배타적 배타논리를 이용한 DES(SX-DES) 키 확장

노 우 식°, 김 혁 구*
부천전문대학 전자계산과°
부천전문대학 전자과*

Expanding Effective DES Key using Self Exclusive XOR : SX-DES

Woo-Shik Rho°, Hyeog-Gu Kim*
Dept. Computer Science, Bucheon Tech College°
Dept. Electronics, Bucheon Tech College*

요 약

DES의 키 길이를 확장 시킴에 있어서 처리 속도의 저하없이 112 비트의 키를 사용할 수 있는 SX-DES 구조를 제안하고 SX-DES에서 DES의 P-Box가 SX-DES에 대한 Differential Crytanalysis 공격에 의해 키 길이가 감소되는 효과를 가지고 있으므로 P-Box를 재구성하여 SX-DES가 확장된 키 효과를 충분히 가질 수 있도록 하였다. 처리시간은 DES보다 2 % 정도 더 소요 되었다.

I. 서 론

DES는 미국 상무성 표준으로 채택되어 사용된 이후 지속적으로 키 길이가 짧은 것이 문제점으로 지적되어 왔다. 그리고, 1990년 Biham과 Shamir에 의해 평문의 입력 차이와 암호문의 차이를 분석한 Differential Cryptanalysis 공격방법을 발표하여 변형된 DES를 사용하는데 대한 위험성이 입증되었고[2], 1993년 마쯔이는 선형해독법을 발표함으로써 56 비트의 DES 알고리즘은 기지의 평문과 암호문 쌍을 이용한 공격 대상이 됨을 보여주고 있다[3]. 이 공격방법은 키의 전수 검사보다 빠른 DES 공격방법으로 주목 받고 있다. 그러나, 키 길이가 짧아서 발생하는 취약성 이외에는 DES가 공포된지 20여년이 지난 오늘날까지 큰 문제점은 알려지지 않고 있다.

따라서, DES의 골격은 그대로 유지한 DES-like 암호화 방식으로 키 길이를 확장한 방식들이 [5,6,7] 제안되었으나 이들은 기존의 DES와 호환성이 없거나 Differential Cryptanalysis 공격에는 취약함을 보인다. DES 블록을 이용한 확장 방법으로 Chained DES 방법[6]을 제안하였으나

Differential Cryptanalysis에 대해서는 확장된 키 효과를 얻을 수 없었고, GDES 또한 DC 공격에는 매우 취약하다[2]. 2중 DES는 'Meet-in-the-Middle' 공격에 취약하며[4], 3중 DES는 키 길이를 효과적으로 확장은 할 수 있으나 DES를 3회 반복하는데 필요한 3배의 연산을 해야하는 어려움이 있다[4].

본 논문에서는 XOR 특성을 사용하여 16 바이트의 데이터를 한 블럭으로 암호화하면서 키 길이를 112 비트의 효과를 갖도록 확장할 수 있는 방법을 제안한다. 이 방법은 전수 검사 방법에 대해서는 물론이고 Differential Cryptanalysis 공격에 대해서도 사용된 키 비트의 효과를 거둘 수 있다. 또한, 입력 블록의 데이터와 키 값을 동일하게 사용할 경우에는 기존의 DES와 호환성을 갖도록 할 수도 있다.

II. SX-DES의 제안

정의 1. **배타적 배타논리합(Self-exclusive XOR)**

집합 $X_B = \{B_1, B_2, ..., B_n\}$에서 B_i를 제외한 모든 구성원의 배타적 논리합을 B_i'라하면

$$B_i' = B_1 \oplus B_2 \oplus ... B_{i-1} \oplus B_{i+1} \oplus ... \oplus B_{n-1} \oplus B_n$$

가 된다. 이 때, B_i'을 집합 X_B에서 B_i의 배타적 배타논리합이라 정의한다.

정의 2. **배타적 배타논리합의 집합**

집합 X_B의 각 구성원의 배타적 논리합들을 구성원으로하는

$X_B' = \{B_1', B_2', ..., B_n'\}$를 배타적 배타논리합의 집합이라 정의한다.

정리 1. **배타적 배타논리합의 역연산 특성**

집합 $X_B = \{B_1, B_2, ..., B_n\}$의 (이 때, n은 짝수) 배타적 배타논리합의 집합 X_B'가의 구성원을 알고 있을 때, 집합 X_B' 로부터 집합 X_B를 배타적 배타논리합 연산으로 구할 수 있다.

(증명) 정리의 증명을 위해서는 임의의 i (= 1,2, ..., n)에서 $(B_i')' = B_i$를 만족하면 된다.

B를 집합 X_B의 모든 구성원들의 배타적 논리합이라하고 B'을 집합 X_B'의 모든 구성원들의 배타적 배타논리합이라하자.

즉, $B = \bigoplus_{i=1}^{n} B_i = B_1 \oplus B_2 \oplus \cdots \oplus B_n$ 이고

$B' = \bigoplus_{i=1}^{n} B_i' = B_1' \oplus B_2' \oplus \cdots \oplus B_n'$ 이다.

$$(B_i')' = (\bigoplus_{j=1}^{n} B_j') \oplus B_i'$$
$$= (\bigoplus_{j=1}^{n} (\bigoplus_{k=1}^{n} B_k \oplus B_j)) \oplus ((\bigoplus_{j=1}^{n} B_j) \oplus B_i)$$

$B = \bigoplus_{i=1}^{n} B_i$ 이므로

$$(B')' = \bigoplus_{j=1}^{n} (B \oplus B_j) \oplus (B \oplus B_i)$$
$$= (\bigoplus_{j=1}^{n} B) \oplus (\bigoplus_{j=1}^{n} B_j) \oplus B \oplus B_i$$
$$= (\bigoplus_{j=1}^{n} B) \oplus B \oplus B \oplus B_i$$

이 때, $B \oplus B$ 는 항상 0 이므로

$$(B_i')' = (\bigoplus_{j=1}^{n} B) \oplus B_i$$

이다. 따라서, n이 짝수일 때, $\bigoplus_{j=1}^{n} B$는 항상 0가 되므로

임의의 i $(=1,2,\ldots,n)$ 에 대하여 $(B_i')' = B_i$ 이다.

그림 1은 4개의 구성원을 갖는 집합의 배타적 배타논리합의 블록도이다. 정리 1에 의하여 입력 집합 $\{L'_{j,1}, R'_{j,1}, L'_{j,2}, R'_{j,2}\}$로부터 배타적 배타논리합 집합을 $\{L_{j,1}, R_{j,1}, L_{j,2}, R_{j,2}\}$이라 하자. 집합 $\{L_{j,1}, R_{j,1}, L_{j,2}, R_{j,2}\}$로부터 이 집합의 배타적 배타논리합 집합은 $\{L'_{j,1}, R'_{j,1}, L'_{j,2}, R'_{j,2}\}$가 된다.

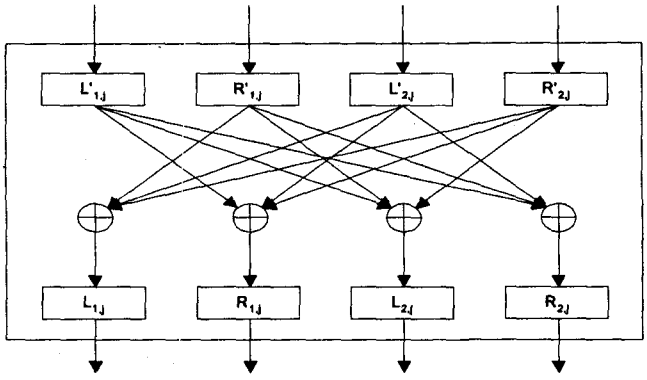

그림 1. j 번째 라운드에서 배타적 배타논리합

이러한 배타적 배타논리합의 특성을 이용하여 그림 2에 나타난 블록도의 SX-DES (Self-exclusive XORed DES)를 제안한다. SX-DES의 구성은 기본적으로 2 개의 DES 블록을 갖

는다. 두 블록의 입력 평문을 각각 D_1, D_2라하고 암호화에 적용되는 키를 K_1, K_2라 하자. j 번째 라운드의 입력을 $L_{j-1,1}$, $R_{j-1,1}$, $L_{j-1,2}$ 그리고, $R_{j-1,2}$라 하고, 이 라운드의 출력을 $L_{j,1}$, $R_{j,1}$, $L_{j,2}$ 그리고, $R_{j,2}$ 라 하자.

2.1 암호화 방법

두 블록은 병렬로 각각 DES 암호화 라운드를 실행하여 라운드 출력을 내 놓으며 j가 짝수면 그대로 다음 라운드의 입력이 되고, j가 홀수면 DES 라운드의 출력 집합 $\{L'_{j,1}, R'_{j,1}, L'_{j,2}, R'_{j,2}\}$에 대하여 배타적 배타논리합을 취하여 다음 라운드의 입력으로 사용한다.

즉, j 가 짝수면

$$R_{j,1}=R_{i,1}'=f(R_{j-1,1}, K_{j,1})\oplus L_{j-1,1} \quad (1)$$

$$L_{j,1}=L_{j,1}'=R_{j-1,1} \quad (2)$$

$$R_{j,2}=R_{j,2}'=f(R_{j-1,2}, K_{j,2})\oplus L_{j-1,2} \quad (3)$$

$$L_{j,2}=L_{j,2}'=R_{j-1,2} \quad (4)$$

이고, j 가 홀수면

$$R_{j,1}'=f(R_{j-1,1}, K_{j,1})\oplus L_{j-1,1} \quad (5)$$

$$L_{j,1}'=R_{j-1,1} \quad (6)$$

$$R_{j,2}'=f(R_{j-1,2}, K_{j,2})\oplus L_{j-1,2} \quad (7)$$

$$L_{j,2}'=R_{j-1,2} \quad (8)$$

(5), (6), (7), (8)을 배타적 배타논리합을 적용하여 다음 라운드의 입력 값

$$R_{j,1}=L_{j,1}'\oplus L_{j,2}'\oplus R_{j,2}' \quad (9)$$

$$L_{j,1}=R_{j,1}'\oplus L_{j,2}'\oplus R_{j,2}' \quad (10)$$

$$R_{j,2}=L_{j,1}'\oplus R_{j,1}'\oplus L_{j,2}' \quad (11)$$

$$L_{j,2}=L_{j,1}'\oplus R_{j,1}'\oplus R_{j,2}' \quad (12)$$

을 구한다. 즉,

$$L_{j,1}= f(R_{j-1,1}, K_{j,1})\oplus L_{j-1,1}\oplus R_{j-1,2}\oplus f(R_{j-1,2}, K_{j,2})\oplus L_{j-1,2} \quad (13)$$

$$R_{j,1}=R_{j-1,1}\oplus R_{j-1,2}\oplus f(R_{j-1,2}, K_{j,2})\oplus L_{j-1,2} \quad (14)$$

$$L_{j,2}= f(R_{j-1,2}, K_{j,2})\oplus L_{j-1,2}\oplus R_{j-1,1}\oplus f(R_{j-1,1}, K_{j,1})\oplus L_{j-1,1} \quad (15)$$

$$R_{j,2}= R_{j-1,2}\oplus R_{j-1,1}\oplus f(R_{j-1,1}, K_{j,1})\oplus L_{j-1,1} \quad (16)$$

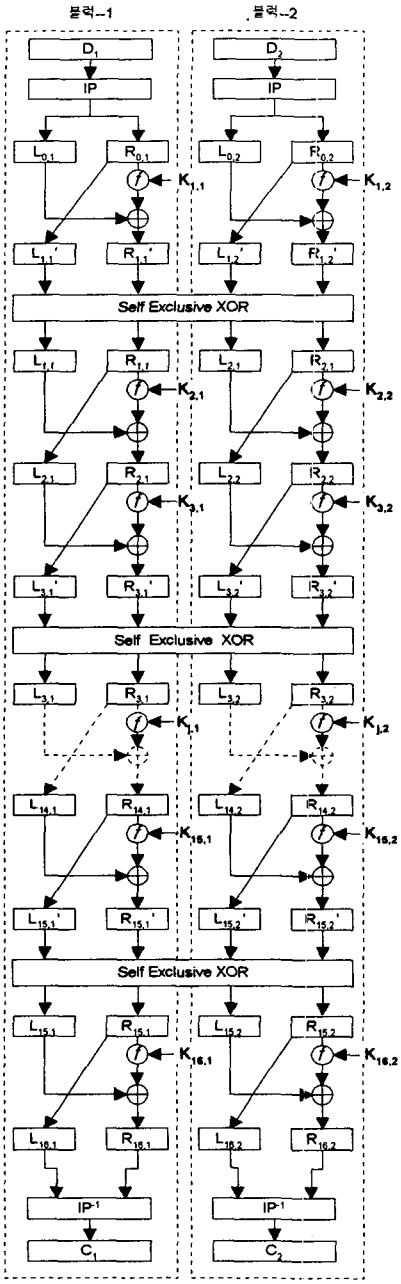

그림 2. 제안된 SX-DES 알고리즘

로 표현된다. 식 (1)~(4)와 (13)~(16)를 보면 j 번째 라운드의 출력은 모두 j 번째 라운드의 입력으로부터 구할 수 있다.

2.2 복호화 방법

복호시에는 j가 짝수면 식 (2)와 (4)에서 각각

$$R_{j-1,1} = L_{j,1}' \tag{17}$$

$$R_{j-1,2} = L_{j,2}' \tag{18}$$

가 되고, 식 (1)과 (3)에서

$$L_{j-1,1} = f(R_{j-1,1}, K_{j,1}) \oplus R_{j,1} \tag{19}$$

$$L_{j-1,2} = f(R_{j-1,2}, K_{j,2}) \oplus R_{j,2} \tag{20}$$

식 (17), (18)을 식 (19), (20)에 각각 대입하면

$$L_{j-1,1} = f(L_{j,1}, K_{j,1}) \oplus R_{j,1} \tag{21}$$

$$L_{j-1,2} = f(L_{j,2}, K_{j,2}) \oplus R_{j,2} \tag{22}$$

를 구할 수 있다. 따라서, 식 (17), (18), (21), 그리고, (22)에서 j 라운드의 값으로 j-1 번째 라운드의 입력 값을 구할 수 있다.

또, j 가 홀수면 식 (5), (6), (7) 그리고, (8)로부터

$$L_{j-1,1} = f(R_{j-1,1}, K_{j,1}) \oplus R_{j,1}' \tag{23}$$

$$R_{j-1,1} = L_{j,1}' \tag{24}$$

$$L_{j-1,2} = f(R_{j-1,2}, K_{j,2}) \oplus R_{j,2}' \tag{25}$$

$$R_{j-1,2} = L_{j,2}' \tag{26}$$

를 구한 다음 식 (23)~(26)으로부터

$$L_{j-1,1}' = L_{j,1}' \oplus L_{j,2}' \oplus f(L_{j,2}', K_{j,2}) \oplus R_{j,2}' \tag{27}$$

$$R_{j-1,1}' = f(L_{j,1}', K_{j,1}) \oplus R_{j,1}' \oplus L_{j,2} \oplus 'f(L_{j,1}', K_{j,2}) \oplus R_{j,2}' \tag{28}$$

$$L_{j-1,2}' = L_{j,2}' \oplus L_{j,1}' \oplus f(L_{j,1}', K_{j,1}) \oplus R_{j,1}' \tag{29}$$

$$R_{j-1,2}' = f(L_{j,2}', K_{j,2}) \oplus R_{j,2}' \oplus L_{j,1} \oplus 'f(L_{j,1}', K_{j,1}) \oplus R_{j,1}' \tag{30}$$

를 구할 수 있다. 식 (27)~(30)에서 *j-1* 번째 라운드의 값을 그 뒤 라운드인 *j* 번째 라운드의 값으로부터 구할 수 있다. 또한, 식 (27)~(30)은 식 (13)~(16)와 같은 연산이므로 적용되는 라운드 키의 순서만 역으로 사용하면 복호화 과정도 암호화 과정과 같은 알고리즘을 사용할 수 있다.

2.3 P-Box의 개선

DC 공격을 성공적으로 하기 위해서는 높은 확률로 *n*-라운드 특성을 구성할 수 있어야 한다. 16-라운드 SX-DES 공격에 사용할 *2*-라운드 특성을 구성하기 위하여 그림 3(a)와 같이 *2*-라운드 특성이 구성될 때, B와 D의 값이 0가 될 때, 출력 XOR 값이 확률 1 로 0가 되므로 그림 3(b)와 같이 *2*-라운드 특성이 높은 확률로 구성될 수 있다.

그림 3(b)의 *2*-라운드 특성을 구성할 확률은 C --> A⊕C 확률 *p*와 A-->A⊕C 확률 *q*의 곱으로 나타낼 수 있다. 즉, *2*-라운드 특성을 구성할 확률은 $p \cdot q$ 이다.

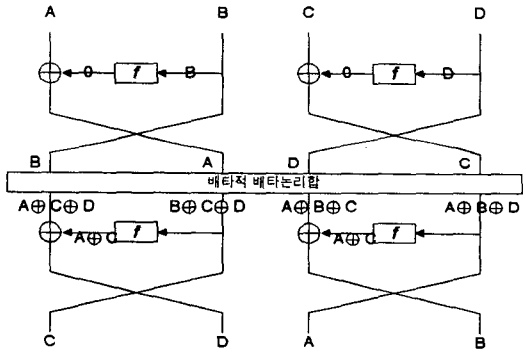

그림 3(a) 2-라운드특성 구성요건

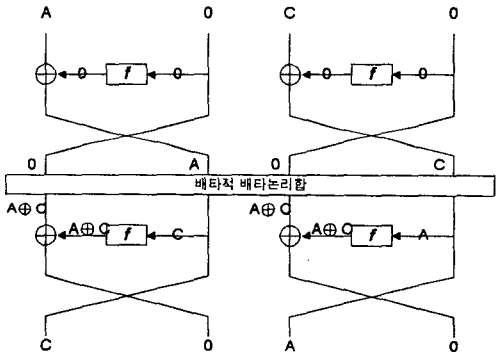

그림 3(b) 높은 확률로 2-라운드특성 구성 시의 입력 값

그림 3(b)에서 A = (e000 0004$_x$), C = (e000 0006$_x$)가 입력 XOR 값일 때, A⊕C 는 (0000 0002$_x$)가 되어 DES의 f 함수 의 XOR 분포에서 2-라운드 특성이 구성된다.
A를 확장하면 (1c 00 00 00 00 00 00 09$_x$) 가 되어

S1-Box : 1c$_x$ --> 1 확률은 10/64 이고
S8-Box : 09$_x$ --> 0 확률은 8/64 이므로
A --> A⊕C 확률 $p = \frac{10 \times 8}{64 \times 64}$ 가 된다.

또, 같은 방법으로 C를 확장하면 (1c 00 00 00 00 00 00 0d$_x$) 가 되므로

S1-Box : $1c_x$ --> 1 확률은 10/64 이고
S8-Box : $0d_x$ --> 0 확률은 6/64이므로
C --> A⊕C 확률 $q = \frac{10 \times 6}{64 \times 64}$ 가 되므로

2-라운드 반복특성 구성 확률은 $\frac{10 \times 8 \times 10 \times 6}{64 \times 64 \times 64 \times 64} \cong \frac{1}{3495}$ 이다.

이와 같이 높은 확률로 *2*-라운드 반복특성이 구성될 수 있는 것은 S1-Box의 출력 비트가 P-Box 치환에 의하여 인접한 S8-Box의 입력으로 사용되기 때문에 2개의 S-Box 입력이 0이 아닌 형태로 *2*-라운드 특성이 구성될 수 있기 때문이다.

따라서, 2개 이상의 S-Box 입력이 0이 되지 않도록 하기 위하여 P-Box 재배열을 다음의 조건에 따라 재구성하도록 한다.

조건 1. 각각의 S-Box 출력 4 비트는 자신의 블록과 자신과 인접한 S-Box블록으로 재배열되지 않도록 한다.

조건 2. 출력 4 비트는 하나의 블록에 1 비트만 재배열되도록 한다.

조건 3. s 번째 S-Box 출력 4 비트 (b1,b2,b3,b4)의 가운데 비트 (b2 혹은 b3) 중 1 비트가 재배열된 S-Box 블록을 t 번째 블록이라 할 때, t 번째 블록의 가운데 비트는 s 번째 S-Box 블록으로 재배열되지 않는다.

P-Box 재배열 구성을 조건 1과 조건 2를 만족하도록 표 1에 나타내었다.

표 1. 제안된 P-Box 재배열

구 분	S1-Box				S2-Box				S3-Box				S4-Box			
S-Box 출력 비트	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
P-Box 출력 비트	23	15	25	10	18	13	21	26	27	20	4	29	30	24	28	7
구 분	S5-Box				S6-Box				S7-Box				S8-Box			
S-Box 출력 비트	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
P-Box 출력 비트	2	9	8	31	11	5	32	1	14	12	19	3	16	17	6	22

III. SX-DES의 비도

DES의 비도는 전수 검사, Differential Cryptanalysis 공격, 선형 해독법 등이 사용 될 수 있는데 본 논문에서는 전수 검사와 Differential Cryptanalysis에 대한 비도를 분석한다.

3.1 전수 검사

K_1과 K_2는 각각 2 개의 DES 블록에 적용된 키이다. 식 (13)과 (16)에서 $L_{j,1}$, $L_{j,2}$는 각각 K_1과 K_2, 의 라운드 키 모두에 종속된 함수이다. $L_{j,1}$, $L_{j,2}$는 $j+1$ 번째 라운드에서 식 (1), (3)과 같이 $R_{j+1,1}$, $R_{j+1,2}$에 영향을 주므로 K_1, K_2는 두 DES 블록에 서로 영향을 준다. 따라서, f 함수는 확장 재배열 후 라운드 키와 XOR를 취한 다음 S-Box 치환, 그리고 P-Box 재배열을 포함하고 있으며 S-Box 치환이 비선형이므로 한 비트의 키 변화도 최종 출력의 모든 비트에 영향을 미치게된다. SX-DES에서 키를 전수 검사하기 위해서는 2^{112}개의 키를 검사하여야 한다.

3.2 Differential Cryptanlaysis

표 1의 P-Box 재배열은 조건 1, 2, 그리고, 3에 의하여 만들어 졌으므로 두 개의 0이 아닌 S-Box 입력 값으로,

A --> (A ⊕ C) , C --> (A ⊕ C) 를 구성하는 확률을 구성하지 못한다.

따라서, SX-DES를 공격하기 위해서는 A = C 일 때 2-round 특성을 구성할 수 있다. 그림 5에서

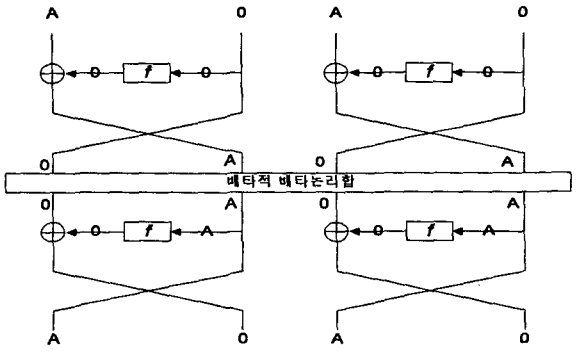

그림 5. (A 0 A 0) 일 때의 2-라운드 특성

A --> 0 가 될 최상의 확률은 A = (1960 0000x) 일 때, A를 확장 재배열을 취하면
(03 32 2c 00 00 00 00 00x)가 되고

S1-Box : 03x --> 0 확률 14/64,
S2-Box : 32x --> 0 확률 8/64,
S3-Box : 2cx --> 0 확률 10/64로 구성되므로

SX-DES의 2-라운드 반복 특성은 확률 $p = \frac{14\times6\times10\times14\times6\times10}{64\times64\times64\times64\times64\times64} \cong \frac{1}{54756}$ 로 구성된다.

DES에서 2-라운드 반복 특성을 구성할 확률이 1/234 이므로, 이 결과는 SX-DES를 Differential Cryptanalysis 공격시 DES에 비해 두 배의 키 효과를 가지는 것을 말한다.

3.3 DES를 변형한 다른 알고리즘과 비교

그림 5는 3중 DES 알고리즘을 블록도로 나타낸 것이다. 3 중 DES 알고리즘은 112 비트의 키 효과를 얻기 위하여 3번의 DES 처리과정을 반복하므로 3배의 시간이 소요된다. 또, 두 개의 DES 블록을 단순히 Chaining 한 경우에는 DC 공격에 취약하다.

표 2. DES 변형 알고리즘의 비교

	DES (기존)	SX-DES	3 DES	Chained DES
키 비트 수	56	112	112	112
암복호화 속도	1	1.02	3	1
DC 공격의 복잡도	2^{55}	2^{110}	약 2^{170}	2^{56}
키 효과	56 비트	112 비트	112 비트	57 비트
DES와 호환성	N/A	있음	있음	있음

IV. 결 론

DES의 키 길이의 문제점과 3-DES의 처리속도 문제점을 해결할 수 있는 방안인 SX-DES 알고리즘은 처리 속도의 저하 없이 112 비트 길이로 키를 확장할 수 있는 구조이다. DES의 P-Box를 변경하지 않고 SX-DES를 구성할 경우 DES와 호환이 가능하나 Differential Cryptanalysis 공격으로 인하여 키 길이의 증가 효과가 감소될 수 있다. 이를 개선하기 위한 방안으로 P-Box를 재구성하여 SX-DES가 확장된 키 효과를 충분히 가질 수 있도록 하였다. 제안된 SX-DES는 키 길이를 2배로 확장시키면서도 처리시간은 DES에 비해 약 2 % 증가에 불과하다. 또한, 논문에는 언급하지 않았으나 4개의 DES 블록을 유사한 방법으로 구현함으로써 224 비트의 키 길이 증가 효과도 가질 수 있다. 제안된 SX-DES의 또 다른 공격방법인 선형 공격법에 대하여는 연구 중에 있다.

참고문헌

1. Charles Pfleeger, Security in Computing, Prentice Hall, 1989, pp 106-107
2. Eli Biham and Adi Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, No. 4, 1991,pp.3-72
3. M. Matsui, "Linear Cryptanalysis of DES Cipher (I)", Symposium on Cryptography and Information Security '93, 1993
4. Ralph C. Merkle, Martin E. Hellman, "On the Security of Multiple Encryption", Communications of the ACM, July 1981 Vol.24 No. 7 pp.465-467
5. 임웅택, "EX-DES의 설계와 Differential Cryptanalysis에 관한 연구", 국방대학원 석사학위논문, 1992
6. 이상번, "DES 키 길이 확장에 관한 연구", 국방대학원 석사학위논문, 1991
7. 윤용정, 공헌택, 남길현, "80 비트 블록 암호알고리즘(80-DES)의 설계 및 비도 분석에 관한 연구,vol. 5 No. 1, 통신정보보호학회 논문지, 1995