.

[3] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, Advances in Cryptology -Eurocrypt'93, volume 765 of Lecture Notes in Computer Science, pages 386-397. Springer-Verlag, Berlin, 1994.

[4] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher square. In Eli Biham, editor, Fast Software Encryption, volume 1267 of Lecture Notes in Computer Science, pages 149--165. Springer, 1997.

[5] Howard M. Heys and Stafford E. Tavares. Substitution-permutation networks resistant to differential and linear cryptanalysis. Journal of Cryptology, volume 9, number 1, pages 1-19, 1996.

[6] Lars R. Knudsen. Practically secure feistel ciphers. In Ross Anderson, editor, Fast Software Encryption, Cambridge Security Workshop, volume 809 of Lecture Notes in Computer Science, pages 211--221. Springer-Verlag, Berlin, 1994.

[7] Vincent Rijmen, Joan Daemen, Bart Preneel, Anton Bosselaers, and Erik De Win. The cipher shark. In Dieter Gollman, editor, Fast Software Encryption, Third International Workshop, volume 1039 of Lecture Notes in Computer Science, pages 99--112. Springer, 1996.

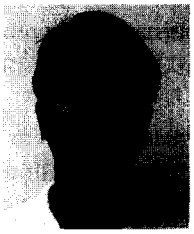
[8] NTT-Nippon Telegraph and Telephone Corporation. E2: Efficient Encryption algorithm, AES Proposal, 1998.

[9] Masayuki Kanda, Youichi Takashima, Tsutomu Matsumoto, Kazumaro Aoki, and Kazuo Ohta. A strategy for constructing fast round functions with practical security against differential and linear cryptanalysis. In Stafford Tavares and Henk Meijer, editors, 5th Annual International Workshop, SAC'98, volume 1556 of Lecture Notes in Computer Science, pages 264--279. Springer, 1998.

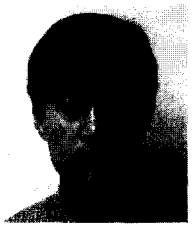
[10] Ju-Sung Kang, Choonsik Park, Sangjin Lee, and Jong-In Lim. On the optimal diffusion layers with practical security against differential and linear cryptanalysis. In JooSeok Song, editor,

Information Security and Cryptology - ICISC'99, volume 1787 of Lecture Notes in Computer Science, pages 38--52. Springer, 1999.

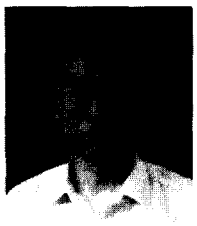
〈著者紹介〉



박 상 우(Sangwoo Park) 정회원
1989년 2월 : 고려대학교 수학교육과 졸업
1991년 8월 : 고려대학교 수학과 석사
1991년 8월~1999년 12월 : 한국전자통신연구원 선임연구원
2000년 1월~현재 : 국가보안기술연구소 선임연구원



지 성 택(Seongtaek Chee) 정회원
1985년 2월 : 서강대학교 수학과 졸업
1987년 2월 : 서강대학교 수학과 석사
1999년 2월 : 고려대학교 수학과 박사
1989년 ~1999년 12월 : 한국전자통신연구원 선임연구원
2000년 1월~현재 : 국가보안기술연구소 책임연구원



박 춘 식(Choonskip Park) 정회원
광운대학교 전자통신과 졸업(학사)
한양대학교 대학원 전자통신과 졸업(석사)
일본 공격동업대학 졸업(암호학 전공, 공학박사)
1989년 10월~1990년 9월 : 일본 공격공업대학 객원 연구원
1989년~1999년 12월 : 한국전자통신연구원 책임연구원
2000년 1월~현재 : 국가보안기술연구소 책임연구원

성 수 학(Soo Hak Sung) 정회원
1982년 2월 : 경북대학교 수학과(학사)
1985년 2월 : KAIST 응용수학과(석사)
1988년 2월 : KAIST 응용수학과(박사)
1988년~1991년 : 한국전자통신연구원 선임연구원
1991년~현재 : 배재대학교 전산정보수학과 교수