通信情報保護學會論文誌
第 2 卷 第 1 號, 1992. 6

FEAL-8의 심볼간 상호의존도

황금화* · 문상재*

The Intersymbol Dependence of FEAL-8

Gum-Hwa Hwang and Sang-Jae Moon

요 약

본 논문에서는 FEAL-8의 암호화 함수 특성을 분석하고 이를 이용하여 FEAL-8의 입출력 심볼간 상호의존도를 조사하였다. 심볼간 상호의존도 분석 방법에 Meyer와 Matas의 방법을 적용하였다.

Abstract

This paper investigates the characteristics of the encryption function, and analyzes the intersymbol dependence of the FEAL-8. The Meyer and Matas's method is employed for the analysis of the intersymbol dependence.

1. 서 론

FEAL-8은 1986년에 일본 NTT에서 연구 발표한 관용 암호 알고리듬이다.[1-2] 이외에 관용 암호 알고리듬의 대표적인 것으로 미국에서 1970년대 초 개발된 Lucifer[3]와 1974년에 발표된 DES[4]등이 있다.

관용 암호 알고리듬은 주로 키이의 크기에 관련되는 exhaustive attack과 암호화된 출력의 불규칙성 및 입출력간의 심볼간 상호의존성에 의해 주로 측정되는 대수적 및 확률적 암호분석 등으로부터 안전해야 한다. 입력되는 심볼의 변화에 대한 출력문의 모든 심볼의 변화율을 표시하는 심볼간 상호의존성은 암호화 알고리듬의 구조에 의해 결정되며, 암호화 알고리듬의 설계에 중요한 역할을 한다. 암호화 알고리듬의 출력비트는 입력되는 정보비트들과 키이 비트들의 함수로 볼 수 있으며, 출력비트와 어떤 입력비트의 두 비트 사이에 이러한 함수적인 관계를 지니게 되면 상호의존한다고 하고, 임의의 출력비

* 경북대학교 전자공학과

트가 입력비트 전체와 이러한 함수적인 관계를 가지면 이 출력비트는 입력에 상호의존 한다고 한다. 입력 전체에 대한 전체 출력비트의 상호의존을 백분율로 나타낸 것을 심볼간 상호의존도라 한다.[5]

본 논문에서는 FEAL-8의 심볼간 상호의존도를 분석하였다. 그리고 다른 관용 암호 알고리듬의 심볼간 상호의존도와 비교하였다.

2. FEAL-8 알고리듬

FEAL-8에 입력되는 키이, 정보문 및 출력되는 암호문은 모두 64비트이며, 크게 보조키이 생성과정과 데이타 랜덤화 과정으로 나눌 수 있다. 전자는 암호화 과정에서 사용될 보조키이를 입력된 키이를 사용하여 생성하는 과정이고, 후자는 생성된 보조키

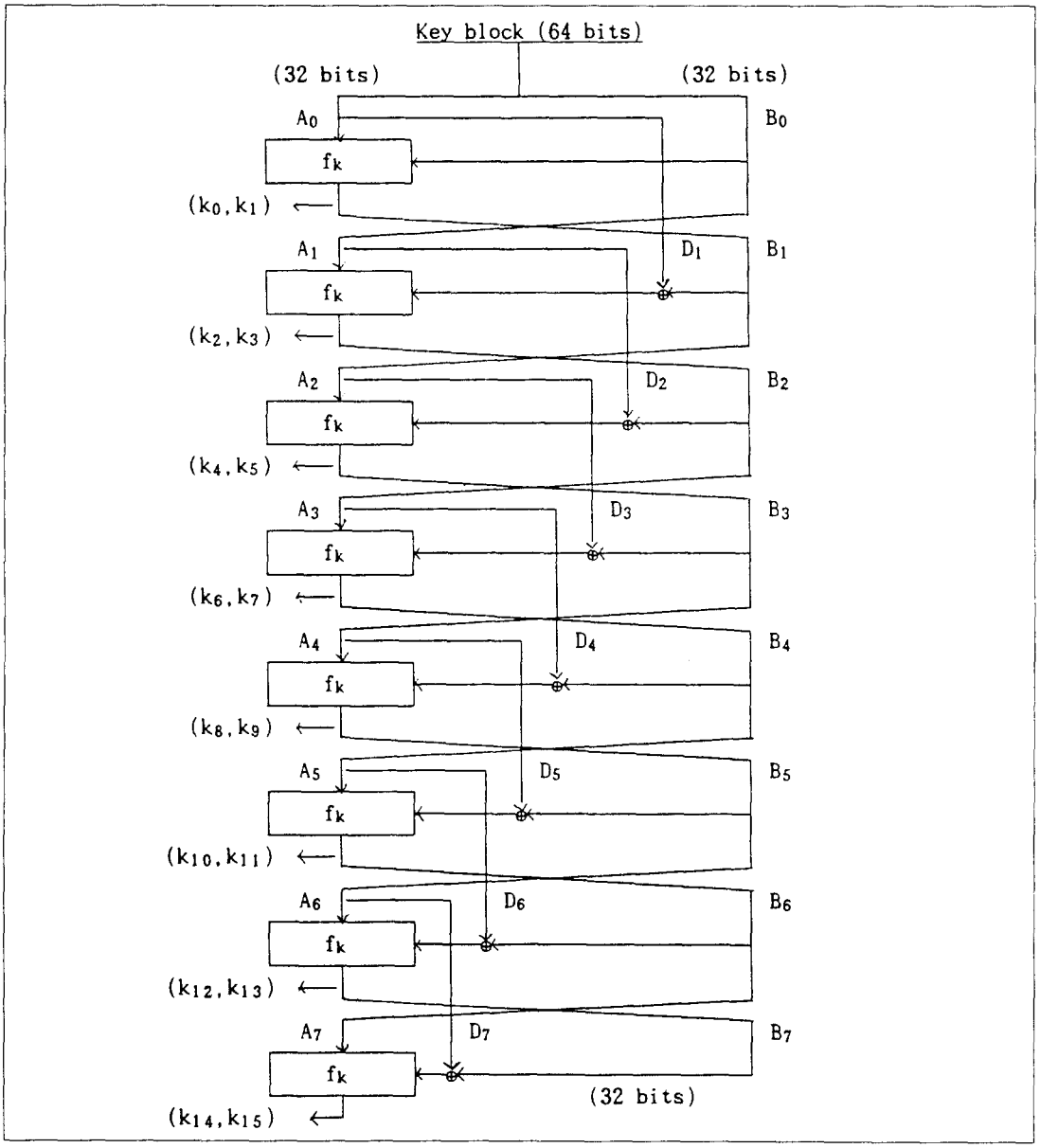


그림 1. 보조키이 생성과정 블럭도

이를 사용하여 실제로 암호화를 수행하는 과정이다.

그림 1은 보조키이 생성과정을 나타낸 블럭도이다. 전체는 8라운드로 구성되며 모든 수행과정이 끝나면 16비트 보조키이 16개가 만들어진다. 내부에 사용된 f_k함수는 그림 2에 도시하였다. 그림 1과 그림 2의 과정을 사용된 기호를 이용하여 관계식으로 표현하면 다음과 같다.

$$D_r = A_{r-1} \quad (1)$$

$$A_r = B_{r-1} \quad (2)$$

$$B_r = f_k(A_{r-1},\ B_{r-1} \oplus D_{r-1}) \quad (3)$$

여기서 $1 \le r \le 7$이고, A_0와 B_0는 첫 라운드의 입력이다.

$$f_{k1}' = \alpha_1 \oplus \alpha_0 \quad (4)$$

$$f_{k2}' = \alpha_2 \oplus \alpha_3 \quad (5)$$

$$f_{k1} = S_Q(f_{k1}',\ f_{k2}',\ \oplus\ \beta_0,\ Q=1) \quad (6)$$

$$f_{k2} = S_Q(f_{k2}',\ f_{k1},\ \oplus\ \beta_1,\ Q=0) \quad (7)$$

$$f_{k0} = S_Q(\alpha_0,\ f_{k1},\ \oplus\ \beta_2,\ Q=0) \quad (8)$$

$$f_{k3} = S_Q(\alpha_3,\ f_{k2},\ \oplus\ \beta_3,\ Q=1) \quad (9)$$

$$f_k(\alpha, \beta) = (f_{k0},\ f_{k1},\ f_{k2},\ f_{k3}) \quad (10)$$

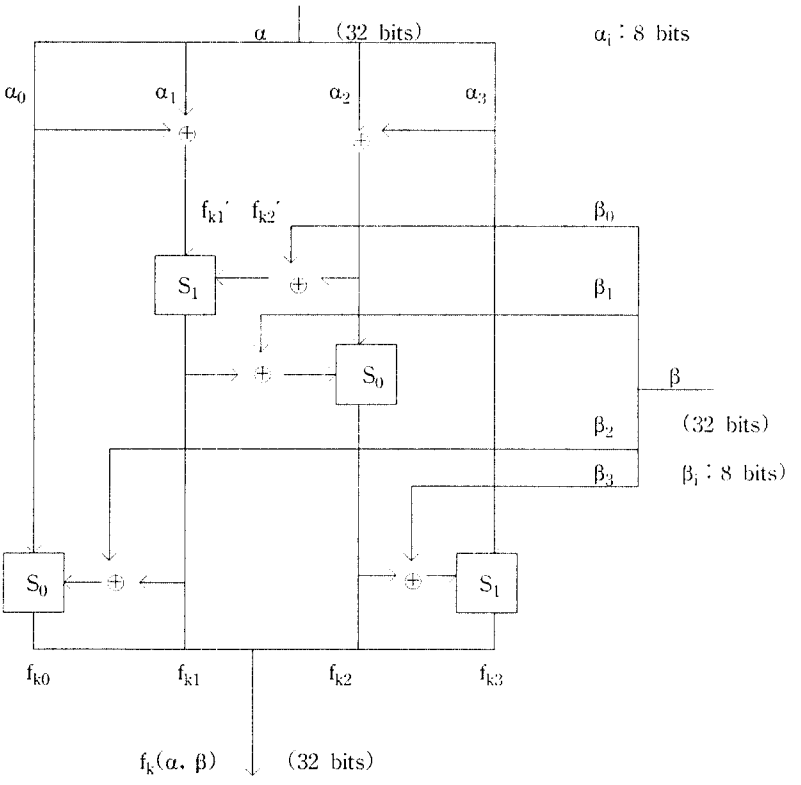


그림 2. f_k 함수

그림 3은 데이타 랜덤화 과정을 도시한 것이며 사용된 f함수는 그림 4와 같다. 그림 3과 그림 4의 과정을 사용된 기호를 이용하여 관계식으로 표현하면 다음과 같다.

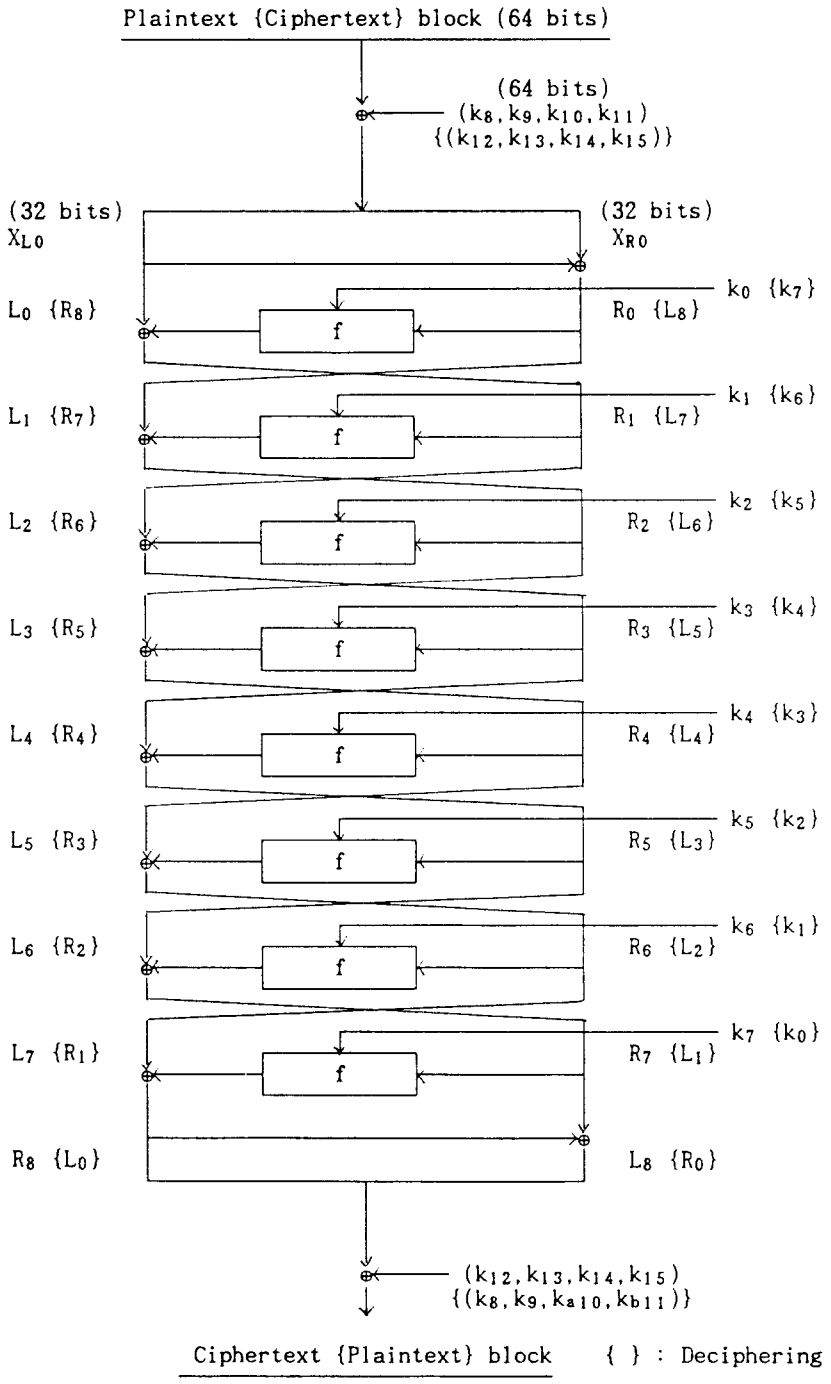


그림 3. 데이타 랜덤화과정 블럭도

$$L_r = R_{r-1} \quad (11)$$

$$R_r = L_{r-1} \oplus f(R_{r-1}, k_{r-1}) \quad (12)$$

$$f_1' = \alpha_1 \oplus \beta_0 \oplus \alpha_0 \quad (13)$$

$$f_2' = \alpha_2 \oplus \beta_1 \oplus \alpha_3 \quad (14)$$

$$f_1 = S_Q(f_1', f_2', Q=1) \quad (15)$$

$$f_2 = S_Q(f_2', f_1, Q=0) \quad (16)$$

$$f_0 = S_Q(\alpha_0, f_1, Q=0) \quad (17)$$

$$f_3 = S_Q(\alpha_3, f_2, Q=1) \quad (18)$$

$$f(\alpha, \beta) = (f_0, f_1, f_2, f_3) \quad (19)$$

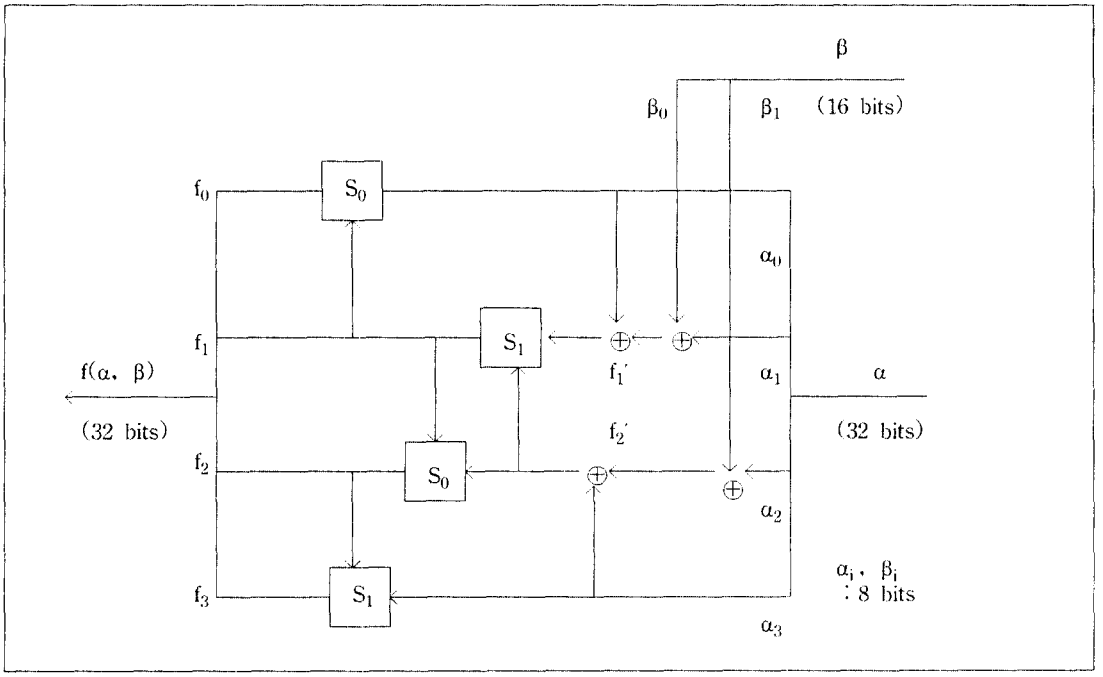


그림 4. f 함수

3. FEAL-8의 암호화 함수 특성 분석

FEAL-8에 사용된 S 함수, f_k함수, 및 f 함수의 특성을 조사함으로써 심볼간 상호의존도를 해석할 수 있다.

3.1 S함수 특성

f 함수와 f_k함수 내에 있는 S 함수는 한 바이트 데이타 대체 함수이다. S 함수는 두 입력 바이트 x및 y와 함수내의 고정된 상수 Q를 더하여 modulo 256을 행한 후 상위 비트쪽으로 두 비트 순회시킨다. 이 여기서 x와 y는 한 바이트 길이의 데이타이고 Q는 0 혹은 1이다. 그리고 ROT2(T)는 T를 상위 비트쪽으로 두 비트 순회시키는 함수이다. S 함수의 입출력 비트간 상호의존 확률을 나타내면 표 1과 같다.[6]

과정을 식으로 표현하면 다음과 같다.

$$S(x, y, Q) = ROT2(T) \quad (20)$$

$$T = x+y+Q \mod 256 \quad (21)$$

표 1. S 함수 입출력 심볼간 상호의존 행렬

[input byte]

[LSB]

$$Z=\begin{bmatrix} 1/64 & 1/32 & 1/16 & 1/8 & 1/4 & 1/2 & 1 & 0 \\ 1/128 & 1/64 & 1/32 & 1/16 & 1/8 & 1/4 & 1/2 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/4 & 1/2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1/8 & 1/4 & 1/2 & 1 & 0 & 0 & 0 & 0 \\ 1/16 & 1/8 & 1/4 & 1/2 & 1 & 0 & 0 & 0 \\ 1/32 & 1/16 & 1/8 & 1/4 & 1/2 & 1 & 0 & 0 \end{bmatrix}$$

3.2 f_k함수 특성

각각 32 비트인 입력 α와 β가 32비트 출력 $f_k(\alpha, \beta)$에 미치는 영향을 조사하여 f_k함수의 입출력 상관관계를 알아보면 식 (6), (7), (8), 및 (9)에 의해 표 2와 같이 된다. 행렬 Z의 제곱은 일반적인 행렬곱이 아니라 비트당 확률인자에 의한 곱이다.

표 2. f_k 함수 입출력 심볼간 상호의존 행렬
(a) α 입력과 f_k 출력
(b) β 입력과 f_k 출력

(a)

	α_0	α_1	α_2	α_3
f_{k0}	$Z+Z^2$	Z^2	Z^2	Z^2
f_{k1}	Z	Z	Z	Z
f_{k2}	Z^2	Z^2	Z^2+Z	Z^2+Z
f_{k3}	Z^3	Z^3	Z^2+Z^3	$Z+Z^2+Z^3$

(b)

	α_0	α_1	α_2	α_3
f_{k0}	Z^2		Z	
f_{k1}	Z			
f_{k2}	Z^2	Z		
f_{k3}	Z^3	Z^2		Z

3.3 f 함수 특성

f함수는 16비트 β와 32비트 α를 입력으로 받아 32비트 $f(\alpha, \beta)=(f_0, f_1, f_2, f_3)$를 출력한다. f함수는 입력 α는 f_k함수와 f함수에서 같은 위치에 작동되어, 출력까지 가는 과정이 동일하므로 입력과 출력 $f(\alpha, \beta)$ 사이의 상호의존 관계는 표 2.(a)와 같다. 입력 β와 출력 $f(\alpha, \beta)$ 사이의 상호의존 관계는 식 (15), (16), (17), 및 (18)에 의해 표 3.(b)와 같음을 알 수 있다.

표 2. f 함수 입출력 심볼간 상호의존 행렬
(a) α 입력과 f 출력 (b) β 입력과 f 출력

(a)

	α_0	α_1	α_2	α_3
f_{k0}	$Z+Z^2$	Z^2	Z^2	Z^2
f_{k1}	Z	Z	Z	Z
f_{k2}	Z^2	Z^2	Z^2+Z	Z^2+Z
f_{k3}	Z^3	Z^3	Z^2+Z^3	$Z+Z^2+Z^3$

(b)

	β_0	β_1(subkey)
f_0	Z^2	Z^2
f_1	Z	Z
f_2	Z^2	$Z+Z^2$
f_3	Z^3	Z^2+Z^3

4. FEAL-8의 심볼간 상호의존도 분석

FEAL-8 알고리듬에서 매라운드마다 출력되는 암호문의 각 비트는 입력된 평문과 키이의 함수로 간주될 수 있다. 만약 매라운드 출력되는 암호문의 한 비트가 입력된 평문의 모든 비트의 영향을 받아 변환되었다면, 이 출력 비트는 평문과 상호의존 한다고 한다. 또한 한 블럭의 암호문에 대해 평문과 상호의존하는 암호문 비트의 백분율(%)을 평문과 암호문간의 심볼간 상호의존도라 한다. 키이와 암호문 사이에도 같은 관계가 성립한다.

암호문과 평문간의 심볼간 상호의존도와 암호문과 키이간의 심볼간 상호의존도가 각각 100%를 갖기 위한 최소 라운드를 조사함으로써 FEAL-8 암호 알고리듬의 복잡성을 알아본다. 각 입력 비트 변화에 대해 각각의 출력 비트가 0.5이상의 확률로 영향을 받는다면 입출력 비트는 상호의존 한다고 한다.[6,7] 여기서 분석방법은 Meyer와 Matas의 방법을 사용하였다.[5]

4.1 평문과 암호문 심볼간 상호의존도

i라운드 출력에 대하여 j+1라운드 입력이 미치는 상호 의존 관계를 64×64 행렬 $G_{i,j}$로 나타내면 $G_{i,j}$의 (l, m)번째 원소 $g_{l,m}$ (l, m=0, 1, …, 63)은 i라운드 출력문 X_i의 1번째 비트가 j+1라운드 입력문 X_j의 m번째 비트에 상호의존할 확률을 나타낸다. 해석의 편의상 $G_{i,j}$를 4개의 부분 행렬로 분리하면 다음과 같다.

$$G_{i,j} = \begin{bmatrix} G_{i,j}^{(L,L)} & G_{i,j}^{(L,R)} \\ G_{i,j}^{(R,L)} & G_{i,j}^{(R,R)} \end{bmatrix}$$

부분 행렬 $G_{i,j}^{(L,R)}$은 i라운드 출력문 X_i의 좌반수 32비트 L_i가 j+1라운드 입력문 X_j의 우반부 32비트 R_j에 상호의존할 확률을 나타내는 32×32 행렬이다.

먼저 $G_{i,i-1}$을 구하면 식(11)에 의해 L_i의 어떠한 비트도 L_{i-1}에 상호의존하지 않으며, L_i는 R_{i-1}에 그리고 식 (12)에서 L_{i-1}는 R_i에 선형으로 상호의존하게 되며, R_i는 R_{i-1}에 표 3.(a)의 확률로 상호의존하게 되어 행렬 $G_{i,i-1}$은 아래와 같다.

BLANK $G_{i,i-1}^{(L,L)}$	LINEAR $G_{i,i-1}^{(L,R)}$
LINEAR $G_{i,i-1}^{(R,L)}$	Table 3.(a) $G_{i,i-1}^{(R,R)}$

Matrix $G_{i,i-1}$

이것을 식 (11), (12)를 이용하여 j+1라운드 입력과 i라운드 출력 사이의 상호의존 관계를 구하는 식으로 바꾸면 다음과 같다.

$$G_{i,j}^{(L,L)} = G_{i-1,j}^{(L,R)} \tag{24}$$

$$G_{i,j}^{(L,R)} = G_{i,j}^{(R,L)} = G_{i-1,j}^{(R,R)} \tag{25}$$

$$G_{i,j}^{(R,R)} = f(G_{i-1,j}^{(R,R)}) + G_{i-1,j}^{(L,R)} \tag{26}$$

또한 입력된 평문 X는 그림 3에서 X_{L0}와 X_{R0}로 분리되어 X_{L0}는 그대로 L_0가 되고 X_{R0}와 X_{L0}는 XOR되어 R_0가 되므로 이를 행렬 U로 나타내면 다음과 같다.

	X_{L0}	X_{R0}
L_0	LINEAR $U^{(L,L)}$	BLANK $U^{(L,R)}$
R_0	LINEAR $U^{(R,L)}$	LINEAR $U^{(R,R)}$

Matrix U

행렬 U와 식 (24), (25), 및 (26)을 이용하여 입력된 평문 X와 매 라운드 출력 X_i 사이의 입출력 비트간 상호의존도를 구하면 표 4와 같다.

4.2 키이와 암호문 심볼간 상호의존도

암호문과 입력된 키이 사이의 심볼간 상호의존도를 분석하기 위해서는 먼저 입력 키이와 암호화 과정의

표 4. FEAL8-의 평문과 암호문 심볼간 상호의존도

Round	FEAL-8				
i	L_i VS. X_{L0}	L_i V_s. X_{R0}	R_i V_s. X_{L0}	R_i V_s. X_{R0}	X_i V_s. X
1	3.13	3.13	44.34	41.99	23.14
2	44.34	41.99	99.61	99.61	71.39
3	99.61	99.61	100.00	100.00	99.80
4	100.00	100.00	100.00	100.00	100.00

각 라운드에서 사용되는 보조키이 사이의 심볼간 상호의존도를 알아야 한다. 앞에서와 같은 방법으로 상호의존도 행렬 G를 네개의 부분행렬로 나누어서 식(1), (2). 및 (3)을 이용하여 행렬 $G_{i,\,i-1}$을 구하면 아래와 같다.

BLANK $G_{i,\,i-1}^{(A,\,A)}$	LINEAR $G_{i,\,i-1}^{(A,\,B)}$
Table 2.(a) $G_{i,\,i-1}^{(B,\,A)}$	Table 2.(b) $G_{i,\,i-1}^{(B,\,B)}$

Matrix $G_{i,\,i-1}$

두라운드 이상 차이나는 상호의존 행렬을 구할 때에는 식 (2), (3)에 의해서 B_i는 A_{i-1}가 f_k 함수의 β입력으로 들어갔을 때의 입출력 상호의존 관계를 추가로 가지게 되며 이를 행렬 $G_{si,\,i-2}$로 나타내면 아래와 같다.

BLANK $G_{si,\,i-2}^{(A,\,A)}$	BLANK $G_{si,\,i-2}^{(A,\,B)}$
Table 2.(b) $G_{si,\,i-2}^{(B,\,A)}$	BLANK $G_{si,\,i-2}^{(B,\,B)}$

Matrix $G_{si,\,i-2}$

위의 행렬들을 사용하여 각 라운드 후의 행렬 상호의존 행렬을 구한다. 이때 보조 키이로 사용되는 부분은 출력의 B부분만이므로, 상호의존 행렬 전체에 대한 심볼간 상호의존도를 구해서는 안되며 출력의 아래 부분에 대해서만 상호의존도를 구해야 한다. 보조키이와 입력된 키이 사이의 상호의존도를 나타내는 행렬을 F라 하고, 상호의존도 행렬을 하단인 $G^{(B,\,A)}$, $G^{(B,\,B)}$을 32×64 행렬 F로 나타낸다.

$$F_i=[F_i^{(A)}\ F_i^{(B)}]=[G_{i,\,0}^{(B,\,A)}\quad G_{i,\,0}^{(B,\,B)}],\qquad 1\le i\le 8 \tag{27}$$

표 5는 입력키이와 보조키이간의 입출력 심볼간 상호의존도를 각 라운드별로 나타낸 것이다.

표 5. FEAL-8의 입력키이와 보조키이 심볼간 상호의존도

Round	FEAL-8		
i	k_i	k_i V_s. key	F_i V_s. key
1	k_0	20.02	28.27
	k_1	36.52	
2	k_2	60.94	71.39
	k_3	81.84	
3	k_4	93.16	96.14
	k_5	99.12	
4	k_6	100.00	100.00
	k_7	100.00	

보조 키이 생성 부분의 4라운드 후에 보조 키이는 입력된 키이에 100% 의존한다. 데이타 랜덤화 과정에서 첫번재 라운드 직전에 보조키이 k_8, k_9, k_{10} 및 k_{11}과 입력된 평문이 XOR되므로, 첫번째 라운드로 입력되기 전의 암호문의 키이 의존도는 보조키이 k_8, k_9, k_{10} 및 k_{11}의 입력키이 의존도와 같다. 그러므로 암호문의 입력키이 의존도는 첫 라운드 직전의 XOR후에 100%를 달성한다.

5. Lucifer, DES 및 FEAL-8의 심볼간 상호의존도 비교

표 6에 나타낸 바와 같이 Lucifer는 6라운드 후부터, 그리고 DES는 5라운드 후부터 암호문은 평문에 100%의 심볼간 상호의존도를 가지게 된다.[5, 8] 그러나 FEAL-8은 그보다 빠른 4라운드 후부터 100%의 심볼간 상호의존도를 가지며, Lucifer나 DES 보다 평문의 각 비트의 변화에 대해 암호문의 모든 비트의 변화가 더 빨리 일어남을 알 수 있다.

표 6. 평문과 암호문 심볼간 상호의존도

Round i	Lucifer	D E S	FEAL-8
1	2.34	6.25	23.14
2	10.05	32.06	71.39
3	32.98	73.49	99.80
4	68.25	96.90	100.00
5	93.36	100.00	100.00
6	100.00	100.00	100.00

표 5에서 알 수 있듯이 FEAL-8의 키이와 암호문간의 심볼간 상호의존도는 첫 라운드 바로 전부터 100%이다. Lucifer나 DES의 경우에는 암호화 과정의 각 라운드에 사용되는 보조 키이는 보조 키이 생성과정의 각각의 라운드에서 생성된 순서대로 사용되므로 입력된 키이와 보조 키이 그리고 보조 키이와 암호문 사이의 상호의존 관계를 모두 고려하여 입력키이와 암호문 간의 심볼간 상호의존도를 구해야 하며 그 결과는 표 7과 같다.[5, 8] 즉 Lucifer는 9라운드 후에, DES는 5라운드 후에 키이에 대한 심볼간 상호의존도가 100%이다.

6. 결 론

FEAL-8 알고리듬에서 사용된 암호화 함수인 S 함수, f_k함수, 및 f 함수의 특성을 조사하고 이를 이용하여 평문과 키이에 대한 암호문의 심볼간 상호의존도를 분석하였다. FEAL-8에서 평문에 대한 암호문의 심볼간 상호의존도는 4라운드에서 100%

표 7. 입력키이와 암호문 심볼간 상호의존도

Round i	Lucifer	D E S
1	0.78	5.36
2	4.53	44.87
3	16.87	87.72
4	46.47	98.21
5	77.89	100.00
6	93.53	100.00
7	98.75	100.00
8	99.76	100.00
9	100.00	100.00

이며, Lucifer와 DES의 경우는 6라운드와 5라운드에서 각각 100%이다. 키이에 대한 암호문의 심볼간 상호의존도는 FEAL-8의 경우 키이와 보조키이 사이의 심볼간 상호의존도가 4라운드에서 100%이므로 입력키이와 암호문 사이의 심볼간 상호의존도는 데이타 랜덤화과정의 첫 라운드 바로 전부터 100%가 된다. Lucifer나 DES의 경우에는 9라운드와 5라운드에 각각 100%의 상호의존도를 가진다. FEAL-8의 키이에 대한 심볼간 상호의존도는 첫 라운드를 시작하는 단계에서 100%이며, FEAL-8의 평문에 대한 암호화 함수 라운드수는 Lucifer나 DES에 비해 절반이나, 반면에 상호의존도는 보다 빨리 100%를 지니는 특성을 가지고 있다.

참 고 문 헌

1. A. Shimizu and S. Miyaguchi, "Fast Data Encipherment Algorithm FEAL," Eurocrypt pp. 267-278, 1987.

2. Henk C.A. van Tilborg, *An Introduction to Cryptology*, Boston, Kluwer Academic Publishers, chep. 6, chap. 7, 1987.

3. A. Sorkin, "Lucifer, a cryptographic algorithm", Cryptologia, vol. 8, no. 1, pp. 22-35, Jan. 1984.

4. National Bureau of Standards, Data Encryption Standard, U.S.FIFP PUB 46, pp. 1-18,

1977.

5. C.Meyer and S. Matyas, *Cryptography: A New Dimension in computer Data Security*, NewYork, John Wiley Sons, 1982.

6. W.Fumy, "On the F-function of FEAL", Advances in Cryptology Crypto'87, pp.434-438, Aug. 1987.

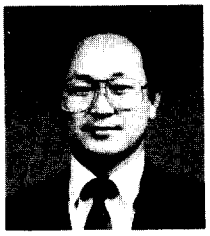
7. A.F. Webster, S.E. Tavares, "On the design of S-boxes", Eurocrypt pp.523-534. 1985.

8. 이훈재, 문상재, "LUCIFER와 DES에서의 심볼간 상호의존성에 관한 연구," 경북대학교 전자기술연구지, 제 8 권, pp.89-92, 1987년 8월.

□ 著者紹介

황 금 화(정회원)

경북대학교 전자공학과(학사)
경북대학교 전자공학과(석사)
주관심분야 : 암호이론 및 컴퓨터 네트워크 등



문 상 재(정회원)

1948년 4월
서울대학교 공업교육과(전자전공 학사)
서울대학교 대학원 전자공학과(석사)
미국 UNLA 공학박사(통신공학 전공)
금성전기주식회사 근무
미국 UCLA 연구조원 근무
미국 Satelite Tech. Management Inc. 근무/미국 UCLA Postdoctor 근무(Dept. of Elec. Eng)/
美國 OMNET 주식회사 Consultant 근무
현재 : 경북대학교 전자공학과 교수
주관심분야 : 부호기술 및 디지틀통신 등