論文 95-12-12-14

정보누설 기준에 대한 고찰과 S-box의 설계

正會員 李 周 鎬*, 金 炯 明*

A Study on the Information Leakage Criterion and the Design of S-boxes

Ju Ho Lee*, Hyung Myung Kim* Regular Members

要 約

이 논문에서는 특정한 경우의 정보누설량을 0으로 하기 위해 S-box를 구성하는 Boolean 함수가 만족해야 하는 조건을 Walsh 변환을 이용하여 유도하였다. 그러한 조건들간의 관계를 고찰함으로써 정보누설 기준은 정보누설이 큰 S-box를 걸러내는 역할을 하는 것이 바람직함을 알 수 있었다. 또한 Data Encryption Standard (DES)의 구조 및 DES에 대한 암호분석 그리고 정보누설을 고려하여 S-box 설계 기준을 선정하고 이에 의해 구성된 8개의 S-box를 이용하는 LDES를 제안한다. LDES의 분석 결과는 이 논문에서 제안하는 설계 기준이 DES의 안전도를 강화하는 S-box를 구성할 수 있음을 보여주고 있다.

ABSTRACT

Using Walsh transform, we derive a set of conditions under which the information leakage of S-box reduces to zero in particular cases. And then we observe that it is desirable for the information leakage criterion to discard the S-boxes which have significant information leakage. We set up the S-box design criteria considering the structure of Data Encryption Standard (DES), the cryptanalysis of DES, and the information leakage. And we suggest LDES using 8 S-boxes designed using the proposed criteria. Analysis results of LDES show that the proposed S-box design criteria can produce S-boxes which strengthen the security of DES.

* 한국과학기술원 전기 및 전자공학과
論文番號 : 95084-0225
接受日字 : 1995年 2月 25日

Ⅰ. 서 론

현대 사회가 고도 정보화 사회로 발전해감에 따라 정보보호의 중요성은 점차 커지고 있다. 정보보호를 위한 가장 효율적이고 경제적인 방법은 암호시스템을 구성하는 것이다. Shannon은 confusion과 diffusion의 개념에 기초하여 강력한 암호 알고리즘을 얻기 위한 방법으로 Substitution-Permutation network (SP network)을 제안하였는데[1], 블럭 (block)단위로 암호화 및 복호화를 수행하는 블럭 암호시스템은 대부분 SP network의 구조에 기초를 두고 있다[2,3,4]. SP network는 치환 (substitution)과 전위 (permutation)의 반복으로 이루어지며, 치환과 전위는 각각 confusion과 diffusion을 제공한다. 치환은 일반적으로 S-box라고 불리며, SP network에 기초한 암호시스템의 안전도는 유일한 비선형 연산인 S-box에 크게 의존하게 된다.

현재 가장 널리 쓰이고 있는 블럭 암호시스템인 Data Encryption Standard (DES)는 SP network에 기초한 암호시스템으로 Feistel cipher[5]의 구조로 구성되어 있으며, 1977년 미국 상무성 표준국 (NBS)에 의해 상용암호표준으로 채택되었다[2]. 최근에 DES를 공략하는데 성공하고 있는 암호분석 방법으로는 differential 암호분석[6,7]과 선형 암호분석[8,9]이 있으며, 이로 인해 DES를 개선해야할 필요성이 커지고 있다. 따라서 DES를 구성하는 요소중 가장 핵심적인 S-box에 관한 연구의 필요성이 증가하고 있다.

Dawson은 정보누설의 관점에서 S-box를 설계할 것을 제안하였다[10]. 정보누설 기준은 S-box의 입력 혹은 출력에 관한 부분적인 정보에 의해 알지 못하는 출력의 불확실성이 감소하는 양 즉 정보누설량 (information leakage)을 측정하여 S-box를 평가한다. 정보누설의 관점에서 이상적인 S-box는 입력에 관한 정보가 완전히 주어져 있지 않을 때 정보누설이 전혀 없는 것이다.

이 논문에서는 특정한 경우의 정보누설량을 0으로 하기 위해 S-box를 구성하는 Boolean 함수가 만족해야 하는 조건을 Walsh 변환을 이용하여 유도하고, 그러한 조건들간의 관계를 고찰함으로써 정보누설 기준이 어떤 역할을 해야할지를 결정한다. 또한 DES의 구조 및 DES에 대한 암호분석 그리고 정보누설을 고려하여 S-box 설계 기준을 선정하고, 실제 설계된 8개의 S-box로 DES S-box를 대신하는 LDES를 제안한다.

이 논문의 구성은 다음과 같다. 2장에서는 DES S-box의 알려진 설계 기준을 살펴본다. 3장에서는 정보누설 기준의 역할에 대해 고찰한다. 4장에서는 S-box 설계 기준을 설정하고 이에 따라 DES에 쓰일 수 있는 6×4 S-box를 설계하며, 끝으로 5장에서 결론을 맺는다.

Ⅱ. DES S-box의 설계 기준

그림 1에서 DES의 각 라운드 (round)에서 사용되는 암호화 함수 F의 구조를 보인다. 암호화 함수 F는 32비트의 데이타 블럭과 48비트의 라운드키 (round key)를 입력으로 하며 32비트 블럭을 출력한다. F 함수는 선형 연산인 비트선택표 E와 전위 P, 그리고 DES에서 유일하게 비선형 연산인 8개의 S-box로 구성되어 있다.

각 S-box는 6비트 입력과 4비트 출력을 가지며 (4×16)의 행렬 형태로 구성되어 있는데, 각 행은 0, …, 15에 대한 가역적인 치환이다. S-box S의 6비트 입력을 $\boldsymbol{x} = x_5x_4\cdots x_0$라 하면, 행 번호 $i = x_5x_0$와 열 번호 $j = x_4x_3x_2x_1$에 의해 4비트 출력 $S(\boldsymbol{x})$가 결정된다. DES S-box와 같은 형태의 $m\times n(m\geq n)$ S-box를 regular[11] S-box라고 한다. DES에 사용되는 S-box의 발표된 설계 기준은 다음과 같다[11].

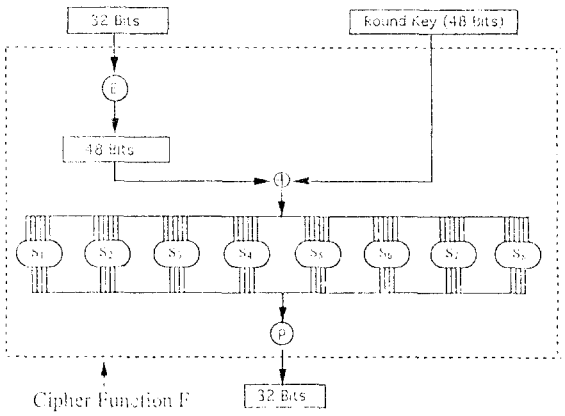

그림 1. 암호화 함수 F의 구조
Fig. 1. Structure of cipher function F

P0. S-box의 각 행은 0, …, 15의 정수에 대한 치환이다.

P1. 어떤 S-box도 선형[2]이거나 affine[3] 함수가 아니다.

P2. S-box의 6개의 입력비트들 중 하나의 비트값을 바꾸면, 적어도 2개 이상의 출력 비트가 바뀐다.

P3. $S(\boldsymbol{x})$와 $S(\boldsymbol{x}\oplus 001100)$은 적어도 2비트 이상이 달라야 한다.

P4. 임의의 e, $f(e, f\in Z_2)$에 대해 $S(\boldsymbol{x})\neq S(\boldsymbol{x}\oplus 11ef00)$이다.

P5. 한 개의 입력비트값을 고정하였을 때 S-box의 어떤 출력비트에서도 0과 1의 차이가 최소화되도록 S-box를 선택한다.

Ⅲ. 정보누설 기준

SP network에 기초한 DES류의 암호시스템에서 사용되는 S-box는 그 구조가 고정되어 있기 때문에 입력을 완전히 아는 것은 출력을 완전히 아는 것과 동일하다. 그러나, S-box의 역할이 confusion을 제공하는 것이기 때문에 입력 혹은 출력에 관한 부분적인 정보에 의해 알려지지 않은 출력의 불확실성이 감소하는 양을 되도록 작게 해야 한다[12]. 정보누설 기준은 입력 혹은 출력에 관한 부분적인 정보에 의해 알려지지 않은 출력의 불확실성이 감소하는 양을 측정하여 S-box를 평가하며, 불확실성이 감소하는 양을 정보누설량이라 한다. 이후의 논의에서 $m\times n$ S-box는 n개의 m비트 입력 Boolean 함수로 이루어진 m비트 입력과 n비트 출력사이의 변환을 뜻하며 그림 2와 같이 표현할 수 있다. 이때, 비트 0은 LSB를 뜻하며, n개의 출력비트를 구성하는 Boolean 함수는 LSB부터 f_0, f_1, …, f_{n-1}로 표시한다.

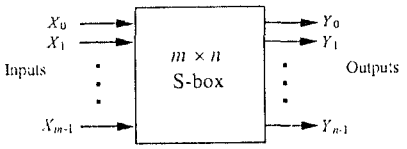

그림 2. m×n S-box
Fig. 2. m×n S-box

1. 정보누설량의 정의

$m\times n(m\geq n)$ S-box의 정보누설은 크게 정적 관점(static view)과 동적 관점 (dynamic view)에서 생각할 수 있다[10]. 정적 관점은 입력이 변화하지 않을 때 알고 있는 부분적인 정보에 의해 S-box 출력의 불확실성이 감소하는 현상을 묘사한다. 동적 관점은 입력이 변화하는 경우, 입력의 변화 혹은 출력의 변화에 대한 부분적인 정보에 의해 S-box 출력 변화의 불확실성이 감소하는 현상을 묘사한다. 이 때, 일반적으로 현재의 입력은 알지 못한다고 가정한다. 정보누설을 논할 때, S-box의 입력비트 X_0, X_1, …, X_{m-1}과 입력비트의 변화 ΔX_0, ΔX_1, …, ΔX_{m-1}은 각각 0 혹은 1을 가질 확률이 $\frac{1}{2}$이며 서로 독립적인 확률변수 (random variable)로 가정한다. 또한 S-box의 출력비트 Y_0, Y_1, …, Y_{n-1}과 출력비트 변화 ΔY_0, ΔY_1, …, ΔY_{n-1}도 확률변수로 취급한다. 이제 $m\times n(m\geq n)$ S-box를 정보누설 관점에서 평가하기 위해 필요한 정보누설량들을 정의한다[13,14].

(1) Static Input-Output Information Leakage (SL(I;O))

k개의 입력비트로 구성된 랜덤벡터 (random vector) $\boldsymbol{X_k}$가 $\boldsymbol{x_k}$로 주어진 경우 t개의 출력비트로 구성된 랜덤벡터 $\boldsymbol{Y_t}$의 정보누설량 $SL(\boldsymbol{Y_t}|\boldsymbol{X_k}=\boldsymbol{x_k})$은 다음과 같이 정의한다.

$$SL(\boldsymbol{Y_t}|\boldsymbol{X_k}=\boldsymbol{x_k}) = t-H(\boldsymbol{Y_t}|\boldsymbol{X_k}=x_k) \quad (1)$$
$$\boldsymbol{X_k} = (X_{j_1}, X_{j_2}, \cdots, X_{j_k}),\ 1\leq k\leq m-1$$
$$\boldsymbol{Y_t} = (Y_{l_1}, Y_{l_2}, \cdots, Y_{l_t}),\ 1\leq t\leq n$$

1) m×n(m≥n) regular S-box는 $2^{m}!$개의 n×n bijective S-box로 이루어진다.
2) $Z_2^m(Z_2=\{0,1\})$에서 정의되는 Boolean 함수 f가 선형이라면 f는 다음과 같다.
$f(\boldsymbol{x}) = a_0x_0\oplus a_1x_1\oplus\cdots\oplus a_{m-1}x_{m-1},\ a_i\in\{0,1\},\ i=0,\cdots,m-1$
3) Z_2^m에서 정의되는 Boolean 함수 f가 affine이라면 f는 다음과 같다.
$f(\boldsymbol{x}) = 1\oplus a_0x_0\oplus a_1x_1\oplus\cdots\oplus a_{m-1}x_{m-1},\ a_i\in\{0,1\},\ i=0,\cdots,m-1$

$j_1, j_2, \cdots, j_k \in \{0, 1, \cdots, m-1\}$,
$l_1, l_2, \cdots, l_t \in \{0, 1, \cdots, n-1\}$

$SL(\boldsymbol{Y}_t|\boldsymbol{X}_k = \boldsymbol{x}_k)$는 m비트 입력 중 특정한 k비트가 알려지는 경우에 n비트 출력에서 선택된 t개의 출력비트의 불확실성의 감소량을 측정한다. 단, $k=m$인 경우는 입력을 완전히 아는 경우이기 때문에 제외한다. 입력비트들을 독립적인 확률변수로 가정하기 때문에 $\boldsymbol{X}_k$와 $\boldsymbol{Y}_t$사이의 정보누설량 $SL(\boldsymbol{Y}_t|\boldsymbol{X}_k)$은 다음과 같다.

$$SL(Y_t|X_k) = 2^{-k} \sum_{x_k \in Z_2^k} SL(Y_t|X_k = x_k) \quad (2)$$

(2) Dynamic Input-Output Information Leakage (DL[I:O])

k개의 입력비트의 변화로 구성된 랜덤벡터 $\Delta\boldsymbol{X}_k$가 $\Delta\boldsymbol{x}_k$로 알려진 경우 t개의 출력비트의 변화로 구성된 랜덤벡터 $\Delta\boldsymbol{Y}_t$의 정보누설량 $DL(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{X}_k = \Delta\boldsymbol{x}_k)$은 다음과 같이 정의한다.

$$DL(\Delta Y_t|\Delta\boldsymbol{X}_k = \Delta\boldsymbol{x}_k) = t - H(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{X}_k = \Delta\boldsymbol{x}_k) \quad (3)$$
$\Delta\boldsymbol{X}_k = (\Delta X_{j_1}, \Delta X_{j_2}, \cdots, \Delta X_{j_k}),\ 1 \le k \le m$
$\Delta\boldsymbol{Y}_t = (\Delta Y_{l_1}, \Delta Y_{l_2}, \cdots, \Delta Y_{l_t}),\ 1 \le t \le n$
$j_1, j_2, \cdots, j_k \in \{0, 1, \cdots, m-1\}$,
$l_1, l_2, \cdots, l_t \in \{0, 1, \cdots, n-1\}\}$

$DL(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{X}_k = \Delta\boldsymbol{x}_k)$는 m비트 입력의 변화 중 특정한 k비트의 변화가 알려지는 경우에 n비트 출력에서 선택된 t개의 출력비트 변화의 불확실성의 감소량을 측정한다. 현재 입력을 모른다고 가정하기 때문에 $k=m$인 경우도 포함한다. 입력비트의 변화 역시 독립적인 확률변수로 가정하기 때문에 $\Delta\boldsymbol{X}_k$와 $\Delta\boldsymbol{Y}_t$사이의 정보누설량 $DL(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{X}_k)$은 다음과 같다.

$$DL(\Delta Y_t|\Delta X_k) = 2^{-k} \sum_{\Delta x_k \in Z_2^k} DL(\Delta Y_t|\Delta X_k = \Delta x_k) \quad (4)$$

(3) Dynamic Output-Output Information Leakage (DL[O:O])

입력 변화 $\Delta\boldsymbol{X}$가 $\Delta\boldsymbol{x}(\Delta\boldsymbol{x} \neq 0,\ \Delta\boldsymbol{x} \in Z_2^m)$로 완전히 알려지는 경우에 k개의 출력비트 변화로 구성된 랜덤벡터 $\Delta\boldsymbol{Y}_k$와 t개의 출력비트 변화로 구성된 랜덤벡터 $\Delta\boldsymbol{Y}_t$사이의 정보누설량 $DL_{\Delta x}(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{Y}_k)$는 다음과 같이 정의한다.

$$DL_{\Delta x}(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{Y}_k) = H(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{X} = \Delta\boldsymbol{x}) - H(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{Y}_k,\ \Delta\boldsymbol{X} = \Delta\boldsymbol{x}) \quad (5)$$

$\Delta\boldsymbol{Y}_k = (\Delta Y_{j_1}, \Delta Y_{j_2}, \cdots, \Delta Y_{j_k}),\ 1 \le k \le n-1$
$\Delta\boldsymbol{Y}_t = (\Delta Y_{l_1}, \Delta Y_{l_2}, \cdots, \Delta Y_{l_t}),\ 1 \le t \le n-1$
$\Delta\boldsymbol{Y}_k \cap \Delta\boldsymbol{Y}_t = \emptyset$
$j_1, j_2, \cdots, j_k \in \{0, 1, \cdots, n-1\}$,
$l_1, l_2, \cdots, l_t \in \{0, 1, \cdots, n-1\}\}$

$DL_{\Delta x}(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{Y}_k)$는 입력 변화가 완전히 알려진다는 가정하에 특정한 k개의 출력비트 변화가 알려질 때, 나머지 출력비트 중에서 t개의 출력비트 변화의 불확실성이 감소하는 양을 측정한다.

2. Walsh 변환을 이용한 정보누설 기준에 대한 고찰

Walsh 변환은 그 정의된 형태 때문에 Boolean 함수의 통계적인 성질을 분석하는데 유용하다. 그러므로 Walsh 변환을 이용하여 조건부 확률을 표현하고 특정한 경우의 입력과 출력간의 정보누설량을 0으로 하기 위해 $m \times n (m \ge n)$ S-box를 구성하는 Boolean 함수가 만족해야 하는 조건을 유도한다. 이들 조건을 살펴봄으로써 특정한 경우에 입력과 출력간의 정보누설량을 0으로 하려는 것은 S-box 설계 기준으로서 적절하지 않음을 보인다.

Z_2^m에서 정의된 임의의 실수 함수 $f(\boldsymbol{x})$의 Walsh 변환 및 역변환은 다음과 같다.

$$F(w) = WT\{f(x)\} = \sum_{x \in Z_2^m} f(x)(-1)^{x \cdot w} \quad (6)$$

$$f(x) = WT^{-1}\{F(w)\} = \frac{1}{2^m} \sum_{w \in Z_2^m} F(w)(-1)^{x \cdot w} \quad (7)$$

$$\boldsymbol{x} \cdot \boldsymbol{w} = x_0 w_0 \oplus x_1 w_1 \oplus \cdots \oplus x_{m-1} w_{m-1}$$

Boolean 함수를 0과 1의 값을 갖는 실수 함수로 여기면, Walsh 변환 및 역변환을 Boolean 함수에 적용할 수 있다. Walsh 변환을 이용하여 Boolean 함수의 통계적인 성질을 분석하는 경우, 0/1 대신 1/-1의 값을 갖도록 변형된 형태의 함수를 사용하는 것이 더 편리하기 때문에 함수 $\hat{f}(\boldsymbol{x})$를 다음과 같이 정의한다.

$$\hat{f}(\boldsymbol{x}) = (-1)^{f(\boldsymbol{x})} = 1 - 2f(\boldsymbol{x}) \quad (8)$$

2.1. Static Input-Output Information Leakage

$\boldsymbol{x}_k$가 주어질 때 $\boldsymbol{Y}_t$의 조건부 엔트로피 $H(\boldsymbol{Y}_t|\boldsymbol{X}_k = \boldsymbol{x}_k)$는 다음과 같다.

$$H(Y_t|X_k=x_k) = \sum_{y_t\in Z_2^t} -P\{Y_t=y_t|X_k=x_k\}\log_2 P\{Y_t=y_t|X_k=x_k\} \quad (9)$$

조건부 확률 $P\{Y_t = y_t|X_k = x_k\}$은 다음과 같다.

$$P\{Y_t=y_t|X_k=x_k\} = \frac{1}{2^{m-k}}\#\{X : X_k=x_k, f_{l_1}(X)=y_{l_1},\cdots,f_{l_t}(X)=y_{l_t}\} \quad (10)$$

여기서, $\#\{\cdot\}$는 집합 $\{\cdot\}$에 속하는 원소의 갯수를 뜻한다.

$N_{x_k}{}^{X_k}(y_t)$를 다음과 같이 정의한다.

$$N_{x_k}{}^{X_k}(y_t) = \#\{X : X_k = x_k, f_{l_1}(X) = y_{l_1},\cdots, f_{l_t}(X)=y_{l_t}\} \quad (11)$$

t개의 Boolean 함수 $f_{l_1}(x)$, $f_{l_2}(x)$, $\cdots$, $f_{l_t}(x)$중에서 a개를 선택하여 선형 조합한 함수를 다음과 같이 정의한다.

$$f_{l_{i_1}l_{i_2}\cdots l_{i_a}}(x) = f_{l_{i_1}}(x)\oplus f_{l_{i_2}}(x)\oplus\cdots\oplus f_{l_{i_a}}(x)$$
$$i_1, i_2,\cdots, i_a \in \{1,2,\cdots,t\},\ 1\le a\le t \quad (12)$$

$Z_2{}^t$에서 정의되며 i_1, i_2, $\cdots$, i_a에 해당하는 위치에서 1을 가지고 나머지 위치에서는 0을 가지는 벡터를 α라 하고, w_k에 0을 덧붙여서 얻은 m차원 벡터를 $O_m(w_k)$라 하면, $\hat{f}_{l_{i_1}l_{i_2}\cdots l_{i_a}}(x)$의 Walsh 변환 $\hat{F}_{l_{i_1}l_{i_2}\cdots l_{i_a}}(w)$는 $N_{x_k}{}^{X_k}(y_t)$를 이용하여 다음과 같이 표현할 수 있다.

$$\begin{aligned}\hat{F}_{l_{i_1}l_{i_2}\cdots l_{i_a}}(O_m(w_k)) &= \sum_{x\in Z_2^m}\hat{f}_{l_{i_1}l_{i_2}\cdots l_{i_a}}(x)(-1)^{x\cdot O_m(w_k)}\\ &= \sum_{x_k\in Z_2^k}\Big\{\sum_{x_{m-k}\in Z_2^{m-k}}\hat{f}_{l_{i_1}l_{i_2}\cdots l_{i_a}}(x_k,x_{m-k})\Big\}(-1)^{x_k\cdot w_k}\\ &= \sum_{x_k\in Z_2^k}\Big\{\sum_{y_t\in Z_2^t}N_{x_k}^{X_k}(y_t)(-1)^{y_t\cdot\alpha}\Big\}(-1)^{x_k\cdot w_k}\end{aligned} \quad (13)$$
$$x_k\cap x_{m-k}=\emptyset,\ x_k\cup x_{m-k}=x,\ w_k=(w_{j_1},w_{j_2},\cdots,w_{j_k})\in Z_2^k$$

$M(x_k, \alpha)$를 다음과 같이 정의한다.

$$M(x_k,\alpha) = \sum_{y_t\in Z_2^t}N_{x_k}^{X_k}(y_t)(-1)^{y_t\cdot\alpha},\ \forall x_k\in Z_2^k \quad (14)$$

$M(x_k, \alpha)$와 $\hat{F}_{l_{i_1}l_{i_2}\cdots l_{i_a}}(O_m(w_k))$는 0이 아닌 모든 α에 대해서 x_k와 w_k에 대한 Walsh 변환쌍이며, $M(x_k, \alpha)$와 $N_{x_k}{}^{X_k}(y_t)$는 모든 x_k에 대해서 y_t와 α에 대한 Walsh 변환쌍이므로 조건부 확률은 다음과 같이 나타낼 수 있다.

$$P\{Y_t = y_t|X_k = x_k\} = \frac{1}{2^t}+\frac{1}{2^{m-k+t}}\sum_{\substack{\alpha\in Z_2^t\\ \alpha\neq 0}}\Big\{\frac{1}{2^k}\sum_{w_k\in Z_2^k}\hat{F}_{l_{i_1}l_{i_2}\cdots l_{i_a}}(O_m(w_k))(-1)^{x_k\cdot w_k}\Big\}(-1)^{y_t\cdot\alpha} \quad (15)$$

조건부 확률은 $1/2^t$을 중심으로 t개의 Boolean 함수의 선형 조합의 Walsh 변환에 의존하여 변한다는 것을 알 수 있다.

정리 1 $m-k<t$인 경우에는 X_k와 Y_t사이에 정보누설이 발생할 수 밖에 없으며, 정보누설량 $SL(Y_t|X_k)$의 가능한 최소값은 다음과 같다.

$$SL(Y_t|X_k) = t+k-m \quad (16)$$

(증명) $m-k<t$인 경우, y_t의 가능한 경우의 수 2^t은 x_{m-k}의 가능한 경우의 수 2^{m-k}보다 크기 때문에 x_k가 주어질 때 조건부 확률의 가능한 가장 균일한 분포는 다음과 같다.

$$P\{Y_t=y_t|X_k=x_k\} = \begin{cases}\frac{1}{2^{m-k}}, & \text{for } 2^{m-k}\ y_t\\ 0, & \text{for } 2^t-2^{m-k}\ y_t\end{cases} \quad (17)$$

x_k가 주어질 때 조건부 확률이 (17)의 분포를 만족하면 식 (1)과 (9)에 의해,

$$SL(Y_t|X_k = x_k) = t+k-m \quad (18)$$

가능한 모든 x_k에 대해 조건부 확률이 (17)의 분포를 갖게 되면 (18)을 식 (2)에 대입함으로써 (16)과 같은 최소값을 얻게 된다. □

정리 2 $m-k\ge t$인 경우, k개의 입력비트가 알려질 때 Y_t의 정보누설량을 0으로 하기 위해서는 Y_t를 이루는 t개의 Boolean 함수는 다음의 조건을 만족해야 한다.

$$\hat{F}_{l_{i_1}l_{i_2}\cdots l_{i_a}}(w) = 0,\ \forall w\in Z_2^m,\ wt(w)\le k$$
$$i_1, i_2,\cdots, i_a\in\{1,2,\cdots,t\},\ 1\le a\le t \quad (19)$$

4) Hamming weight $wt(\cdot)$는 Z_2^m에서 정의된 벡터에 사용되는 경우 벡터중의 1의 갯수를 뜻하며, Z_2^m에서 정의된 Boolean 함수에 사용될 때는 진리표상에서 1의 갯수를 뜻한다.

여기서 wt(·)는 Hamming weight[4]를 뜻한다.

(증명) $m-k \geq t$인 경우, $\boldsymbol{y}_t$의 가능한 경우의 수 2^t은 $\boldsymbol{x}_{m-k}$의 가능한 경우의 수 2^{m-k}보다 작거나 같기 때문에 조건부 확률의 가능한 가장 균일한 분포는 다음과 같다.

$$P\{\boldsymbol{Y}_t = \boldsymbol{y}_t | \boldsymbol{X}_k = \boldsymbol{x}_k\} = \frac{1}{2^t}, \ \forall \boldsymbol{y}_t \in Z_2^t, \ \boldsymbol{x}_k \in Z_2^k \quad (20)$$

조건부 확률이 (20)의 분포를 만족하는 경우 $M(\boldsymbol{x}_k, \boldsymbol{\alpha})$는 다음과 같다.

$$M(\boldsymbol{x}_k, \alpha) = \sum_{\boldsymbol{y}_t \in Z_2^t} 2^{m-k-t}(-1)^{\boldsymbol{y}_t \cdot \alpha} = 2^{m-k}\delta(\alpha), \quad \forall \boldsymbol{x}_k \in Z_2^k$$
$$\delta(\alpha) = \begin{cases} 1, & \alpha = 0 \\ 0, & \alpha \neq 0 \end{cases} \quad (21)$$

그러므로,

$$\hat{F}_{i_1 i_2 \cdots i_a}(O_m(\boldsymbol{w}_k)) = \sum_{\boldsymbol{x}_k \in Z_2^k} M(\boldsymbol{x}_k, \alpha)(-1)^{\boldsymbol{x}_k \cdot \boldsymbol{w}_k}$$
$$= 0, \ \forall \alpha \in Z_2^t, \ \alpha \neq 0 \quad (22)$$

따라서, 어떤 k개의 입력비트가 알려지더라도 $\boldsymbol{Y}_t$의 정보누설량을 0으로 하기 위해서는 (19)를 만족해야 한다. □

정리 2의 조건을 관찰하면, K개의 입력비트가 알려질 때 정보누설량이 0이면 K보다 작은 수의 입력비트가 알려질 때 정보누설량 역시 0이 됨을 알 수 있다. $k=m-1$인 경우 정보누설량을 0으로 하는 함수는 $x_0 \oplus x_1 \oplus \cdots \oplus x_{m-1}$ 혹은 $x_0 \oplus x_1 \oplus \cdots \oplus x_{m-1} \oplus 1$의 두 함수뿐이며 이는 Sigenthaler[15]에 의해서도 밝혀졌다. 그러나, 이 두 함수는 비선형 함수가 아니어서 선형 암호분석에 대해서 DES류의 암호시스템을 치명적으로 약화시키기 때문에 사용할 수 없다. 그리고, 입력이 변할 때 출력은 항상 변하거나 혹은 변하지 않기 때문에 DL[I:O]면에서 바람직하지 않다.

정리 2가 S-box에 사용될 수 있는 Boolean 함수를 어느 정도로 제한하는지를 알아보기 위해 0과 1의 균형이 유지되며 비선형인 4비트 입력 Boolean 함수 12,840개 중에서 입력 한 비트가 알려지는 경우 정보누설량이 0인 함수를 찾아본 결과 222개만을 찾을 수 있었다. 이로부터 작은 k 및 t에 대해서도 k개의 입력비트와 t개의 출력비트간의 정보누설량을 0으로 하기 위해서 정리 2가 t개의 Boolean 함수에 가하는 조건은 너무 제한적이라는 것을 알 수 있다. 그러므로 몇 가지의 특정한 경우에 SL[I:O]가 0인 S-box를 설계하려는 것은 바람직하지 않다.

2.2. Dynamic Input-Output Information Leakage

$\Delta \boldsymbol{X}_k$가 주어질 때 $\Delta \boldsymbol{Y}_t$의 조건부 엔트로피 $H(\Delta \boldsymbol{Y}_t | \Delta \boldsymbol{X}_k = \Delta \boldsymbol{x}_k)$는 다음과 같다.

$$H(\Delta \boldsymbol{Y}_t | \Delta \boldsymbol{X}_k = \Delta \boldsymbol{x}_k) = \sum_{\Delta \boldsymbol{y}_t \in Z_2^t} -P\{\Delta \boldsymbol{Y}_t = \Delta \boldsymbol{y}_t | \Delta \boldsymbol{X}_k = \Delta \boldsymbol{x}_k\} \log_2 P\{\Delta \boldsymbol{Y}_t = \Delta \boldsymbol{y}_t | \Delta \boldsymbol{X}_k = \Delta \boldsymbol{x}_k\} \quad (23)$$

조건부 확률 $P\{\Delta \boldsymbol{Y}_t = \Delta \boldsymbol{y}_t | \Delta \boldsymbol{X}_k = \Delta \boldsymbol{x}_k\}$은 다음과 같다.

$$P\{\Delta \boldsymbol{Y}_t = \Delta \boldsymbol{y}_t | \Delta \boldsymbol{X}_k = \Delta \boldsymbol{x}_k\} = \frac{1}{2^{2m-k}} \#\{(X, \Delta X) : \Delta X_k = \Delta \boldsymbol{x}_k, \ f_{i_1}(X) \oplus f_{i_1}(X \oplus \Delta X) = \Delta y_{i_1}, \ i = 1, \cdots, t\} \quad (24)$$

$N_{\Delta \boldsymbol{x}_k}^{\Delta \boldsymbol{X}_k}(\Delta \boldsymbol{y}_t)$를 다음과 같이 정의한다.

$$N_{\Delta \boldsymbol{x}_k}^{\Delta \boldsymbol{X}_k}(\Delta y_i) = \#\{(X, \Delta X) : \Delta X_k = \Delta \boldsymbol{x}_k, \ f_{i_1}(X) \oplus f_{i_1}(X \oplus \Delta X) = \Delta y_{i_1}, \ i = 1, \cdots, t\} \quad (25)$$

이제 $\hat{f}_{i_1 i_2 \cdots i_a}(\boldsymbol{x})$의 Walsh 변환의 크기의 제곱 $|\hat{F}_{i_1 i_2 \cdots i_a}(\boldsymbol{w})|^2$를 $N_{\Delta \boldsymbol{x}_k}^{\Delta \boldsymbol{X}_k}(\Delta \boldsymbol{y}_t)$를 이용하여 표현하면,

$$\begin{aligned} |\hat{F}_{i_1 i_2 \cdots i_a}(O_m(\boldsymbol{w}_k))|^2 &= \sum_{\Delta \boldsymbol{x}_k \in Z_2^k} \left\{ \sum_{\boldsymbol{x} \in Z_2^m} \hat{f}_{i_1 i_2 \cdots i_a}(\boldsymbol{x}) \hat{f}_{i_1 i_2 \cdots i_a}(\boldsymbol{x} \oplus \Delta \boldsymbol{x}) \right\} (-1)^{\Delta \boldsymbol{x} \cdot O_m(\boldsymbol{w}_k)} \\ &= \sum_{\Delta \boldsymbol{x}_k \in Z_2^k} \left\{ \sum_{\Delta \boldsymbol{x}_{m-k} \in Z_2^{m-k}} \left\{ \sum_{\boldsymbol{x} \in Z_2^m} \hat{f}_{i_1 i_2 \cdots i_a}(\boldsymbol{x}) \hat{f}_{i_1 i_2 \cdots i_a}(\boldsymbol{x} \oplus (\Delta \boldsymbol{x}_k, \Delta \boldsymbol{x}_{m-k})) \right\} \right\} (-1)^{\Delta \boldsymbol{x}_k \cdot \boldsymbol{w}_k} \\ &= \sum_{\Delta \boldsymbol{x}_k \in Z_2^k} \left\{ \sum_{\Delta \boldsymbol{y}_t \in Z_2^t} N_{\Delta \boldsymbol{x}_k}^{\Delta \boldsymbol{X}_k}(\Delta \boldsymbol{y}_t)(-1)^{\Delta \boldsymbol{y}_t \cdot \alpha} \right\} (-1)^{\Delta \boldsymbol{x}_k \cdot \boldsymbol{w}_k} \end{aligned} \quad (26)$$

$$\Delta \boldsymbol{x}_k \cap \Delta \boldsymbol{x}_{m-k} = \emptyset, \ \Delta \boldsymbol{x}_k \cup \Delta \boldsymbol{x}_{m-k} = \Delta \boldsymbol{x}, \ \boldsymbol{w}_k = (w_{j_1}, w_{j_2}, \cdots, w_{j_k}) \in Z_2^k$$

$M(\Delta \boldsymbol{x}_k, \boldsymbol{\alpha})$를 다음과 같이 정의한다.

$$M(\Delta \boldsymbol{x}_k, \alpha) = \sum_{\Delta \boldsymbol{y}_t \in Z_2^t} N_{\Delta \boldsymbol{x}_k}^{\Delta \boldsymbol{X}_k}(\Delta \boldsymbol{y}_t)(-1)^{\Delta \boldsymbol{y}_t \cdot \alpha}, \quad \forall \Delta \boldsymbol{x}_k \in Z_2^k \quad (27)$$

$M(\Delta \boldsymbol{x}_k, \boldsymbol{\alpha})$와 $|\hat{F}_{i_1 i_2 \cdots i_a}(O_m(\boldsymbol{w}_k))|^2$는 0이 아닌 모든 $\boldsymbol{\alpha}$에 대해서 $\Delta \boldsymbol{x}_k$와 $\boldsymbol{w}_k$에 대한 Walsh 변환쌍이며, $M(\Delta \boldsymbol{x}_k, \boldsymbol{\alpha})$와 $N_{\Delta \boldsymbol{x}_k}^{\Delta \boldsymbol{X}_k}(\Delta \boldsymbol{y}_t)$는 모든 $\Delta \boldsymbol{x}_k$에 대해서 $\Delta \boldsymbol{y}_t$와 $\boldsymbol{\alpha}$에 대한 Walsh 변환쌍이므로 조건부 확률은 다음과 같이 나타낼 수 있다.

$$P\{\Delta Y_t = \Delta y_t | \Delta X_k = \Delta x_k\}$$

$$= \frac{1}{2^t} + \frac{1}{2^{2m-k+t}} \sum_{\substack{\alpha \in Z_2^t \\ \alpha \neq 0}} \left\{ \frac{1}{2^k} \sum_{w_k \in Z_2^k} \left| \hat{F}_{i_1 i_2 \cdots i_a}(O_m(w_k)) \right|^2 (-1)^{\Delta x_k \cdot w_k} \right\} (-1)^{\Delta y_t \cdot \alpha} \quad (28)$$

조건부 확률은 $1/2^t$을 중심으로 Walsh 변환의 크기의 제곱에 의존하여 변한다는 것을 알 수 있다. $n \times n$ S-box의 경우 정보누설량을 작게 할 수 있는 한계는 다음과 같다. $k<n$인 경우, 모든 $t(1 \le t \le n)$에 대해 정보누설량을 0으로 하는 것이 가능하다. $k=n$인 경우, $t<n$일 때는 정보누설량을 0으로 하는 것이 가능하지만 $t=n$일 때는 정보누설량을 0으로 하는 것이 불가능한데 그 이유는 다음과 같다. $x \oplus x' = \Delta x$인 x, x'에 대해 $S(x) \oplus S(x') = S(x') \oplus S(x)$이어서 특정한 출력 변화 Δy가 나타나는 횟수는 반드시 2의 배수이다. 그러므로 가장 균일하게 나타나는 경우라도 Z_2^n에 속하는 Δy중에서 절반만이 나타날 수 있다. 이제 $m \times n (m>n)$ S-box의 정보누설량을 0으로 하기 위한 조건을 알아보겠다.

정리 3 $k(1 \le k < m)$개의 입력비트의 변화가 알려질 때 ΔY_t의 정보누설량을 0으로 하기 위해서는 Y_t를 이루는 t개의 Boolean 함수는 다음의 조건을 만족해야 한다.

$$\left| \hat{F}_{i_1 i_2 \cdots i_a}(w) \right|^2 = 0 \ i.e. \ \hat{F}_{i_1 i_2 \cdots i_a}(w) = 0, \quad \forall w \in Z_2^m, \ wt(w) \le k$$
$$i_1, i_2, \cdots, i_a \in \{1, 2, \cdots, t\}, \ 1 \le a \le t \quad (29)$$

(증명) $k<m$인 경우 모든 $t(1 \le t \le n)$에 대해 조건부 확률의 가능한 가장 균일한 분포는 다음과 같다.

$$P\{\Delta Y_t = \Delta y_t | \Delta X_k = \Delta x_k\} = \frac{1}{2^t}, \quad \forall \Delta y_t \in Z_2^t, \ \Delta x_k \in Z_2^k \quad (30)$$

(30)의 분포를 만족하는 경우 $M(\Delta x_k, \alpha)$는 다음과 같다.

$$M(\Delta x_k, \alpha) = \sum_{\Delta y_t \in Z_2^t} 2^{2m-k-t} (-1)^{\Delta y_t \cdot \alpha} = 2^{2m-k} \delta(\alpha), \ \forall \Delta x_k \in Z_2^k \quad (31)$$

그러므로,

$$\left| \hat{F}_{i_1 i_2 \cdots i_a}(O_m(w_k)) \right|^2 = \sum_{\Delta x_k \in Z_2^k} M(\Delta x_k, \alpha)(-1)^{\Delta x_k \cdot w_k} = 0, \ \forall \alpha \in Z_2^t, \ \alpha \neq 0 \quad (32)$$

따라서, 어떤 k개의 입력비트가 알려지더라도 ΔY_t의 정보누설량을 0으로 하기 위해서는 (29)를 만족해야 한다. □

정리 3을 살펴보면 알려진 k개의 입력비트의 변화와 t개의 출력비트의 변화사이의 정보누설량을 0으로 하기 위한 조건이 정리 2와 동일한 형태임을 알 수 있다. 이는 두 정리 모두 입력 혹은 입력 변화에 관한 정보가 완전히 주어지지 않았다고 가정하기 때문이다. 정리 3에 따르면 $m-1$개의 입력비트의 변화를 알더라도 출력 변화의 불확실성이 감소하지 않도록 하기 위해서는 Boolean 함수는 $x_0 \oplus x_1 \oplus \cdots \oplus x_{m-1}$ 혹은 $x_0 \oplus x_1 \oplus \cdots \oplus x_{m-1} \oplus 1$의 형태이어야 한다. 그러나 이러한 형태의 함수는 Ⅲ.2.1절에서 지적했듯이 바람직하지 않다. 한편, 알려진 m-1개의 입력비트의 변화와 $t(t \le 2)$개의 출력비트의 변화사이의 정보누설량을 0으로 하기 위해서는 t개의 Boolean 함수의 모든 선형 조합이 $x_0 \oplus x_1 \oplus \cdots \oplus x_{m-1}$ 혹은 $x_0 \oplus x_1 \oplus \cdots \oplus x_{m-1} \oplus 1$의 형태이어야 하는데 이를 만족하는 t개의 함수를 찾는 것은 불가능하다. 또한 작은 k 및 t에 대해서도 정리 3의 조건은 너무 제한적이다. 그러므로 입력 변화에 관한 정보가 완전히 알려지지 않을 때 몇 가지의 특정한 경우에 대하여 DL[I:O]가 0인 S-box를 설계하려는 것은 바람직하지 않다.

정리 4 입력 변화 Δx가 완전히 알려져 있는 경우 $\Delta x = 0$인 명백한 경우를 제외하고 ΔY_t의 정보누설량을 0으로 하기 위해서는 Y_t를 구성하는 t개의 Boolean 함수는 다음의 조건을 만족해야 한다.

$$\left| \hat{F}_{i_1 i_2 \cdots i_a}(w) \right|^2 = 2^m \ i.e. \ \left| \hat{F}_{i_1 i_2 \cdots i_a}(w) \right| = 2^{\frac{m}{2}}, \quad \forall w \in Z_2^m$$
$$i_1, i_2, \cdots, i_a \in \{1, 2, \cdots, t\}, \ 1 \le a \le t \quad (33)$$

(증명) $k=m$인 경우에는 $\Delta x \neq 0$일 때, 모든 $t(1 \le t \le n)$에 대해 다음과 같은 균일한 조건부 확률을 얻을 수 있으며,

$$P\{\Delta Y_t = \Delta y_t | \Delta X = \Delta x\} = \frac{1}{2^t}, \ \forall \Delta y_t \in Z_2^t \quad (34)$$

$\Delta x = 0$인 경우에는 명백하게 조건부 확률은 다음과 같다.

$$P\{\Delta Y_t = \Delta y_t | \Delta X = 0\} = \begin{cases} 1, & \Delta y_t = 0 \\ 0, & \Delta y_t \neq 0 \end{cases} \quad (35)$$

(34)와 (35)의 분포를 만족하는 경우 $M(\Delta x, \alpha)$는 다음과 같다.

$$M(\Delta x, \alpha) = 2^m(1-\delta(\Delta x))\delta(\alpha) + 2^m\delta(\Delta x) \quad (36)$$

그러므로, Walsh 변환에 의해 (33)을 얻는다. □

Boolean 함수의 Walsh 변환 $\hat{F}(w)$는 항상 짝수이기 때문에 m이 홀수인 경우에는 정리 4의 조건을 만족하는 함수는 존재하지 않는다. m이 짝수인 경우 정리 4를 만족하는 함수는 조합이론에서 bent 함수라고 알려져 있다[16]. 그러나 bent 함수는 0과 1의 균형이 맞지 않기 때문에 regular S-box에는 사용할 수 없으며 SL(I:O)면에서 좋지 않다. m이 짝수이고 $2 \le t \le n$인 경우 입력 변화와 t개의 출력비트 변화사이의 정보누설량을 0으로 하기 위해서는 정리 4에 의해 t개의 Boolean 함수는 모두 bent 함수이어야 하며, 모든 선형 조합 역시 bent 함수이어야 한다. 모든 선형 조합이 bent 함수인 n개의 bent 함수를 이용하여 $m \times n$ S-box를 구성하면, 입력 변화 $\Delta x (\Delta x \neq 0)$가 완전히 알려질 때 출력 변화 Δy의 정보누설량을 0으로 하여 S-box의 XOR 분포테이블을 균일하게 할 수 있다. 그러나, 오히려 DES류의 암호시스템을 differential 암호분석에 매우 취약하게 함이 밝혀져 있으며[17], DES S-box와 같은 regular S-box에는 그러한 구성을 이용할 수 없다.

2.3. S-box 설계 기준으로서 정보누설 기준의 역할

Ⅲ.2.1절과 Ⅲ.2.2절에서는 각각의 경우에 SL(I:O) 및 DL(I:O)를 0으로 하기 위한 조건들을 유도하였다. 정리 3과 정리 4는 각각 $1 \le k \le m-1$인 경우와 $k=m$인 경우에 입력 변화와 출력 변화사이의 정보누설량을 0으로 하기 위한 조건을 제시하고 있는데 두 조건은 서로 모순됨을 알 수 있다. 또한 정리 2의 SL(I:O)를 0으로 하기 위한 조건과 정리 4의 DL(I:O)를 0으로 하기 위한 조건 역시 서로 모순됨을 알 수 있다. 따라서 정리 2, 3, 4의 조건 중 어느 하나를 완전히 만족시켜서 (만족시키는 것이 가능한 경우에) 특정한 경우의 정보누설량을 0으로 하는 것은 다른 경우의 정보누설량을 증가시키는 결과를 가져올 수 있다. 또한 작은 k 및 t에 대해서도 정보누설량을 0으로 하려는 것은 S-box에 이용될 수 있는 Boolean 함수를 너무 제한하게 되어 바람직하지 않다는 것은 Ⅲ.2.1절과 Ⅲ.2.2절에서 언급하였다. 이상의 논의로부터 어느 특정한 경우의 정보누설량을 0으로 하기 위한 시도는 S-box의 설계 기준으로서 적합하지 않음을 알 수 있다. 결국, 정보누설의 관점에서 좋은 S-box는 전체적으로 정보누설량이 크지 않은 S-box이다. 따라서 정보누설 기준은 정보누설량이 큰 S-box를 걸러내는 역할을 수행하는 것이 바람직하다.

정보누설면에서 S-box들간의 비교를 쉽게 하기 위해서는 S-box의 정보누설을 대표할 수 있는 단일한 수치가 필요하다. 각 경우의 이론적으로 가능한 최소 정보누설량과 S-box의 정보누설량의 차이를 모두 더한 값의 크기를 비교함으로써 S-box들간의 비교를 쉽게 할 수 있을 것이다. $m \times n (m \rangle n)$ S-box의 정보누설량 SL(I:O)와 DL(I:O), 그리고 DL(O:O)의 k 및 t에 따른 이론적으로 가능한 최소 정보누설량을 각각 $\overline{SL}(Y_t|X_k)$, $\overline{DL}(\Delta Y_t|\Delta X_k)$, $\overline{DL}_{\Delta x}(\Delta Y_t|\Delta Y_k)$라 하면 다음과 같다.

$$\overline{SL}(Y_t|X_k) = \begin{cases} k+t-m, & \text{if } m-k<t \\ 0, & otherwise \end{cases} \quad (37)$$

$$\overline{DL}(\Delta Y_t|\Delta X_k) = 0, \quad 1 \le k \le m, \quad 1 \le t \le n \quad (38)$$

$$\overline{DL}_{\Delta x}(\Delta Y_t|\Delta Y_k) = 0, \quad 1 \le k < n, \quad 1 \le t \le n-k \quad (39)$$

S-box의 정보누설을 대표하는 단일한 수치로서 TL을 다음과 같이 정의하면,

$$\begin{aligned} TL = & \sum_{k=1}^{m-1}\sum_{t=1}^{n} a(k,t)\{SL(Y_t|X_k) - \overline{SL}(Y_t|X_k)\} \\ & + \sum_{k=1}^{m}\sum_{t=1}^{n} b(k,t)\{DL(\Delta Y_t|\Delta X_k) - \overline{DL}(\Delta Y_t|\Delta X_k)\} \\ & + \sum_{k=1}^{n-1}\sum_{t=1}^{n-k} c(k,t)\{DL_{\Delta x}(\Delta Y_t|\Delta Y_k) \\ & - \overline{DL}_{\Delta x}(\Delta Y_t|\Delta Y_k)\} \end{aligned} \quad (40)$$

TL은 S-box의 전체적인 정보누설을 대표하기 때문에 정보누설 관점에서의 S-box들간의 비교를 쉽게 해준다. 여기서 각 정보누설량과 이론적인 최소치와의 차이에 곱해지는 계수 $a(k,t)$, $b(k,t)$, $c(k,t)$는 S-box의 전체적인 정보누설을 나타냄에 있어서 각각의 정보누설량의 중요도를 어떻게 평가하는가에 따라 다르게 정해질 수 있다. 이 논문에서는 모든 계수의 값을 1로 하고 즉,

각각의 정보누설량의 중요도가 같다고 보고 TL을 계산하겠다.

Ⅳ. S-box의 설계

1. S-box 설계 기준의 선정

최근 DES에 대한 공략에 성공하고 있는 암호분석 방법에는 differential 암호분석 (DC)과 선형 암호분석 (LC)이 있다. 두 암호분석 방법은 DES의 안전도에 큰 위협이 되고 있기 때문에 새로운 S-box를 설계할 때에는 DC와 LC에 대한 고려가 필요하다. LC는 S-box의 선형 근사식을 이용하기 때문에 S-box의 nonlinearity는 LC와 관련하여 평가해야 한다. 또한 근본적으로 DES는 SP network의 일종이기 때문에 좋은 avalanche를 보장할 수 있도록 S-box를 설계해야 하며, 좋은 confusion을 얻기 위해 S-box의 입력 및 출력에 관한 부분적인 정보에 의한 정보누설 역시 고려해야 한다.

1.1. Nonlinearity에 대한 고려

두 Boolean 함수 f와 g사이의 거리 (distance) $d(f,g)$는 Hamming weight를 이용하여 다음과 같이 정의한다.

$$d(f, g) = wt(f \oplus g) \tag{41}$$

Pieprzyk와 Finkelstein은 Z_2^m에서 정의된 함수 f의 nonlinearity N_f를 f와의 거리를 최소로 하는 선형 혹은 affine 함수와 f간의 거리로 정의하였으며 다음과 같다[18].

$$N_f = d(f, L_m) = \min \; d(f, \alpha),\ \alpha \in L_m \tag{42}$$

여기서 L_m은 Z_2^m에서 정의되는 선형 함수와 affine 함수의 집합을 의미한다.

LC에서 이용하는 선형 근사식을 살펴보고 이로부터 S-box의 nonlinearity가 어떤 관점에서 평가되어야 하는지를 결정하겠다. $m \times n$ S-box S의 선형 근사식은 0이 아닌 벡터 $\alpha \in Z_2^m$, $\beta \in Z_2^n$에 의해 다음과 같이 정의된다.

$$\boldsymbol{x} \cdot \alpha = S(\boldsymbol{x}) \cdot \beta \tag{43}$$

$NS(\alpha, \beta)$를 다음과 같이 정의하면 α, β에 의해 각각 선택된 입력비트와 출력비트의 상관 관계는 $|NS(\alpha, \beta)-2^{m-1}|$에 의해 측정되며 이는 선형 근사식의 유용성을 나타낸다.

$$NS(\alpha, \beta) = \#\{\boldsymbol{x} | \boldsymbol{x} \cdot \alpha = S(\boldsymbol{x}) \cdot \beta\} \tag{44}$$

$S(\boldsymbol{x}) \cdot \beta$는 $m \times n$ S-box S를 구성하는 n개의 m비트 입력 Boolean 함수들 중 β에 의해 지정된 함수들의 선형 조합을 뜻하며 이를 f_β라 하겠다. 만일 f_β가 선형 혹은 affine 함수이면 확률 1 혹은 0을 갖는 S-box의 선형 근사식을 찾을 수 있어서 DES를 LC에 대해 치명적으로 약화시키기 때문에, 모든 β에 대해 f_β는 반드시 비선형 함수이어야 한다. 따라서 S-box의 nonlinearity N_S를 다음과 같이 정의하여 S-box의 nonlinearity를 평가하겠다.

$$N_S = \min N_{f_\beta} \tag{45}$$

위와 같이 S-box의 nonlinearity를 정의할 때 $|NS(\alpha, \beta)-2^{m-1}|$는 $2^{m-1}-N_S$이하로 제한되므로 가능한 N_S를 크게 하는 것이 바람직하다.

실제로 6×4 S-box를 구성하는 실험을 해본 결과 N_S의 허용되는 최소값을 16으로 하는 것이 적절하였다. DES에 쓰일 수 있는 6×4 S-box를 설계하기 위한 nonlinearity 기준은 다음과 같이 설정한다.

$$N_S \geq 16 \tag{46}$$

1.2. Differential 암호분석에 대한 고려

DC에 대해 DES류의 암호시스템을 약화시키지 않으려면 암호시스템에서 사용되는 $m \times n$ S-box는 DC에서 가장 유용하게 이용되는 반복특성 (iterative characteristic)의 확률이 작아지도록 설계해야 한다. 또한 어떤 특성의 확률이 너무 커지지 않도록 하기 위해서 XOR 분포테이블의 최대값을 제한해야 한다. Knudsen은 DC에 대해 DES를 약하게 하지 않으려면 DES에 사용되는 6×4 S-box는 반드시 DES S-box 설계 기준 P0, …, P4를 만족해야 한다는 것을 밝혀내었다[19]. 김 광조는 2라운드 반복특성의 확률을 작게함으로써 DC의 효율을 떨어뜨릴 수 있다는 점에 착안하여 S-box가 다음의 조건 P6을 만족하도록 설계할 것을 제안하였다.

P6. 임의의 e, f에 대해 $S(\boldsymbol{x}) \neq S(\boldsymbol{x} \oplus 11ef10)$이다.

또한 P0, …, P4 및 P6을 만족하는 8개의 S-box를 사용하면 S-box의 XOR 분포테이블에서 허용되는 최대값이 λ일 때 2라운드 반복특성의 확률이 $(\frac{\lambda}{64})^8$이하가 됨을 보이고, 실제로 DES S-box 설계 기준 P0, …, P5 및 P6을 만족하는 8개의 S-box를 만들어 DES의 S-box를 대신한 s^3DES를 제안하고 있다[20].

따라서, DC에 대해 DES를 강하게 하기 위해서 P0, …, P4 및 P6을 새로운 S-box의 설계 기준에 포함한다. DC에 이용될 수 있는 특성의 확률이 너무 커지는 것을 방지하기 위해서는 S-box의 XOR 분포테이블의 최대값을 제한해야 한다. 실제로 S-box를 생성하는 실험을 해본 결과 허용되는 최대값 λ는 20으로 하는 것이 적절하였다. DES S-box의 XOR 분포테이블의 최대값은 모든 S-box에 대해 16이어서 λ를 20으로 할 경우 S-box의 입력 XOR와 출력 XOR 쌍의 확률의 최대값이 DES의 경우보다 커질 수 있지만, 2라운드 반복특성의 확률이 DES에 비해 현저히 작으므로 문제가 되지 않는다.

1.3. Avalanche에 대한 고려

DES와 같이 SP network에 기초한 블럭 암호시스템에서 사용되는 S-box는 평문의 작은 변화가 라운드를 반복하면서 예측할 수 없는 형태로 퍼지는 avalanche가 나타나도록 설계해야 하며, 이를 위해 strict avalanche criterion (SAC)[21]이 도입되었다. i번째 비트만 1이고 나머지 비트는 모두 0인 벡터를 $\boldsymbol{c}_i$라 하면, $m\times n$ S-box S의 입력비트 i가 변화할 때 출력비트 j가 변할 확률 p_{ij}^S는 (47)과 같으며 SAC는 p_{ij}^S가 (48)을 만족할 것을 요구한다.

$$p_{ij}^S=\frac{1}{2^m}\sum_{x\in Z_2^m}\{f_j(\boldsymbol{x})\oplus f_j(\boldsymbol{x}\oplus\boldsymbol{c}_i)\},\ 0\le i<m,\ 0\le j<n \quad (47)$$

$$p_{ij}^S=\frac{1}{2},\ 0\le i<m,\ 0\le j<n \quad (48)$$

SAC를 만족하는 S-box는 입력의 한 비트가 변할 때 각 출력비트의 변화를 예측할 수 없기 때문에 DES류의 암호시스템에서 입력 블럭의 작은 변화가 라운드를 반복하면서 예측할 수 없는 형태로 퍼져나가도록 한다. 특히 DES와 같이 작은 S-box들을 모아서 데이타 블럭을 치환하는 블럭 암호시스템의 경우, 초기의 몇 라운드에서는 S-box의 입력 중 한 비트가 변할 확률이 높기 때문에 S-box는 SAC를 고려하여 설계하는 것이 바람직하다. $m\times n$ S-box가 SAC를 어느 정도로 근접하여 만족하는지를 평가하기 위해서 p_{ij}^S의 $\frac{1}{2}$로부터의 편차를 나타내는 ρ를 다음과 같이 정의한다.

$$\rho=\sqrt{\frac{\sum_{i=0}^{m}\sum_{j=0}^{n}|p_{ij}^S-0.5|^2}{mn}} \quad (49)$$

DES에 쓰일 수 있는 6×4 S-box와 S-box를 구성하는 4×4 치환 G는 근사적으로 SAC를 만족하도록 한다. 구체적으로 설명하면 다음과 같다. 4×4 치환 G는 다음을 만족하도록 한다.

$$0.25\le p_{ij}^G\le 0.75,\ 0\le i<4,\ 0\le j<4 \quad (50)$$

DES에 쓰일 수 있는 6×4 S-box는 MSB와 LSB에 의해 4개의 4×4 치환 중 하나를 선택하기 때문에 각 치환이 (50)을 만족하는 경우 다음이 성립한다.

$$0.25\le p_{ij}^S\le 0.75,\ 1\le i\le 4,\ 0\le j<4 \quad (51)$$

따라서 4개의 치환으로 S-box를 구성한 뒤 다음의 조건을 만족하는지를 검사하여 SAC를 근사적으로 만족하는 S-box를 찾는다.

$$0.25\le p_{ij}^S\le 0.75,\ i=0,5,\ 0\le j<4 \quad (52)$$

1.4. 정보누설에 대한 고려

Ⅲ장에서는 특정한 경우에 S-box의 입력과 출력사이의 정보누설량을 0으로 하려는 시도가 S-box 설계 기준으로서 적절하지 않으며 정보누설 기준은 정보누설이 큰 S-box를 걸러내는 역할을 담당하는 것이 바람직함을 보였다. DES에 쓰일 수 있는 6×4 S-box를 설계하기 위한 정보누설 기준은 다음과 같이 설정한다. S-box를 구성하는 4×4 치환의 정보누설량이 너무 클 경우 S-box의 정보누설량을 작게 할 수 없기 때문에 4×4 치환과 S-box 모두 정보누설량에 의해 평가한다. 정보누설 기준에서 사용하는 정보누설량은 $SL(\boldsymbol{Y}_t|\boldsymbol{X}_k)$, $DL(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{X}_k)$, 그리고 $DL_{\Delta x}(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{Y}_k)$이다. 각 정보누설량은 주어진 k 비트 벡터와 정보누설량을 측정하고자 하는 t비트 벡터의 가능한 모든 조합의 정보누설량의 평균값으로 한다. $DL_{\Delta x}(\Delta\boldsymbol{Y}_t|\Delta\boldsymbol{Y}_k)$는 모든 $\Delta\boldsymbol{x}(\Delta\boldsymbol{x}\neq 0)$에 대해 위와 같이 정보누설량을 계산한 뒤 다시 평균값을 취하여 사용한다. 각 경우의 정보누설량이 DES의 경우보다 커지지 않도록 하기 위해 4×4 치환 및 S-

box를 걸러내는 기준값들은 DES에서의 최대값으로 한다.

한편, DES S-box 설계 기준 중 P5는 모든 4×4 치환이 다음을 만족하도록 한다[22].

$$\left| P\{y_j = b \mid x_i = a\} - \frac{1}{2} \right| \le \frac{1}{8}, \quad 0 \le i, j < 4, \ \forall a, b \in Z_2 \tag{53}$$

이는 이용할 수 있는 4비트 입력 Boolean 함수를 비현실적으로 제한하지 않으면서 입력 한 비트를 알 때 각 출력비트의 불확실성의 감소를 작게 할 수 있는 실질적인 한계치이다. 그러므로 6×4 S-box의 입력 1비트를 아는 경우 각 출력비트의 불확실성의 감소를 최소화하기 위해서 P5 역시 설계 기준에 포함한다. 입력 1비트를 고정하였을 때 각 출력비트에서의 0과 1의 차이를 단일한 수치로 비교하기 위해 입력비트 i를 고정하였을 때 출력비트 j의 0과 1의 차이를 D_{ij}라 하고, D를 다음과 같이 정의한다.

$$D = \frac{1}{16} \sum_{i=1}^{4} \sum_{j=0}^{3} D_{ij} \tag{54}$$

DES에 쓰일 수 있는 6×4 S-box는 MSB 혹은 LSB를 고정했을 때 각 출력비트에서 0과 1이 발생하는 횟수가 같으므로 i=0,5인 경우는 포함하지 않는다.

2. 설계 기준에 의한 6×4 S-box의 구성

Ⅳ.1절에서 선정한 설계 기준에 의해 4×4 치환 G는 다음을 만족해야 한다.

A1. 치환을 구성하는 4비트 입력 Boolean 함수는 모두 비선형이다.

A2. 4개의 입력비트들 중 하나의 비트값을 바꾸면, 적어도 2개 이상의 출력비트가 바뀐다.

A3. $G(\boldsymbol{x})$와 $G(\boldsymbol{x} \oplus 0110)$은 적어도 2비트 이상이 달라야 한다.

A4. $0.25 \le p_{ij}^{G} \le 0.75$, $0 \le i, j < 4$, $0 \le j < 4$

A5. $|P\{y_j = b \mid x_i = a\} - \frac{1}{2}| \le \frac{1}{8}$, $0 \le i, j < 4$, , $\forall a, b \in Z_2$

A6. 각 경우의 정보누설량이 DES의 4×4 치환의 최대 정보누설량 이하여야 한다.

Ⅳ.1절에서 선정한 설계 기준 중 P2, P4, P6은 S-box를 구성하는 4개의 치환 G_i(i=0,…,3)간의 관계를 모든 $\boldsymbol{x}(\boldsymbol{x} \in Z_2^4)$에 대해 다음과 같이 제한한다.

R1. $wt(G_0(\boldsymbol{x}) \oplus G_1(\boldsymbol{x})) \ge 2$
$wt(G_0(\boldsymbol{x}) \oplus G_2(\boldsymbol{x})) \ge 2$
$wt(G_1(\boldsymbol{x}) \oplus G_3(\boldsymbol{x})) \ge 2$
$wt(G_2(\boldsymbol{x}) \oplus G_3(\boldsymbol{x})) \ge 2$

R2. $G_0(\boldsymbol{x}) \ne G_2(\boldsymbol{x} \oplus 1efg)$, $\forall e, f, g \in Z_2$
$G_1(\boldsymbol{x}) \ne G_3(\boldsymbol{x} \oplus 1efg)$, $\forall e, f, g \in Z_2$

S-box는 다음과 같은 방법으로 구성한다. A1, …, A6을 만족하는 4×4 치환을 선택하고 이를 G_0로 한다. G_0로부터 R1, R2에 의해 차례로 G_i(i=0,…,3)를 구성하는데 이 때 A1, …, A6을 만족하는지를 검사하여 G_i의 사용 여부를 결정하며 최종적으로 S-box를 얻은 뒤 다음의 조건을 만족하는지를 검사한다.

B1. $N_S \ge 16$

B2. $0.25 \le p_{ij}^{S} \le 0.75$, $i = 0,5$, $0 \le j < 4$

B3. XOR 분포테이블의 최대값 ≤ 20

B4. 각 경우의 정보누설량이 DES S-box의 최대 정보누설량 이하여야 한다.

S-box가 B1, …, B4를 만족하는 경우 Ⅳ.1절에서 선정한 기준을 모두 만족하게 된다.

위의 과정에 의해 구성한 8개의 6×4 S-box로 DES의 S-box를 대신하는 암호시스템을 LDES라고 하겠다. 부록 A에서 LDES에 사용되는 8개의 S-box를 보

표 1. Nonlinearity N_S의 비교
Table 1. Comparison of nonlinearity N_S

S-box	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
DES	14	16	16	16	12	18	14	16
s^3DES	16	16	16	8	8	12	12	16
LDES	16	16	16	16	16	16	6	16

인다. 이제 DES 및 s^3 DES와 LDES의 S-box의 특성을 비교하겠다. 표 1에서는 nonlinearity를 비교하고 있다.

DES S-box의 N_S는 12에서 18의 값을 가지며, s^3 DES S-box의 N_S는 8에서 16의 값을 가진다. 그리고, LDES S-box의 N_S는 모두 16이다. Nonlinearity면에서는 DES와 LDES의 S-box가 s^3 DES의 S-box보다 좋음을 알 수 있다. 표 2에서는 avalanche 특성을 비교하고 있다.

LDES S-box들의 p_{ij}^s는 DES나 s^3DES와는 달리 설계 기준에 의해 0.25에서 0.75로 제한되기 때문에 ρ를 비교했을 때 LDES의 경우가 대체로 더 작은 값을 갖는다는 것을 알 수 있다. ρ는 p_{ij}^s의 0.5로부터의 편차를 나타내기 때문에 avalanche면에서 LDES가 DES나 s^3DES보다 좋다고 할 수 있다. 표 3에서는 정보누설을 비교하고 있다.

DES, s^3DES, 그리고 LDES는 모두 DES S-box 설계 기준 중 P5를 만족하도록 하였기 때문에 D는 비슷한 분포를 갖는다. 정보누설량 TL을 살펴보면 s^3DES가 DES나 LDES에 비해 큰 값을 갖는다는 것을 알 수 있다. 따라서, 정보누설면에서는 s^3DES가 DES나 LDES에 비해 좋지 않다. 표 4에서는 XOR 분포테이블의 최대값을 비교하고 있다.

DES S-box는 모두 최대값이 16이며 s^3DES와 LDES는 18에서 20의 최대값을 갖는다. DES의 경우가 최대값이 더 작지만 s^3DES나 LDES는 2라운드 반복특성의 확률이 DES에 비해 현저히 작기 때문에 DC에 대해 DES보다 강하다고 할 수 있다. DES, s^3DES, 그리고 LDES의 S-box들의 특성을 정량적으로 비교한 결과 LDES는 DC에 대해 s^3DES정도의 안

표 2. Avalanche 특성의 비교
Table 2. Comparison of avalanche characteristics

S-box		S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
DES	min p_{ij}^s	0.5000	0.4375	0.5000	0.5000	0.4375	0.5000	0.4375	0.3750
	max p_{ij}^s	0.7500	0.9375	0.8750	0.6875	0.8125	0.8125	0.8750	0.8125
	ρ	0.1455	0.1754	0.1976	0.1276	0.1547	0.1768	0.1901	0.1712
s^3 DES	min p_{ij}^s	0.1250	4375	0.4375	0.4375	0.3750	0.3750	0.3750	0.3750
	max p_{ij}^s	0.9375	0.7500	0.8125	0.8750	0.7500	0.8125	0.8750	0.7500
	ρ	0.1849	0.1362	0.1547	0.1588	0.1578	0.1683	0.1853	0.1614
LDES	min p_{ij}^s	0.5625	0.5625	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000
	max p_{ij}^s	0.7500	0.7500	0.7500	0.6875	0.6875	0.7500	0.7500	0.7500
	ρ	0.1593	0.1593	0.1593	0.1344	0.1344	0.1415	0.1510	0.1520

표 3. 정보누설 특성의 비교
Table 3. Comparison of information leakage characteristics

S-box		S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
DES	TL	6.2009	5.8464	6.0400	6.7414	6.3773	5.8986	6.1994	5.8651
	D	2.4	1.0	1.5	2.0	1.5	1.6	1.9	1.0
s^3DES	TL	6.7805	6.6296	6.9422	7.2493	7.7028	7.0563	6.5244	6.8993
	D	1.5	1.5	1.0	1.3	1.3	1.0	1.4	1.0
LDES	TL	6.0350	6.0350	6.1548	6.2683	6.2683	6.1685	6.0914	9.0757
	D	1.6	1.6	1.6	1.8	1.8	1.5	1.5	1.5

표 4. XOR 분포테이블의 최대값의 비교
Table 4. Comparison of maximal values of XOR distribution tables

S-box	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
DES	16	16	16	16	16	16	16	16
s^3DES	20	18	20	20	20	20	20	20
LDES	18	18	20	20	20	20	18	18

전도를 보장하며 다른 특성들은 DES보다 좋거나 비슷함을 알 수 있다.

V. 결 론

이 논문에서는 특정한 경우의 정보누설량을 0으로 하기 위해 S-box를 구성하는 Boolean 함수가 만족해야 하는 조건을 Walsh 변환을 이용하여 유도하였다. 그러한 조건들간의 관계를 고찰함으로써 특정한 경우에 정보누설량을 0으로 하려는 것은 S-box 설계 기준으로서 바람직하지 않으며, 정보누설 기준은 정보누설량이 큰 S-box를 걸러내는 역할을 하는 것이 적절함을 보였다. 또한 DES에 대한 암호분석 및 DES의 구조 그리고 정보누설을 고려한 S-box 설계 기준을 제시하고 이를 만족하는 8개의 6×4 S-box로 DES의 S-box를 대신하는 LDES를 제안하였다. 설계된 S-box들의 분석 결과는 이 논문에서 제안하는 설계 기준이 DC에 대해 DES를 강하게 하면서 전반적으로 암호학적 특성이 좋은 S-box를 구성할 수 있음을 보여주고 있다.

부록 A. LDES S-boxes

S_1-box

15	1	3	13	5	8	10	6	4	7	14	0	2	11	9	12
0	2	9	2	6	15	3	5	10	1	7	14	13	8	4	11
5	6	15	8	10	1	3	13	9	12	2	11	4	7	14	0
9	3	2	15	5	6	12	0	7	10	8	4	14	1	11	13

S_2-box

7	9	11	5	1	12	14	2	0	3	6	8	10	15	13	4
8	4	13	10	2	7	11	1	14	9	3	6	5	12	0	15
1	2	7	12	14	9	11	5	13	4	10	15	0	3	6	8
13	11	10	7	1	2	4	8	3	14	12	0	6	9	15	5

S_3-box

1	7	2	9	4	10	11	12	13	0	8	6	3	15	14	5
6	0	15	12	3	9	8	5	10	13	1	11	4	2	7	14
7	11	9	12	10	1	4	2	14	5	3	0	13	6	8	15
9	6	0	5	12	15	3	8	7	11	13	14	10	1	4	2

S_4-box

3	13	15	1	5	8	10	6	4	7	2	12	14	11	9	0
10	6	9	12	0	11	15	5	1	8	4	3	7	13	2	14
15	1	5	6	8	13	3	10	2	12	11	0	4	7	14	9
5	15	12	10	11	0	6	9	8	3	7	13	2	14	1	4

S_5-box

4	2	7	14	11	5	13	8	10	9	12	3	6	0	1	15
1	15	8	3	13	10	14	4	6	12	5	9	0	7	11	2
14	5	13	8	7	11	4	2	3	10	0	6	9	12	15	1
13	10	3	15	14	4	8	1	0	7	9	12	5	2	6	11

S_6-box

2	4	5	9	8	3	11	14	12	1	15	10	6	13	0	7
1	8	11	14	7	13	12	2	15	4	6	3	0	10	5	9
11	14	2	5	4	9	8	3	1	7	12	0	15	10	6	13
8	2	13	11	14	7	1	12	4	9	10	5	3	0	15	6

S_7-box

2	7	15	1	5	12	9	10	4	13	8	6	11	0	14	3
5	12	0	6	3	15	14	9	8	7	11	1	13	10	2	4
9	2	5	12	10	7	15	1	14	11	3	0	4	13	8	6
12	9	15	3	6	0	3	14	1	2	4	11	10	7	13	8

S_8-box

13	3	7	4	0	9	10	15	6	8	11	14	5	2	12	1
2	15	9	3	5	6	12	10	13	4	14	8	11	1	0	7
4	9	10	15	7	0	13	3	1	2	12	5	11	14	6	8
9	2	6	5	10	15	3	12	14	8	0	11	7	4	13	1

참고문헌

1. C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Tech. Journal*, vol. 28, pp.656-715, 1949.
2. National Bureau of Standards, "Data Encryption Standard (DES)," Tech. Rep. Pub. 46, Federal Information Processing Standards, 1977.
3. S. Miyaguchi, A. Shiraichi, and A. Shimizu, "Fast data encipherment algorithm FEAL-8," *Review of the Electrical Commun. Lab.*, vol. 36, pp.433-437, 1988.
4. L. Brown, J. Pieprzyk, and J. Seberry, "LOKI-A cryptographic primitive for authentication and secrecy applications," *Advances in Cryptology : Proc. of AUSCRYPT 90*, Sydney, pp.229-236, Springer-Verlag, 1990.
5. H. Feistel, W. Notz, and J. L. Smith, "Some cryptographic techniques for machine-to-machine data communications," *Proc. of IEEE*, vol. 63, pp.1545-1554, 1975.
6. E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, pp.3-72, 1991.
7. E. Biham and A. Shamir, *Differential cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.
8. M. Matsui, "Linear cryptanalysis method for DES cipher," *Pre-proc. of EUROCRYPT 93*, Lofthus, pp.112-123, 1993.
9. M. Matsui, "The first experimental cryptanalysis of the Data Encryption Standard," *Advances in Cryptology : Proc. of CRYPTO 94*, Santa Barbara, pp.1-11, Springer-Verlag, 1994.
10. M. H. Dawson, *A unified framework for substitution box design based on information theory*, M.S. thesis, Queens University, 1991.
11. E. F. Brickell, J. H. Moore, and M. R. Purtill, "Structure in the S-boxes of the DES (extended abstract)," *Advances in Cryptology : Proc. of CRYPTO 86*, Santa Barbara, pp.3-8, Springer-Verlag, 1987.
12. R. Forre, "Methods and instruments for designing S-boxes," *Journal of Cryptology*, vol. 2, pp.115-130, 1990.
13. M. Sivabalan, S. E. Tavares, and L. E. Peppard, "On the design of SP networks from an information theoretic point of view," *Pre-proc. of CRYPTO 92*, Santa Barbara, pp.6.1-6.6, 1992.
14. M. Zhang, S. E. Tavares, and L. L. Campbell, "Information leakage of Boolean functions as a measure of cyptographic strength," *Proc. of SAC 94*, Kingston, pp.40-51, 1994.
15. T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inform. Theory*, vol. IT-30, pp.776-780, 1984.
16. O. S. Rothaus, "On bent functions," *Journal of Comb. Theory (A) 20*, pp.300-305, 1976.
17. L. Brown, M. Kwan, J. Pieprzyk, and J. Seberry, "Improving resistance to differential cryptanalysis and the redesign of LOKI," *Pre-proc. of ASIACRYPT 91*, Fujiyoshida, pp.25-30, 1991.
18. J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," *IEE Proc. E*, vol. 135, pp. 325-335, 1988.
19. L. R. Knudsen, "Iterative characteristics of DES and s^2-DES," *Pre-proc. of CRYPTO 92*, Santa Barbara, pp.12.6-12.11, 1992.
20. K. Kim, S. Park, and S. Lee, "Reconstruction

of s^2DES S-boxes and their immunity to differential cryptanalysis," *Proc. of JW-ISC 93*, Seoul, pp.32.01-32.10, 1993.

21. A. F. Webster and S. E. Tavares, "On the design of S-boxes," *Advances in Cryptology : Proc. of CRYPTO 85*, Santa Barbara, pp.523-534, Springer-Verlag, 1986.
22. J. H. Yang, "The data base of selected permutations," *Pre-proc. of ASIACRYPT 91*, Fujiyoshida, pp.41-45, 1991.

李 周 鎬(Ju Ho Lee) 정회원

1971년 12월 3일생
1993년 2월 : 한국과학기술원 전기 및 전자공학과 학사
1995년 2월 : 한국과학기술원 전기 및 전자공학과 석사
1995년 3월~현재 : 한국과학기술원 전기 및 전자공학과 박사과정
※주관심 분야 : 이동통신, 채널코딩, 통신신호처리, 암호학

金 炯 明(Hyung Myung Kim) 정회원

1952년 10월 24일생
1974년 2월 : 서울대학교 공학사
1982년 4월 : 미국 Pittsburgh 대학 전기공학과 석사
1985년 12월 : 미국 Pittsburgh 대학 전기공학과 공학박사
1986년 4월~1992년 8월 : 한국과학기술원 전기 및 전자공학과 조교수
1992년 9월~현재 : 한국과학기술원 전기 및 전자공학과 부교수
※주관심 분야 : 디지탈 신호와 영상처리, 다차원시스템 이론, 비디오신호 전송통신 이론, 이동 통신 기술 분야