80비트 블록 암호알고리듬(80-DES)의 설계 및 비도분석에 관한 연구

o
윤용정 공헌택 남길현
국 방 대 학 원

A Study on the Design and Cryptanalysis of 80-bit Block Cipher Algorithm(80-DES)

Yong-Jung Yoon, Hun-Taek Kong and Kil-Hyun Nam
National Defense University

요 약

Differential Cryptanalysis(DC) 및 선형암호분석 공격방법은 DES와 같은 비밀키 암호알고리듬을 실질적으로 공격할 수 있는 효과적인 방법들이다. 본 논문에서는 DC 및 선형암호분석을 통한 DES의 취약점을 분석하고 이를 보완할 수 있는 효과적인 80비트 블록 암호알고리듬을 설계하였다. 설계된 암호알고리즘은 DES보다 일반 특성과 DC 및 선형암호분석 공격에 대한 비도를 향상시킨 것으로 분석되었다.

1. 서 론

암호알고리듬 중 세계적으로 널리 알려진 DES(Data Encryption Standard)는 1977년 국가 및 국제 표준 알고리듬으로 채택된 이래 현재까지 사실상 세계 표준암호로서 주로 금융망과 상업용 네트워크를 중심으로 사용하고 있다. 그러나 DES의 안전성에 관하여 발표 초기부터 암호화 키의 크기에 대한 적정성과 S-box 설계기준의 비공개성으로 오늘날까지 많은 논쟁이 있었다. 키 56비트는 너무 짧아 Diffie와 Hellman이 전수검사(exhaustive) 공격에 취약하다고 지적하였다[1]. 또한 CRYPTO'93에서는 캐나다의 Wiener가 DES에 대한 공격이 Key search machine 설계를 발표하여 전수검사 공격방법을 고속화하여 실제적으로 DES에 공격이 가능하다는 것을 제시하였다.

Biham과 Shamir가 발표한 Differential Cryptanalysis(DC)[2]와 일본의 마쯔이가 EUROCRYPT'93에서 발표한 선형암호분석(Linear Cryptanalysis)은 비교적 실질적으로 DES를 공격할 수 있는 방법이다.

더우기 NSA가 1990년대 이후에는 DES를 더 이상 지원하지 않겠다는 뜻을 공식적으로 발표함에 따라 DES는 이제 충분한 안전성을 보장 받을 수 없게 되었으며 DES와 유사한 암호알고리듬 설계시에는 반드시 전수검사 공격뿐만 아니라 DC 및 선형암호분석 공격에 대처할 수 있는 방법이 함께 연구되어야 할 것이다.

본 논문에서는 DES에 대한 일반적인 분석과 전수검사 공격, DC, 그리고 선형암호분석을 통하여, 이러한 공격방법에 강할 수 있는 80비트 블록 암호알고리듬(80-DES)을 설계하고 이에 대한 비도분석을 연구한다.

2. DES 암호알고리듬 분석과 공격방법

DES에서 비도를 결정하는 중요한 부분은 S-box테이블의 비선형성에 영향을 받는 것으로 일반적인 특성 분석에 따른 설계 기준과 주요 공격방법은 다음과 같다.

2.1 일반적인 특성과 설계기준

S-box는 비선형적이어야 하고, 입력에 밀접한 관계가 있지 않아야 한다.

SAC(Strict Avalanche Criterion)[5][6][7] 조건 으로 각 S-box에서 입력 i번째 비트가 complement 될 때 출력 j번째 비트가 변화될 확률은 0.5에 근접해야 한다.

각 S-box에서 입력 k번째 비트가 complement 될 때 출력 j번째 비트의 변화에 대한 상관계수를 $\rho_{ij}(k)$라 하면, 상관계수는 0에 근접해야 한다.

Bijection[8] 조건으로 각 S-box 테이블의 행과 열값은 각 엔트리 에 중복없이 일 대 일 대응되어야 한다.

2.2 Differential Cryptanalysis(DC) 공격방법

DC는 특정한 평문쌍들(plaintext pairs)의 차이(difference)와 이에 대응하는 암호문쌍들(ciphertext pairs)의 차이 관계를 통계적으로 분석하여 적용된 키를 찾는 선택평문 공격방법이다. DES의 공격은 최종 라운드 암호함수로부터 시작되는데 최종 라운드 암호함수의 입력쌍은 암호문의 우측 32비트와 동일하므로 출력XOR를 N-라운드 특성을 이용하여 비교적 높은 확률로 예측할 수 있다. N-라운드 특성은 확률이 높은 특정한 평문쌍을 첫 라운드에 사용하여 중간 라운드들에 확률이 높은 입력XOR가 입력되게 함으로써 최종 N-라운드에 비교적 확률이 높은 입력XOR와 출력XOR가 발생되도록 축소된 N-라운드를 구성할 수 있는 특성을 말한다.

2.3. 선형암호분석(Linear Cryptanalysis)공격방법

선형암호분석[3]은 DES 암호알고리듬에 대하여 그 평문과 암호문의 관계를 비트 단위로 선형근사 시키기 위해서 DES 암호의 비선형 요소인 S-box의 입출력간의 상관관계를 조사하고 S-box 중에서 편차가 가장 큰 입출력을 선택하여 선형근사식을 유도한 후 이 근사식을 암호함수로 부터 알고리듬 전체로 확장하고, 최종적으로 평문에서 암호문에 이르는 일련의 확률적 선형 비트 경로를 구성하여 그 경로에 영향을 주는 키 비트를 전수검사 방법으로 구하는 방법이다.

이 방법으로 16-라운드 DES 에서도 1.76×2^{46} 개의 기지 평문이 있으면 무시할 정도의 메모리 량으로 키의 26 비트를 구하는 것이 가능하고 나머지 30 비트는 전수 검사를 통하여 용이하게 찾을 수 있다[4].

이상에서 알 수 있듯이 DES가 암호학적으로 강할 조건은 DC와 선형암호분석 등에 대처할 수 있도록 S-box를 설계하는 것이 매우 중요한 문제라고 하겠다.

3. 80비트 블록 암호알고리듬(80-DES)의 설계

3.1 80-DES의 설계

그림 1은 새로 제안하는 80-DES의 암호화 및 복호화 과정이다. 80-DES는 기존의 DES의 기본 구조를 그대로 유지하되, 키의 길이를 80비트로 증가시켰다. 이에 따른 키 스케줄은 80비트의 키를 그대로 사용하도록 하여 선택재배열 PC-1과 PC-2를 생략하였다. 또한 초기재배열(IP:Initial Permutation)과 마지막 라운드 후의 최종재배열(IP^{-1})은 비도에는 영향을 주지 않는 일대일 사상이므로 암복호화 효율을 높이기 위하여 삭제하였다. 암호함수는 80비트 입력 블록의 우측 40비트가 입력되도록 하였으며, 따라서 80-DES의 확장재배열(E) 테이블은 입력이 자신의 두 배인 80비트로 확장 재배열되도록 하였다.

3.1.1 확장재배열(E) 및 재배열(P) 설계

재설계한 10개의 S-box 테이블은 입력 8비트중 4비트씩을 행과 열값으로 사용하여 4비트 출력을 얻을 수 있도록 16행 16열로 구성하였다. 따라서 여기에 맞추어 수정된 확장재배열 테이블(E)은 입력 각 비트는 반드시 두 개의 S-box에 영향을 주도록 구성하였다[9]. 출력의 길이가 40비트로 늘어남에 따라 재배열 테이블(P)도 다시 설계 하였다.

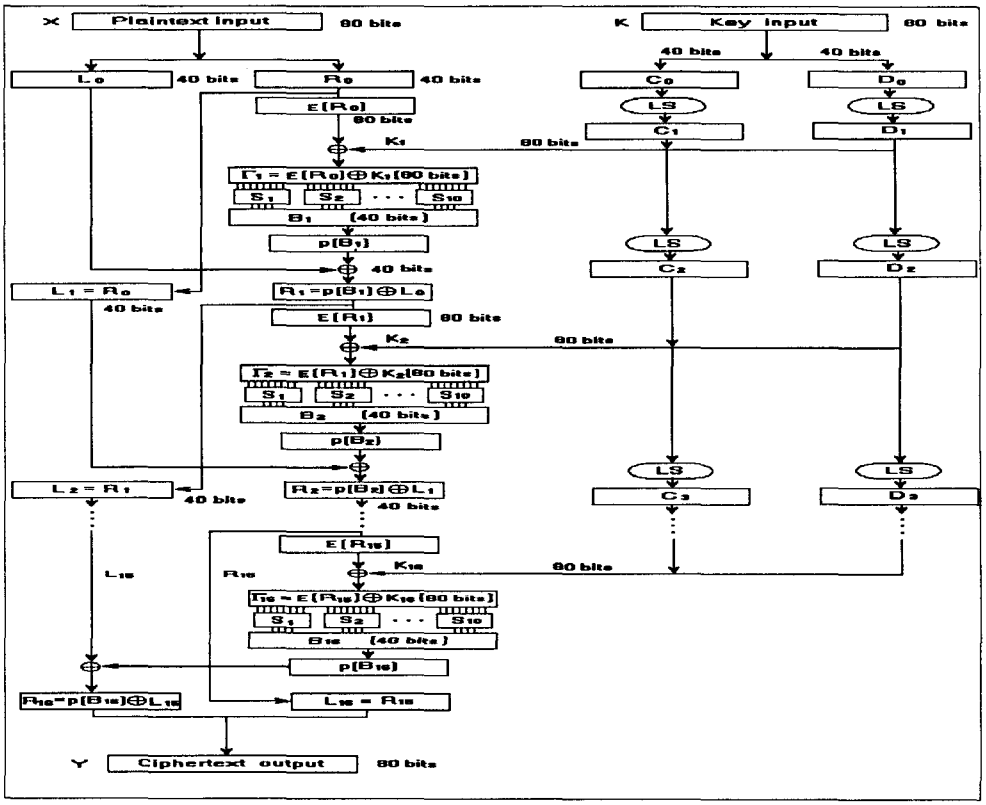

그림 1. 80-DES의 암호화 및 복호화 과정

표 1은 새로 설계된 80-DES의 확장재배열과 재배열 테이블이다.

표 1. 80-DES의 E테이블 및 P테이블

39	40	1	2	3	4	5	6
3	4	5	6	7	8	9	10
7	8	9	10	11	12	13	14
11	12	13	14	15	16	17	18
15	16	17	18	19	20	21	22
19	20	21	22	23	24	25	26
23	24	25	26	27	28	29	30
27	28	29	30	31	32	33	34
31	32	33	34	35	36	37	38
35	36	37	38	39	40	1	2

32	3	19	34
25	10	22	38
30	14	33	28
18	6	8	39
24	29	2	36
12	27	15	31
5	37	20	11
1	35	40	7
13	21	9	4
26	17	23	16

3.1.2 키 스케줄 설계

키 스케줄은 암호함수에 입력이 확장재배열(E)을 거친 80비트 키와 XOR 연산을 위하여 80비트를 사용하게 되는데 키의 블록을 좌우측 40비트씩으로 나누어 각각 홀수 라운드에는 2비트, 짝수 라운드에는 3비트씩을 왼쪽으로 쉬프트하여 마지막 라운드에서는 키 레지스터값을 최초의 위치대로 환원할 수 있도록 설계하였다.

3.1.3 S-box 설계

본 연구에서는 S-box 테이블의 설계는 비선형성 특성을 갖고 Bijection[8] 조건을 만족시킬 수 있도록 하기 위하여 모든 입력에 대해 동일한 확률값을 갖고 출력을 생성하는 state diagram의 일종인 Bruijn diagram을 사용하였다[9]. 이 state diagram은 16개의 각 상태 박스에 초기값(0~15)을 랜덤하게 주어 상태 전이에 따라 출력은 모두 1/16의 동일한 확률로 중복됨이 없이 배치할 수 있다.

표 2. 80-DES의 S_1-box테이블

행 ($b_5b_6b_7b_8$)	열($b_1b_2b_3b_4$)															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	8	11	15	14	4	12	3	5	6	10	7	13	1	9	2
1	5	12	15	11	3	2	8	14	0	9	13	1	10	7	6	4
2	14	10	9	6	0	1	13	5	3	15	8	6	12	4	11	7
3	3	13	6	9	5	7	10	0	14	11	12	4	8	2	15	1
4	6	1	3	14	15	10	7	11	9	0	4	12	2	8	5	13
5	9	7	14	3	11	13	1	15	6	5	2	8	4	12	0	10
6	15	4	5	0	6	8	2	9	11	14	1	13	7	10	3	12
7	11	2	0	5	9	12	4	6	15	3	7	10	1	13	14	8
8	13	11	8	7	12	5	14	1	4	2	9	15	0	3	10	6
9	4	14	7	8	1	6	11	12	13	10	0	3	9	15	2	5
10	12	9	10	2	13	3	0	4	1	7	11	6	14	5	8	15
11	1	0	2	10	4	15	9	13	12	8	14	5	11	6	7	3
12	2	3	1	12	7	9	15	8	10	13	5	14	6	11	4	0
13	10	1	12	1	8	0	3	7	2	4	6	11	5	14	13	9
14	7	5	4	13	2	11	6	10	8	12	3	0	15	9	1	14
15	8	6	13	4	10	14	5	2	7	1	15	9	3	0	12	11

S-box 테이블은 다음과 같은 절차에 따라 설계기준에 적합한지 여부를 판단하여 결정한다.

단계 1. Bruijn diagram의 각 상태 Q_j(j=1...16)를 중복없이 랜덤하게 배치한다.

단계 2. S-box 테이블을 구성한다.

단계 3. SAC(Strict Avalanche Criterion) 조건에 적절한가?

$0.375 \le p_{ij} \le 0.625$ 이면 단계 4로, 아니면 단계 1부터 반복.

단계 4. 출력 비트간 상관관계 조건에 적절한가?

$\rho_{ij}(k)\neq|0|, \rho_{ij}(k)\neq|1|$이면 단계 5로, 아니면 단계 1부터 반복

단계 5. <DC공격에 강하기 위한 조건> XOR분포 특성 판단

non-zero 엔트리의 점유율: 90% 이상, 엔트리의 최대분포는 96 이하

단계 6. <선형암호분석 공격에 강한 조건> S-box 입력 번지에 대응하는 입력 비트들의 XOR한 값과 출력 번지에 대응되는 출력 비트들의 XOR한 값의 수가 전체의 1/2인 128을 기준으로 그 차이가 16% 이내에 드는가?

상기 조건의 단계 6까지 만족하면 S-box를 채택하고 아니면 단계 1부터 다시 반복한다. 그러나 상기 조

건 중에서 단계 6의 바람직한 기준은 256의 1/2인 128에 근접 되어야 하지만 16%로 여유를 준 이유는 위의 기준을 만족하는 10개의 S-box를 선정하기 위해 수행한 횟수가 약 2000만번을 이상이었으며 이렇게 하더라도 선형암호분석 공격에 충분히 강할 수 있다는 판단 때문이다. 이상의 설계 절차에 따라 80-DES의 S_1-box 테이블로 선정된 예는 표 2와 같다. 다른 S-box들에 대해서는 참고문헌[10]을 참조하기 바란다.

4. 80-DES의 비도 분석

80-DES를 DC와 선형암호분석 등을 통하여 분석한 결과 DES 보다 비도면에서 월등히 높은 것으로 나타났다. 선형암호분석은 지면 관계상 공격 확률이 가장 높은 S_3-box를 중심으로 분석하였다. 다른 S-box들의 편차 및 분포등의 분석은 참고문헌[10]을 참조하기 바란다.

4.1 SAC(Strict Avalanche Criteria)

본 연구에서 제시한 설계방법 및 기준에 의해 구성된 80-DES의 S_1-box 테이블에 대한 p_{ij}는 표 3과 같다. 나머지 9개의 S-box에 대한 p_{ij}는 참고문헌[10]을 참조 바란다.

표 3. 80-DES S_1-box의 p_{ij}

입력(i)	출 력 (j)			
	1	2	3	4
C1	0.375	0.625	0.625	0.625
C2	0.500	0.500	0.500	0.500
C3	0.500	0.500	0.500	0.500
C4	0.500	0.500	0.500	0.500
C5	0.531	0.625	0.438	0.562
C6	0.406	0.484	0.609	0.484
C7	0.531	0.484	0.578	0.547
C8	0.562	0.562	0.562	0.469
평균	0.521			

표 4. DES와 p_{ij} 비교

Box	DES	80-DES
S1	0.620	0.521
S2	0.633	0.518
S3	0.661	0.530
S4	0.615	0.531
S5	0.633	0.526
S6	0.651	0.530
S7	0.656	0.521
S8	0.656	0.531
S9	-	0.526
S10	-	0.511
평균	0.641	0.525

각 p_{ij}는 $0.375 \le p_{ij} \le 0.625$ 범위내에 있고, 80-DES의 S-box 테이블이 평균 0.525로 기존 DES의 0.641 보다 더욱 SAC 조건에 근접함을 표 4에서 볼 수 있다.

4..2 출력 비트간 상관관계

본 논문에서 설계된 80-DES의 S_1-box에 대한 $\rho_{ij}(k)$는 표 5와 같다.

표 5. 80-DES S_1-box의 $\rho_{ij}(k)$

출력 (ρ_{ij})	입 력 (k)							
	1	2	3	4	5	6	7	8
ρ_{12}	0.000	0.000	0.000	-0.577	-0.179	-0.167	-0.150	-0.059
ρ_{13}	-0.333	-0.333	0.000	-0.500	0.040	-0.200	-0.122	-0.188
ρ_{14}	0.000	0.333	0.000	-0.500	-0.101	-0.252	-0.121	-0.184
ρ_{23}	0.516	0.577	0.500	0.577	0.260	-0.243	-0.306	0.000
ρ_{24}	-0.000	0.000	-1.000	0.000	-0.116	-0.142	-0.003	-0.129
ρ_{34}	-0.000	-0.333	-0.500	0.000	-0.024	-0.049	0.003	-0.125
평균	-0.100							

표 6은 각 S-box별 상관계수에 대한 평균값을 DES와 비교한 것이다.

구성된 S-box의 출력 비트간 평균 상관계수 ρ는 $-0.100 \le \rho \le -0.062$ 로써 출력 비트간 상관관계가 DES보다 더욱 상호 독립적임을 알 수 있다.

그러나 표 6의 각 S-box 출력 비트간 평균 상관계수 ρ는 표 5의 각 $\rho_{ij}(k)$인 양수와 음수값의 산술 평균으로 상관 관계의 의미가 왜곡됨을 볼 수 있다.

이러한 모순을 배재하여 각 $\rho_{ij}(k)$의 절대값의 평균을 구해보면 표 7과 같다. 그 결과 출력 비트간 상관관계도 DES와 비교하여 볼 때 80-DES가 상호 독립적임을 알 수 있다.

표 6. DES와 ρ 비교

Box	DES	80-DES
S_1	-0.195	-0.100
S_2	-0.188	-0.065
S_3	-0.165	-0.077
S_4	-0.232	-0.079
S_5	-0.184	-0.069
S_6	-0.183	-0.077
S_7	-0.153	-0.100
S_8	-0.176	-0.079
S_9	-	-0.069
S_{10}	-	-0.062
평균	-0.163	-0.078

표 7. DES와 ρ의 절대값 비교

DES	80-DES
0.197	0.202
0.204	0.245
0.197	0.186
0.291	0.198
0.186	0.194
0.216	0.186
0.190	0.202
0.199	0.198
-	0.194
-	0.184
0.210	0.199

4.3 Differential Cryptanalysis(DC) 분석

4.3.1 XOR분포 특성

80-DES의 S-box는 8비트 입력에 4비트 출력을 갖으며, XOR분포 테이블은 표 8과 같다.

표 8. 80-DES S_1-box의 XOR분포 테이블

입력 \ 출력	0x	1x	2x	3x	4x	5x	6x	7x	8x	9x	ax	bx	cx	dx	ex	fx
0x	256	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1x	0	0	16	0	16	16	32	16	32	0	16	32	16	16	32	16
2x	0	32	0	32	64	0	0	0	0	0	64	0	0	32	0	32
3x	0	32	32	0	16	16	0	32	0	0	16	16	16	16	16	48
⋮								⋮								
10x	0	20	20	28	12	12	8	12	8	4	36	28	16	24	20	8
⋮								⋮								
20x	0	12	20	20	24	26	30	0	22	6	12	8	28	14	16	18
⋮								⋮								
30x	0	16	16	8	20	22	22	12	22	18	16	12	20	14	20	18
⋮								⋮								
fcx	16	16	20	12	8	16	16	12	20	20	12	4	28	20	12	24
fdx	0	28	10	16	20	8	24	18	16	16	20	14	16	16	14	20
fex	16	8	16	28	16	16	16	8	20	20	4	8	28	20	16	16
ffx	32	4	22	16	12	24	8	14	16	16	12	18	16	16	18	12

S-box의 XOR분포 테이블은 256개의 가능한 입력XOR(00x~ffx)와 16개의 출력XOR를 갖게 되어 각 XOR분포 엔트리의 평균은 16이며 한 행의 분포 합은 256이 된다. XOR분포 테이블에서 입력XOR값이 $0X_x$ 또는 $X0_x$(여기서 $X\epsilon\{1,2,...,f\}$)일 때, 출력XOR는 0_x인 경우가 발생되지 않는다. 이것은S-box 테이블이 열과 행값에 대한 Bijection 성질을 갖기 때문이다. 즉 두 입력에 의해 결정되는 S-box 테이블 행 또는 열값중 하나만 같고 다른 하나는 틀릴 때 결정되는 출력값은 다를 수 밖에 없기 때문이다.

이러한 특성은 non-zero 입력XOR로 zero인 출력XOR를 만들어내는 2-라운드 반복특성에서 각 S-box는 $0X_x$ 또는 $X0_x$(여기서 $X\epsilon\{1,2,...,f\}$)를 갖지 못한다. 그러므로 모든 S-box는 인접 S-box에 영향을 주게 되고 2-라운드 반복특성이 구성될 확률은 모든 S-box에 대한 확률로 결정되기 때문에 확률이 현저히 떨어진다.

4.3.2 N-라운드 특성

DES의 암호함수에서 확장재배열(E)은 입력의 한 비트가 절반은 다른 하나의 S-box에만 영향을 주고 나머지 절반은 두개의 S-box에 영향을 주는 반면에 80-DES 암호함수의 확장재배열은 입력의 한 비트가 반드시 두 개의 S-box에 영향을 주게 되므로 N-라운드 특성이 구성될 확률을 줄일 수 있다.

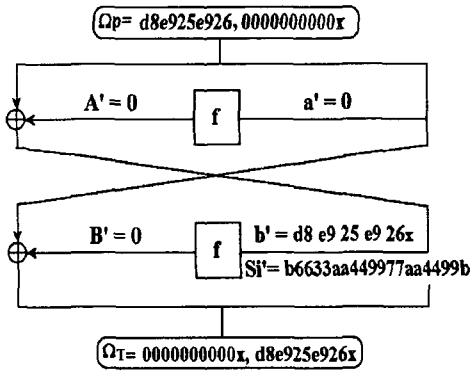

그림 2. 80-DES의 2-라운드 특성

먼저 그림 2에서와 같이 2-라운드 특성을 예로 들어보면 DES에서는 세 개의 S-box 입력XOR를 non-zero로 하여 1/234 확률을 갖는 2-라운드 특성을 얻을 수 있었으나, 80-DES에서는 S-box의 입력XOR가 $0X_x$ 또는 $X0_x$(여기서 $X\epsilon\{1,2,...,f\}$)일 때는 결코 출력XOR가 0인 경우가 발생되지 않으므로 2-라운드 특성은 그림 3과 같이 모든 S-box의 입력XOR가 0이 아닐 수밖에 없다. 그러므로 80-DES에서 2-라운드 특성이 구성될 확률은 다음과 같이 모든 10개 S-box의 확률에 영향을 받게 된다.

S_1:$b6_x \rightarrow 0$ 확률 64/256, S_2:$63_x \rightarrow 0$ 확률 64/256 S_3:$3a_x \rightarrow 0$ 확률 48/256, S_4:$a4_x \rightarrow 0$ 확률 64/256

S_5:$49_x \rightarrow 0$ 확률 48/256, S_6:$97_x \rightarrow 0$ 확률 64/256 S_7:$7a_x \rightarrow 0$ 확률 32/256, S_8:$a4_x \rightarrow 0$ 확률 64/256

S_9:$49_x \rightarrow 0$ 확률 48/256, S_{10}:$9b_x \rightarrow 0$ 확률 64/256

따라서 80-DES에서 2-라운드 특성이 구성될 확률은 6464:4864:4864:3264:4864/$256^{10} \approx 2^{-22}$로 계산된다. 만약 이러한 2-라운드 특성을 7번 반복 사용하여 16라운드 80-DES를 공격할 경우 특성이 성립될 확률은 $(2^{-22})^7 \approx 2^{-154}$ 로써 매우 높은 복잡도를 갖게 된다.

다음에는 6-라운드 공격에 사용되는 3-라운드 특성을 구성할 경우에 DES에서는 1/16의 확률값으로 30비트의 키를 찾을 수 있으나 80-DES에서는 입력 한 비트가 두 S-box에 영향을 주어 3-라운드 특성이 구

성될 확률은 $(48\cdot36/256^2)\cdot(48\cdot36/252^2)\approx1/1,438$ 이고, 처음 3-라운드 특성으로 찾을 수 있는 최종 라운드의 키는 80비트중 32비트에 불과하다. 따라서 축소된 6-라운드를 공격하기 위해 필요한 암호문쌍은 2^{15}개이고 복잡도는 2^{16}이 되며, 16-라운드 공격시 전수검사 공격방법 보다 효과가 없음을 알 수 있다.

80-DES의 5-라운드 특성 구성확률 또한 2^{-37}으로 DES의 1/10,486에 비해 현저히 떨어짐을 알 수 있다.

이상과 같은 방법으로 80-DES를 공격 분석한 결과는 표 9와 같이 종합된다. 여기에서 10-라운드 이상의 80-DES에 대한 DC 공격은 전수검사 공격방법보다 효과가 없음을 알 수 있다.

표 9. 80-DES의 공격 분석결과

80-DES 라운드	복잡도	필요한 암호문쌍	사용된 N-라운드 특성		
			라운드	확률	찾는키 (bit)
4	2^6	2^5	1R	1	48
6	2^{16}	2^{15}	3R	2^{-10}	32
8	2^{39}	2^{38}	5R	2^{-37}	24
9	2^{68}	2^{67}	7R	2^{-66}	80
10	2^{90}	2^{89}	9R	2^{-88}	80

4.4 선형암호분석(Linear Cryptanalysis)에 대한 안전성 분석

4.4.1 80-DES의 S-box 선형 근사

80-DES 가 암호학적으로 강하려면 물론 DC에도 강해야 하지만 선형암호분석 공격에도 강해야 한다. 선형암호분석에 강하려면 S-box 입출력 비트간의 상관관계를 조사하여 256의 1/2인 128에 근사하도록 구성해야 한다.

표 10은 본 논문에서 설계된 S-box들 중에서 선형암호분석이 가장 용이하다고 판단되는 S_3-box에 대하여 식(1)로 분석한 결과를 나타낸 것으로 128을 기준으로 그 차이를 나타내었다.

$$NS_a(\alpha,\beta) = \#\{x \mid 0\le x\le 255,\ \bigoplus_{s=0}^{7}(x[s]\cdot\alpha[s]) = \bigoplus_{t=0}^{3}(S_a(x)[t]\cdot\beta[t])\} \qquad (1)$$

표 10에 나타난 바와 같이 80-DES 에서 입·출력 비트간에 128을 기준으로 얼마나 차이가 있느냐가 선형암호분석에 많은 영향을 미친다.

80-DES의 S-box중에서 가장 편차가 큰 S_3-box는 $NS_3(6e,3)= 168/256= 0.656$으로 DES의 $NS_5(16,15)= 12/64= 0.19$와 비교해 볼 때 훨씬 양호하다고 볼 수 있다.

4.4.2 80-DES의 기지 평문 공격

80-DES의 선형암호분석 공격을 하기 위한 단계는 다음과 같다.

첫째, 각 S-box의 입력 비트 위치와 출력 비트의 XOR 값이 일치되는 경우의 수를 계산한다.

(표 10과 같은 표 작성)

둘째, 계산된 입·출력 비트간에 상관 관계가 많이 있다고 생각되는 모든 S-box 중에서 편차가 가장 큰 것 즉, 128을 기준으로 특별히 치우쳐 분산되어 있는 값을 이용하여 암호함수의 최량표현을 구한다.

셋째, 암호함수의 최량표현을 알고리듬 전체로 확장한 선형근사식을 구하여 키 비트를 찾는다.

80-DES 에서 각 S-box 입·출력 비트를 계산한 결과 편차가 가장 큰 것은 128을 기준으로 S_3-box에서 $NS_3(6e,3)=168$이 확률 $168/256=0.656$으로 모든 출력 비트의 XOR와 같아진다는 의미이다. 따라서 암호함

수 내부의 확장재배열(E)과 재배열(P)을 고려한다면 키 K를 고정하여 암호함수 f에 랜덤한 입력 X에 대하여 다음식이 확률 0.656 및 1-0.656=0.344로 성립된다.

표 10. S_3-box 입력위치와 출력 XOR 값 일치 경우의 수 (128 기준)

입력	출력														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	-16	0	-8	-8	8	-8	-16	0	0	0	-8	8	8	8
6	8	-8	0	0	-8	-8	-16	8	-16	0	8	8	0	0	-8
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	32	0	16	16	-16	16	32	0	0	0	16	-16	-16	-16
a	-8	8	0	0	8	8	16	-8	16	0	-8	-8	0	0	8
b	-8	-8	0	8	-16	0	-8	8	16	0	-8	0	-8	-8	0
⋮								⋮							
68	8	0	8	8	0	8	0	-8	0	8	-16	16	8	0	-8
69	-8	0	8	-16	-8	-16	8	-8	0	8	0	8	0	-8	0
6a	16	8	8	0	-16	8	8	0	0	-8	8	0	0	-8	8
6b	0	8	-24	-8	-8	0	0	0	0	-8	-8	8	8	0	0
6c	-8	0	16	-20	-12	-20	12	-16	0	16	-8	20	4	-12	-4
6d	0	0	8	-4	-4	-4	4	-8	0	8	-8	12	4	-4	-4
6e	8	-8	40	12	4	4	4	0	0	8	16	-12	-12	-4	4
6f	8	0	16	4	-4	4	4	0	0	0	8	-4	-4	-4	4
70	0	0	8	-4	-4	-4	4	-8	0	8	-8	12	4	-4	-4
71	8	0	0	12	4	12	-4	0	0	0	-8	4	4	4	-4
⋮											⋮				
f5	16	0	0	8	-8	-24	8	0	0	0	-16	-8	-8	24	8
f6	0	16	0	-8	-8	8	-8	-16	0	0	0	-8	-24	8	-24
f7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
f8	8	8	0	0	-8	-8	0	8	0	16	-8	-8	0	16	8
f9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
fa	0	0	0	-8	-8	8	8	0	0	0	0	-8	-8	8	-24
fb	0	16	0	-8	-8	8	-8	-16	0	0	0	-8	-24	8	-24
fc	-8	0	0	-4	4	12	-4	0	0	0	8	4	4	-12	-4
fd	8	0	0	4	-4	-12	4	0	0	0	-8	-4	-4	12	4
fe	0	-8	0	4	4	-4	4	8	0	0	0	4	12	-4	12
ff	0	-8	0	-12	-12	12	20	8	0	0	0	-12	-4	12	-36

$X[28,22,31,39,29] \oplus f(X,K)[22,31] = K[57,58,59,61,62]$ (2)

$X[28,22,31,39,29] \oplus f(X,K)[22,31] = K[57,58,59,61,62] \oplus 1$ (3)

6e(01101110)는 S_3-box의 입력 1,2,3,5,6번지, 3(0011)은 S_3-box의 출력 0,1번지이다. S_3-box의 입력 1,2,3,5,6번지는 암호함수 f의 입력 X의 28,22,31,39,29번지에 대응되는 키 K의 번지는 57,58,59,61,62번지이다. 그리고 S_3-box의 출력 0,1번지는 암호함수 f의 출력 f(X,K)의 22,31번지에 대응된다.

트를 추정함으로써 기지평문 공격을 할 수가 있다. 그러나 DES는 0.19로 치우쳐 있으나 80-DES는 0.344로 양호한 분포를 갖고 있으므로 선형암호분석에 의한 공격은 훨씬 어렵게 된다.

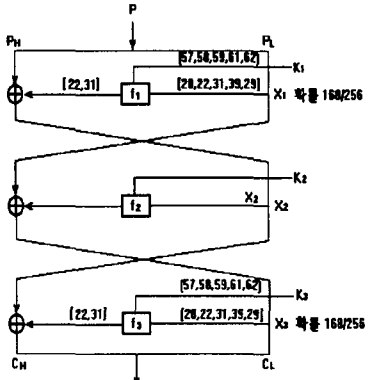

그림 3. 3-라운드 80-DES

암호함수 f의 선형근사식을 알고리듬 전체로 확장하는 방법에 대하여 그림 3의 3-라운드 80-DES를 예를 들어 설명하면 다음과 같다.

1-라운드 암호함수 f에 식 (2)를 적용하면 확률 168/256으로 식 (4)가 성립한다.

$X_1[6,21,28,35] \oplus P_H[9,10,11,12] \oplus P_L[3] = K_1[5,9]$

$X_1[3] \oplus K_1[5,9] = f_1(X_1,K_1)[6,21,28,35]$ (4)

3-라운드 암호함수 f에 식 (2)를 적용하면 확률 168/256으로 식 (5)가 성립한다.

$X_2[6,21,28,35] \oplus C_H[9,10,11,12] \oplus C_L[3] = K_3[5,9]$

$X_3[3] \oplus K_3[5,9] = f_3(X_3,K_3)[6,21,28,35]$ (5)

한편,

$f_1(X_1,K_1)[6,21,28,35] = P_H[6,21,28,35] \oplus X_2[6,21,28,35]$

$f_3(X_3,K_3)[6,21,28,35] = C_H[6,21,28,35] \oplus X_2[6,21,28,35]$

이다. 위의 식을 식 (4)와 (5)에 대입하여 X_2항을 소거하면

$P_H[6,21,28,35] \oplus C_H[6,21,28,35] \oplus P_L[3] \oplus C_L[3] = K_1[5,9] \oplus K_3[5,9]$ (6)

을 얻을 수 있다.

식 (6)이 성립되는 확률은 랜덤하게 주어진 평문에 대응되는 암호문에 대하여 식(10)과 (11)이 동시에 성립할 확률과 동시에 성립하지 않을 확률의 합이므로 $(168/256)^2 + (1-168/256)^2 \approx 0.55$가 되고 식 (6)은 3-라운드 80-DES의 최량 표현이 된다.

이와 같이 3-라운드 DES의 성립할 확률은 0.7에 비해 3-라운드 80-DES의 성립할 확률은 0.55로 DES에 비하여 80-DES의 선형암호분석 공격은 훨씬 어려워짐을 알 수 있다.

[보조정리 1]

독립적인 확률 변수 $X_i(1 \le i \le n)$이 확률 P_i로 0, 확률 $1-P_i$로 1을 취할 때, $X_1 \oplus X_2 \oplus \cdots \oplus X_n = 0$이 되는 확률은 다음 식 (7)과 같이 얻어진다[11].

$$2^{n-1} \prod_{i=1}^{n} (P_i - 1/2) + 1/2 \qquad (7)$$

식 (7)을 이용하면 16-라운드 DES에서 최량확률은 $1/2 - 1.49 \times 2^{-24}$ 이나 80-DES에서 가장 공격에 유

$1/2 \approx 1/2 + 1.11 \times 2^{-28}$의 최량확률을 갖는다. 따라서 DES 보다 현저히 최량확률이 낮아지며 더우기 이러한 방법으로 26비트를 찾는다 하더라도 나머지 54비트를 전수검사 공격으로 찾는다는 것은 무의미할 것으로 판단된다.

5. 결 론

본 논문에서는 DES가 더이상 사용할 수 없도록 다양한 암호분석 공격이 출현함에 따라 보다 안전성 있는 블록 암호알고리듬 개발을 위해서 DES의 기본 구조를 그대로 유지하면서 S-box를 재설계하고 키 길이를 80비트로 확장한 80-DES를 제안하였다.

80-DES의 설계는 DES의 효율성을 유지하면서 DC 및 선형암호분석 공격에 대한 대응방안에 역점을 두었으며, 아울러 DES에서 논란이 되어온 키 길이 및 S-box 설계시 일반적인 고려사항에 대한 문제도 함께 고려하였다. 그 결과 80-DES는 비밀키 80비트를 사용하므로 전수검사 공격에 대한 복잡도를 높일 수 있었고 DC 공격방법에 대해 10라운드 이상부터는 전수검사 공격방법보다 비도가 높은 결과를 가져왔으며, 선형암호분석에 대한 공격에도 DES 보다 강한 것으로 판단되었다.

한편 소프트웨어적인 수행속도 면에서도 DES와 비교 시험한 결과 지장이 없었다.

따라서 80-DES는 DC 및 선형암호분석 공격에 대한 비도를 높일 수 있었고 DES와 같은 수준에서 안전성을 평가한 결과 DES 이상의 높은 비도가 보장되며 실용적인 가치가 있어 관련된 응용 분야에서 효과적으로 활용될 수 있을 것으로 판단된다.

참 고 문 헌

1) W.Diffie and M.E.Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," IEEE, Vol.10, No.6, pp.74-84, 1977.
2) E.Biham and A.Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of CRYPTOLOGY, Vol.4, No.1, 1991.
3) E.Biham and A.Shamir, "Differential Cryptanalysis of the full 16-round DES," proc. of CRYPTO'92, 1992.
4) M.Matsui "Linear Cryptanalysis Method for DES Cipher", Eurocrypt'93 Extended Abstracts, pp.112-123, 1993.
5) H.Feistel,"Cryptography and Computer Privacy, " Science American, Vol.228, No.5, pp.15-23, 1973.
6) J.B.Kam and G.I.Davida, "Structured Design of Substitution Permutation Encryption Network," IEEE Tran. on Computer, Vol.C-28, No.10, Oct., pp.747-753, 1979.
7) A.F.Webster and S.E.Tavares, "On the Design of S-boxes," Proc. of CRYPTO'85, Springer-Verlag, 1985.
8) K.J.Kim, A Study on the Construction and Analysis of Substitution Boxes for Symmetric Cryptosystems, Ph.D. Dissertation, Yokohama University, JAPAN, 1990.
9) 남길현, DES 암호알고리즘의 안전성분석과 확장된 DES-like 암호알고리즘의 설계에 관한 연구, 한국통신정보보호학회논문지, Vol. 3. NO. 2. DEC. 1993
10) 윤용정, 80비트 블록 암호(80-DES)의 설계 및 비도분석에 관한 연구, 국방대학원 석사학위논문, 1994.
11) 김광조, DES의 선형 해독법에 관한 해설(I), 한국통신정보보호학회지, 제3권 제3호 1993.