通信情報保護學會論文誌
第 7 卷 第 3 號, 1997. 9

Differential 공격에 강한 DES-like 암호 알고리즘

김 구 영*, 원 치 선*

A Robust DES-like cryptographic algorithm against Differential Cryptanalysis

Gu Young Kim, Chee Sun Won

요 약

DES가 Differential Cryptanalysis(이하 DC)에 쉽게 공격받을 수 있는 결정적인 취약점은 S-box를 포함한 암호함수의 구조에 있다. 따라서 DES의 DC에 대한 대응방안으로는 XOR분포가 완전하게 균일(입력 XOR가 zero일 경우는 제외)하도록 S-box를 재구성하는 방법과 N-1 라운드 특성이 구성될 확률을 낮추기 위해 DES 알고리즘의 일부를 수정하는 방법을 생각할 수 있다. 그러나 Dawson과 Tavares가 제안한 완전히 균일한 XOR분포 테이블을 갖는 S-box는 오히려 균일하지 않을 때보다 더 취약하다고 Pieprzyk의 연구결과에 의해 증명되었다. 결국 DES가 DC에 대응하기 위해서는 S-box의 재설계만으로는 부족하며 암호함수 자체를 수정해야 할 것이다. 본 논문에서는 DES의 암호함수를 일부 수정하여 DC에 대한 반복 특성이 구성될 확률을 낮추는 방안을 제안하고자 한다. 비교 분석 결과 제안된 알고리즘이 기존의 DES보다 DC 공격에 강함을 확인하였다.

Abstract

Due to the cryptographic functional structure including the S-box, DES is not robust against differential cryptoanalysis (DC). Therefore, to increase the security against DC, we have to redesign the S-box or modify DES algorithm to decrease the probability for the N-1 round characteristics. However, it has been shown that a new design for the S-box is not secure enough. Rather, if will be more reliable to devise a modified cryptographic algorithm. In this paper, we propose a modified DES algorithm to decrease the probability of N-1 round characteristics to be robust against DC. According to our comparative study, the proposed algorithm is shown to be more robust against the DC than DES.

---

* 동국대학교 전자공학과

1. 서 론

1990년 Biham과 Shamir가 발표한 Differential Cryptanalysis(이하 DC)는 DES 뿐만 아니라 대부분의 반복 블록 암호시스템을 쉽게 공격할 수 있는 새로운 공격방법으로 특정한 평문쌍들의 차이와 이에 대응되는 암호문쌍들의 차이 관계를 통계적으로 분석하여 적용된 키를 찾는 선택 평문 공격방법이다. Biham과 Shamir의 연구 결과에 의하면 DES가 DC에 쉽게 공격될 수 있는 결정적인 취약점은 S-box를 포함한 암호함수의 구조에 있다. 즉, 6라운드로 축소된 DES에서는 0.3초 이내에, 8라운드에서는 2분 이내에 공격되었으며, 표준 라운드인 16라운드에서도 전수 검사(exhaustive search) 보다 훨씬 빠르게 공격할 수 있다고 하였다[1][2]. 따라서 DES의 DC에 대한 대응방안으로는 XOR분포가 완전하게 균일(입력 XOR가 zero일 경우는 제외)하도록 S-box를 재구성하는 방법[2]과 N-1 라운드 특성이 구성될 확률을 낮추기 위해 DES 알고리즘의 일부를 수정하는 방법을 생각할 수 있다. 그러나 Dawson과 Tavares[3]가 제안한 완전히 균일한 XOR 분포 테이블을 갖는 S-box는 오히려 균일하지 않을 때보다 더 취약하다고 Pieprzyk의 연구결과에 의해 증명되었다[4]. 결국 DES가 DC에 대응하기 위해서는 S-box만의 재설계만으로는 부족하며 암호함수 자체를 수정해야 할 것이다.

본 논문에서는 DES의 암호함수를 일부 수정하여 DC에 대한 반복 특성이 구성될 확률을 낮추는 방안을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 2장과 3장에서는 DES의 암호함수와 제안된 암호함수에 대해 알아보고 4장에서는 Differential Cryptanalysis란 무엇인지 알아보며, 5장에서는 기존의 암호함수와 제안된 암호함수의 N 라운드 특성에 대해 조사해보고 6장에서 결론을 맺는다.

2. DES의 암호함수

DES 알고리즘은 56비트의 키를 갖는 블록 암호화 알고리즘으로 암호화와 복호화에 같은 알고리즘을 사용한다. DES의 구조는 IP(초기 전치), IP^{-1}(역 초기 전치) 그리고 매 라운드마다 반복되는 암호함수로 나눌 수 있으며 이 암호함수는 E(expantion)-S(substitution)-P(permutation)를 차례로 거치며, 키스케줄에서 생성된 서브키는 E-box를 거친 48비트와 XOR된다. DES의 S-box는 8개로 구성되어 있으며 각 S-box의 입력은 6비트로 최상위 비트와 최하위 비트는 S-box의 행이 되고 나머지 4비트는 S-box의 열 값인 4비트의 출력을 갖는 비선형 함수로 S-box의 설계 원칙은 다음과 같다. 첫째, S-box는 비선형이어야 하고, 입력에 밀접한 관계가 있지 않아야 한다. 둘째, S-box의 6개의 입력 비트중 하나의 비트값을 바꾸면 적어도 2개 이상의 출력 비트가 바뀐다. 셋째, S(x)와 S(x⊕001100)은 2비트 이상 다르다. 넷째, 임의의 e, f 에 대해 $S(x) \neq S(x \oplus 11ef00)$이다. 다섯째, 한 개의 입력 비트값을 고정하였을때 S-box의 출력 비트들의 0과 1의 수의 차이를 최소화한다. 이러한 S-box의 설계원칙으로부터 S-box의 XOR 확률 분포 $(X \oplus X^* = X')$인 S-box의 64개의 입력 벡터 (X, X^*)에 대해 $Y = S(X) \oplus S(X^*)$의 확률 분포를 S-box의 XOR 확률 분포라 하며, 64개 의 (X, X^*)에 대해 $Y = S(X) \oplus S(X^*)$일 때 $S(X^*) = Y$(확률 P)로 쓴다)의 특성을 얻을 수 있으며, 이것은 differential 암호분석에서 아주 중요한 역할을 한다. X와 X*를 S-box의 입력쌍이라 하고 X'를 입력 XOR이라 할 때 X, X*, X'을 다음과 같이 나타낼 수 있으며

X=x(6)x(5)x(4)x(3)x(2)x(1)
X*=x*(6)x*(5)x*(4)x*(3)x*(2)x*(1)
X'=X⊕X*=x'(6)x'(5)x'(4)x'(3)x'(2)x'(1)

X'에 대해 다음의 확률 특성을 갖는다.

(i) x'(6)=x'(1)=0이고 (x'(5)x'(4)x'(3)x'(2))=0일때 S(x'(6)x'(5)x'(4)x'(3)x'(2)x'(1))=0일 확률은1이고, x'(6)=x'(1)=0이고 (x'(5)x'(4)x'(3)x'(2))≠0일때 S(x'(6)x'(5)x'(4)x'(3)x'(2)x'(1))=0일 확률은 0이다.

(ii) x'(6)x'(5)x'(4)x'(3)x'(2)x'(1)중 1비트값이 하나, 나머지 5개의 비트값이 0 일때 S(x'(6)x'(5)x'(4)x'(3)x'(2)x'(1))≠0x, 1x, 2x, 4x, 8x이다.

(iii) S(0'0'1'1'0'0')≠0x, 1x, 2x, 4x, 8x 이다.

(iv) 임의의 e, f에 대해 S(1'1'e'f'0'0')≠0x이다.

그리고 암호함수의 XOR분포의 확률은 대응되는 각 S-box의 XOR분포의 확률의 곱이다.

확장치환(E)는 암호함수의 입력 32비트중 절반인 16비트는 재배열만 되고 나머지 절반은 두배로 확장 재배열된다. 치환 P는 8개의 S-box에서 출력된 32 비트의 위치를 바꾸는 역할로, 평문 데이터와 암호키를 가능한 한 빨리 암호문에 영향을 미치게 하는 diffusion을 수행하여 블록내의 4개의 원소를 그들이 속해있는 블록과는 다른 블록으로 이동시키고, 모든 원소의 이동거리가 5이상이 된다. 이러한 치환 P와 S-box의 출력과의 관계는 다음과 같다.

첫째, 앞 라운드의 S-box 출력은 다음 라운드에서 동일한 S-box에 입력되지 않으며 모두 다른 S-box의 출력들이 입력된다. 둘째, 앞 라운드의 S-box중 S(i-1)의 출력은 다음 라운드 S-box의 입력 6비트를 b1, b2, b3, b4, b5, b6로 나타낼 때 b5, b6중 어느 한 비트에 입력되고, 앞 라운드의 S(i-2)의 출력이 다음 라운드 S-box의 b1, b2중 어느 한 비트에 입력된다. 셋째, 앞 라운드의 S-box중 S(i+1)의 출력은 다음 라운드 S-box의 b3, b4중 어느 한 비트에 입력된다. 넷째, 각 S-box의 출력 4비트중 2비트는 다음 라운드의 b1, b2나 b5, b6의 입력으로 또 다른 2비트는 b3, b4에 입력된다.

3. 제안된 암호함수

그림 1의 제안한 암호함수는 DES 암호함수에서 확장치환(E)은 그대로 사용하고, 대입(S)은 전 라운드의 암호함수의 출력값들과 현 라운드에서의 S-box들의 출력값들이 XOR하는 구조로 바꾸고, 치환(P)은 암호함수의 출력을 우측으로 한 블록(4 비트)씩 쉬프트 시키는 network permutation으로 바꾸어 암호함수가 generalized feister network[5]으로 DES의 암호함수보다 DC의 확률을 줄일 수 있는 구조로 되어 있다.

그림 1에서 X_1', X_2', X_3', . . . , X_8'는 i번째 라운드에서의 암호함수의 입력 블록으로 각각 6비트인 전체 48비트이고, Y_1, Y_2, ... , Y_8은 i번째 라운드에서의 암호함수의 출력 4비트 블록으로 전체 32비트를 나타내며, 입력 블록과 출력 블록의 관계는 다음과 같다. $Y_i=x_i \oplus S_{i+7}(X_{i+7}')$(i=1, 2, . . .8)($x_1$, x_2, ···, x_8는 각각의 X_1', X_2', X_3', ··· , X_8'의 하위 4비트), 그리고 network permutation로 $Yi=>Y_{i+1}'$(i=1, 2, ···, 8)로 된다.

S-box와 network permutation의 관계는 다음과 같다. 첫째, 앞 라운드의 S-box 출력은 다음 라운드에서 동일한 S-box에 입력되지 않으며 모두 다른 S-box의 출력들이 입력된다. 둘째, 앞 라운드의 S-box중 S(i-1)의 출력은 다음 라운드 S-box의 S(i+1)에 입력된다. 셋째, S(i)의 출력과 xi+1의 XOR 4비트중 첫 번째 비트는 S-box의 입력 6비트를 b1, b2, b3, b4, b5, b6로 나타낼 때 다음 라운드 S(i+1)의 b6이 되고, 네 번째 비트는 S(i+3)의 b1이 된다.

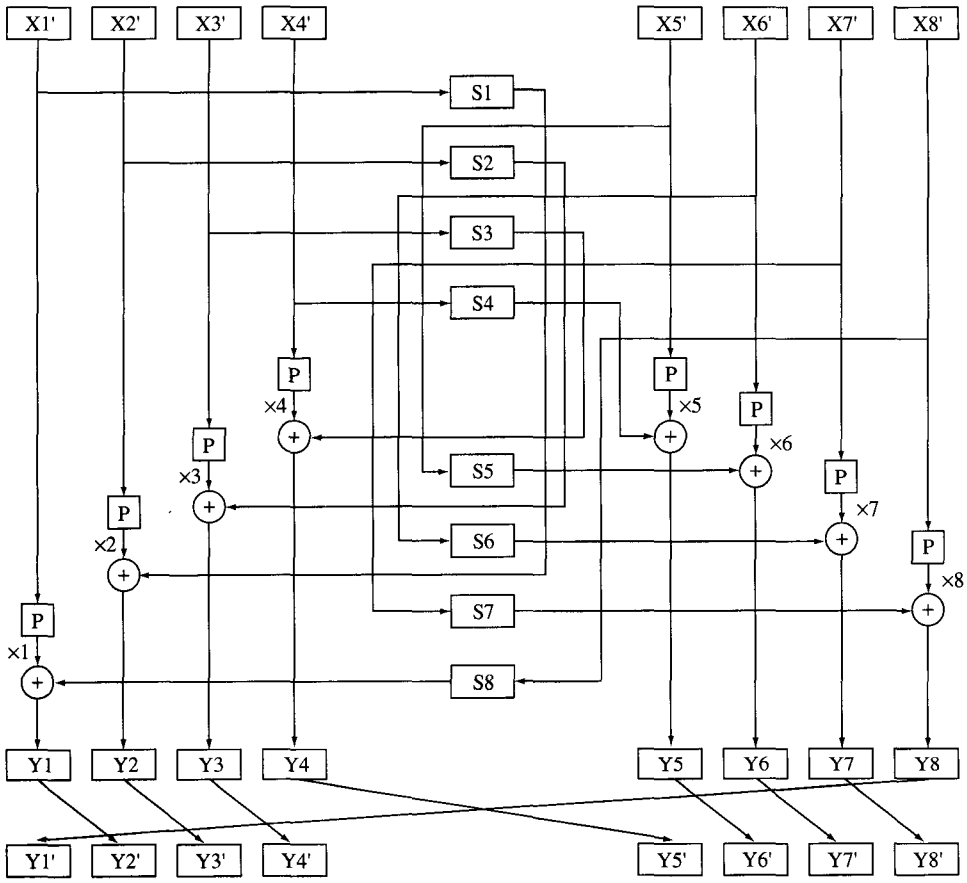


그림 1. 제안한 암호함수

4. Differential Cryptanalysis분석

암호화 알고리즘이 알려진 경우의 한가지 공격 방법은 가능한 모든 키를 시도하는 brute-force 공격이다. 이 방법은 만일 키가 64 비트라면 2^{64}개의 키 조합을 모두 사용하여 해독하는데 많은 시간이 필요하다. 따라서 해독자는 암호문이나 평문으로부터 직접 키를 유추해 내는 기법을 쓰는데 보통 ciphertext-only 공격이나 known-plaintext 공격을 사용한다. 1990년 Biham과 Shamir가 발표한 differential cryptanalysis는 특정한 평문쌍들의 차이와 이에 대응되는 암호문쌍들의 차이 관계를 통계적으로 분석하여 적용된 키를 찾는 선택 평문 공격방법으로 컴퓨터의 파워와 메모리 용량의 면에서 실제적인 공격 방법으로 제시되고 있다.

DES 알고리즘의 암호함수에 한 쌍의 평문을 모듈로2 연산한 값(입력 XOR)에 대해서는 단지 암호함수내의 8개의 S-box들만이 비선형성을 가지게 된다. 즉, 한 쌍의 평문을 각각 X,

X* 그리고 이를 암호화한 한 쌍의 암호문을 Y, Y*라고 하면 암호함수내에서 E-box, 암호키, P-box는 다음과 같은 식을 만족한다.

$$E(X)\oplus E(X^*)=E(X\oplus X^*) \quad (1)$$

$$(X\ K)(X^*\oplus K)=(X\oplus X^*) \quad (2)$$

$$P(X)\oplus P(X^*)=P(X\oplus X^*) \quad (3)$$

그러므로 입력 XOR은 E-S-P network의 구조를 갖는 암호함수내에서 S-box를 제외한 나머지에서는 선형성을 갖는다. 따라서 사용되는 암호키와 무관하게 입력 XOR에 대한 출력 XOR와의 관계를 다음과 같이 구할 수 있다.

$$\begin{aligned} S_i &= S_i \oplus S_i^* \\ &= (S_e \oplus S_k) \oplus (S_e^* \oplus S_k) \\ &= S_e \oplus S_e^* = S_e' \end{aligned} \quad (4)$$

표 1은 8개의 S-box중의 하나인 S_1-box의 한 쌍의 6비트 입력에 대한 한 쌍의 4비트 출력을 구하고 입출력 모두 각각 XOR하여 그 개수를 카운트한 것으로 여기에서 보듯이 입력 XOR에 대한 출력 XOR의 관계는 비균일함을 알 수 있다. 이와 같은 성질을 이용하여 한 쌍의 S-box의 입력값을 알고 그의 출력 XOR를 알 때 암호키를 찾아내는 방법은 다음과 같다.

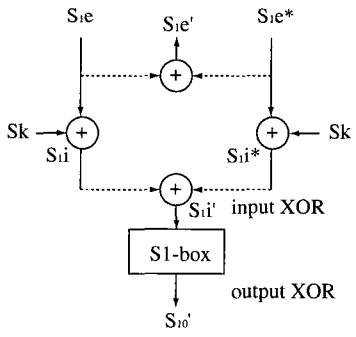


그림 2. S1-box의 입력 XOR과 출력 XOR

그림 2에서와 같이 입력쌍이 각각 $S_{1e}=1_x$, $S_{1e}^*=35_x$라고 하고 출력 XOR을 $S_{1o}'=D_x$라고 한다면 입력 XOR은 $S_{1e}'=S_{1i}'=34_x$이다. 표 1에 따르면 34_x->D_x는 모두 8개의 입력값이 가능성을 가지며 이를 토대로 가능성 있는 암호키들을 구하면 표 2와 같다. 그리고 또 다른 한 쌍의 평문에 대하여 같은 과정을 거친다면 가능한 암호키에 대한 정보를 또 얻을 수 있다. 만약 입력쌍이 각각 $S_{1e}=21_x$, $S_{1e}^*=15_x$라고 하고 출력 XOR를 $S_{1o}'=3_x$라고 한다면 입력 XOR은 역시 $S_{1e}'=S_{1i}'=34_x$이며 이에 대한 가능한 암호키들을 표 3과 같이 구할 수 있다. 이 두 표에서 공통적으로 나타나는 17_x와 23_x로 암호키의 가능성은 더욱 압축된다. 그리고 다른 형태의 여러 개의 입출력 XOR($S_{1e}'=34_x$)에 대해서도 같은 과정을 거친 후 가장 빈번히 중복되어 나타나는 암호키가 실제 암호키일 가능성이 가장 크다.

표 2 $S_{1e}=1_x$, $S_{1e}^*=35_x$이고 $S_{1o}'=D_x$일 때 가능한 키값

S_1-box 입력쌍	가능한 키값
06, 32	07, 3
10, 24 .	11, 25
16, 22	17, 23
1C, 28	1D, 29

표 3. $S_{1e}=1_x$, $S_{1e}^*=35_x$이고 $S_{1o}'=3_x$일 때 가능한 키값

S_1-box 입력쌍	가능한 키값
01, 35	03, 37
02, 36	00, 34
15 21	17, 23

표 1 S_i-box의 입력 XOR과 출력 XOR의 관계

S1-box	출력 XOR															
입 력 XOR	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	2	4	4	0	10	12	4	10	12	2	4
2	0	0	0	0	0	4	4	4	0	6	8	6	12	8	4	2
3	14	4	2	10	8	6	4	2	6	4	4	0	2	2	2	0
4	0	0	0	0	0	10	10	6	0	4	6	4	8	2	6	2
5	4	8	6	2	2	4	4	2	0	4	4	0	4	12	4	6
6	0	4	2	8	0	2	6	2	8	4	4	2	6	4	0	12
7	2	4	10	0	6	4	8	4	2	4	8	2	0	2	4	4
8	0	0	0	0	0	8	8	4	0	6	2	8	4	8	2	4
9	10	2	4	2	6	4	6	0	2	2	8	0	6	10	2	12
a	0	8	6	2	10	8	6	0	6	4	6	0	4	4	2	10
b	2	4	0	2	0	2	4	0	2	6	2	6	0	6	2	12
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
32	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	2
33	4	4	6	2	2	8	4	2	4	0	2	2	4	6	2	4
34	0	8	16	6	0	0	0	12	6	0	0	0	0	8	0	6
35	2	2	4	0	4	0	0	0	14	4	6	8	0	2	14	0
36	2	6	1	2	8	0	2	2	4	2	6	8	6	4	10	0
37	2	2	12	4	2	4	4	10	4	4	2	6	9	2	2	4
38	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
39	6	2	2	4	10	6	4	8	4	0	2	4	2	4	4	0
3a	6	4	6	4	8	8	0	6	2	2	6	2	2	6	4	0
3b	2	6	4	0	2	2	4	6	4	6	8	6	4	4	6	2
3c	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
3d	0	8	5	2	0	6	0	8	4	4	0	4	0	12	4	4
3e	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
3f	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

5. N 라운드 DC 분석

라운드 수가 N인 DES를 DC 공격하기 위해서는 확률이 큰 N-1 라운드의 특성이 필요하다. 라운드 수가 큰 경우 확률이 큰 특성을 찾는 것은 어렵지만 2, 3, 4 라운드의 반복 가능한 특성을 여러 번 연결하여 큰 라운드의 특성을 얻을 수 있다[7].

5.1 2 라운드 반복 가능한 특성

DES의 2 라운드 특성이 존재할 조건으로 f(a')=0, f(b')=0이 되는 a', b'(a', b'는 암호함수의 입력 32비트)이 존재하는 것으로, 그림 3과 같이 DES의 2 라운드 특성을 구성할 수 있다. 반복 가능한 2 라운드 특성을 구성하기 위해 a'=0으로 하였을 때 2 라운드 특성이 구성될 확률은 non-zero 입력 XOR을 갖는 적어도 3개의 S-boxes(S1, S2, S3 box)에 영향을 받아 b' = 19 60 00 00x일 때 f(b')=0이 될 확률은 이미 잘 알려진 결과로 (14/64)*(8/64)*(10/64)으로 약 1/234이다.

제안된 암호함수의 2 라운드 반복 특성도 f(a')=0, f(b')=0이 되는 a', b'이 존재할 확률을 구하는 것으로, 제안된 암호함수의 2 라운드 반복 특성이 존재하기 위해서는 암호함수내의 모든 Si-box의 출력 $S_i(X_i')$과 x_{i+1}의 XOR이 모두 zero이어야 한다. 즉, $S_i(X_i')\oplus x_{i+1}=0$ (i=1, 2, . . . , 8)이 되어야 한다.

(1) 각 S_i-box의 XOR 확률분포 특성으로부터 $X_i'=0$ 일 때 $S_i(X_i') = 0$일 확률은 1이고, $X_i' \neq 0$ 일 때 $S_i(X_i')=x_{i+1}$(x_{i+1}은 임의의 4비트)일 확률은 16/64이하이다. 따라서, 모든 S_i-box에서 확률 1로 $S_i(X_i')=x_{i+1}$되는 X_i'와 x_{i+1}은 zero밖에 없고, 이 때 b'는 모두 zero이므로 이 경우에 f(b')=0 (b'≠0)은 성립하지 않는다.

(2) 하나의 S_i-box에만 non-zero의 입력값을 갖고 나머지 S-box들은 모두 zero인 입력값을 가질 때의 제안된 암호함수의 2 라운드 특성을 조사해 보자.

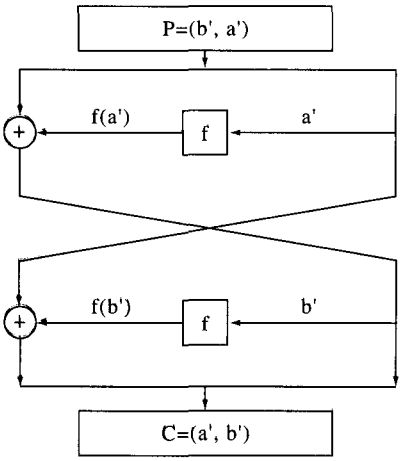


그림 3. 2-라운드 특성

제안된 암호함수의 2 라운드 특성이 존재하기 위해서는 S_i-box에서 $X_i' \neq 0$일 때 $S_i(X_i')=x_{i+1}$일 확률과 $x_i \oplus S_i(X_{i+7}')=0$이어야 한다. S_i-box만 제외한 모든 S-box들의 입력값이 zero이므로, 확장치환(E)의 특성에 의해 X_i'의 상위 2비트와 하위 2비트는 모두 zero로 $X_i' = 00??00$이 되고 X_i'의 하위 4비트인 x_i는 ??00이 된다. 또한 x_{i+1}은 X_{i+1}'의 하위 4비트로 모두 zero이므로 $S_i(X_i')=0(X_i' \neq 0)$일 확률은 S-box의 XOR 확률분포 특성 (ii)와 (iii)에 의해서 $S_i(X_i') \neq 0(X_i' \neq 0)$이다. 따라서 이 경우에도 f(b')=0 (b'≠0)은 성립하지 않는다.

(3) 연속적인 두 개의 S-box들에서만 non-zero의 입력값을 갖고, 나머지 S-box들은 모두 zero인 입력값을 가질 때의 제안된 암호함수의 2 라운드 특성이 존재하기 위해서는 S_i-box에서 $X_i' \neq 0$일때 $S_i(X_i')=x_{i+1}$일 확률 p와 S_{i+1}-box에서 $X_{i+1}' \neq 0$일때 $S_{i+1}(X_{i+1}')=x_{i+2}$일 확률 q가 존재해야 하며, $x_i=S_{i-1}(X_{i-1}')$, $x_{i+2}=S_{i+1}(X_{i+1}')$이어야 한다. 그러나 S_i-box와 S_{i+1}-box을 제외한 나머지 S-box들의 입력값이 모두 zero이므로 X_{i-1}'과 X_{i+2}'은 0이고, 확장치환(E)의 특성에 의해 X_i'의 상위 2비트와 X_{i+1}의 하위 2비트는 zero로 $X_i'=00????$, $X_{i+1}'=????00$이 된다. 또한 2 라운드 반복 특성이 존재하기 위해서는 $x_i \oplus S_{i-1}(X_{i-1}')=0$이어야 하고, 따라서 X_i'의 하위 4비트인 x_i은 zero이고 $X_i'=000000$, $X_i'=0????00$이 된다. 또한 X_{i+2}'의 하위 4비트인 x_{i+2}도 zero이므로 $S_{i+1}(X_{i+1}')=x_{i+2}(X_{i+1}' \neq 0)$는 $S_{i+1}(X_{i+1}')=0$ $(X_{i+1}' \neq 0)$일 확률로 바뀌고, $X_{i+1}'=0????00$으로 S-box의 XOR 확률분포 특성(i)에 의해 $S_{i+1}(X_{i+1}')=0$ (Xi+1'≠0)일 확률은 zero이다. 따라서 이 경우에도 f(b')=0 (b'≠0)은 성립하지 않는다.

(4) 연속적인 세 개의 S-box들, 즉 S_i-box와 S_{i+1}-box 그리고 S_{i+2}-box에서만 non-zero의 입력값을 갖고 나머지 S-box들은 모두 zero인 입력값을 가질 때의 제안된 암호함수의 2 라운드 특성이 존재하기 위해서는 S_i-box에서 $X_i' \neq 0$일 때 $S_i(X_i')= x_{i+1}$일 확률 p와, S_{i+1}-box에서 $X_{i+1}' \neq 0$일 때 $S_{i+1}(X_{i+1}')= x_{i+2}$일 확률 q와, S_{i+2}-box에서 $X_{i+2}' \neq 0$일 때 $S_{i+2}(X_{i+2}')=x_{i+3}$일 확률 r이 존재 해야 하며, $S_{i-1}(X_{i-1}')=x_i$, $S_{i+2}(X_{i+2}')=x_{i+3}$이어야 한다.

그러나 S_i-box와 S_{i+1}-box 그리고 S_{i+2}-box을 제외한 나머지 S-box들의 입력값이 모두 zero이므로 X_{i-1}', X_{i+3}'은 zero로 $X_i'=0????$, $X_{i+1}'=??????$, $X_{i+2}'=????00$가 된다. 그러나 제안된 암호함수의 2 라운드 특성이 존재하기 위해서는 X_i'의 하위 4비트인 x_i가 zero이어야 하므로 $X_i'=000000$이다. 따라서 $X_i' \neq 0$일 때 $S_i(X_i')=x_{i+1}$의 확률이 p라는 가정이 성립하지 않는다.

(5) (1), (2), (3), (4)로부터 제안된 암호함수의 2 라운드 반복 특성이 존재하기 위해서는 모든 S-box의 입력 XOR이 non-zero가 될 수밖에 없다.

S_i-box에서 $S_i(X_i')=x_{i+2}(X_i'\neq 0)$의 확률이 p_0이고, S_{i+7}-box에서 $S_{i+7}(X_{i+7}')=x_i(X_{i+7}'\neq 0)$의 확률이 p_7이고, S_{i+6}-box에서 $S_{i+6}(X_{i+6}')=x_{i+7}(X_{i+6}'\neq 0)$의 확률이 p_6이고, S_{i+5}-box에서 $S_{i+5}(X_{i+5}')=x_{i+6}(X_{i+5}'\neq 0)$의 확률이 p_5이고, S_{i+4}-box에서 $S_{i+4}(X_{i+4}')=x_{i+5}(X_{i+4}'\neq 0)$의 확률이 p_4이고, S_{i+3}-box에서 $S_{i+3}(X_{i+3}')=x_{i+4}(X_{i+3}'\neq 0)$의 확률이 p_3이고, S_{i+2}-box에서 $S_{i+2}(X_{i+2}')=x_{i+3}(X_{i+2}'\neq 0)$의 확률이 p_2이고, S_{i+1}-box에서 $S_{i+1}(X_{i+1}')=x_{i+2}(X_{i+1}'\neq 0)$의 확률이 p_1일 때이다.(p_i의 확률은 $0<p_i<1$로 16/64 이하이다). 따라서 2 라운드 반복 가능한 최대 확률은 $p_0*p_1*p_2*p_3*p_4*p_5*p_6*p_7$로 $(16/64)^8$ 이하인 2^{-16}이하이다. 만약 이러한 2 라운드 반복특성을 6번 사용하여 제안된 16 라운드 암호함수를 공격할 경우 반복 특성이 성립될 확률은 $((1/4)^8)^6=2^{-96}$로써 매우 낮아진다.

5.2 3 라운드 반복 가능한 특성

DES의 3 라운드 특성이 존재할 조건은 $a'\oplus f(a')=b'\oplus f(b')$, $f(a'\oplus f(b'))=a'\oplus b'$을 만족하는 a', b'이 존재하는 것이다. 2 라운드 반복 가능한 특성을 찾을 때의 암호함수내의 치환 P는 아무런 영향을 주지 못했으나, 3 라운드 반복 가능한 특성을 찾을 때 치환 P는 많은 영향을 미치게 된다. 3 라운드 특성부터는 중앙의 라운드를 중심으로 대칭인 특성을 가질 때 효율적인 공격이 가능한데 이런 특성을 반복 특성이라 하며, 3 라운드 반복 특성은 그림 4에서 a' 또는 b'이 0인 경우와 a'=b'(a'≠0)인 경우를 생각할 수 있다.

(1) a' 또는 b'이 0인 경우의 3 라운드 반복 특성이 존재할 조건식은 a'=0인 경우 f(b')=b'과 f(f(b'))=b으로 바뀌고 f(b')=b'으로부터 f(f(b'))=f(b')=b'이다. 따라서 b'=0

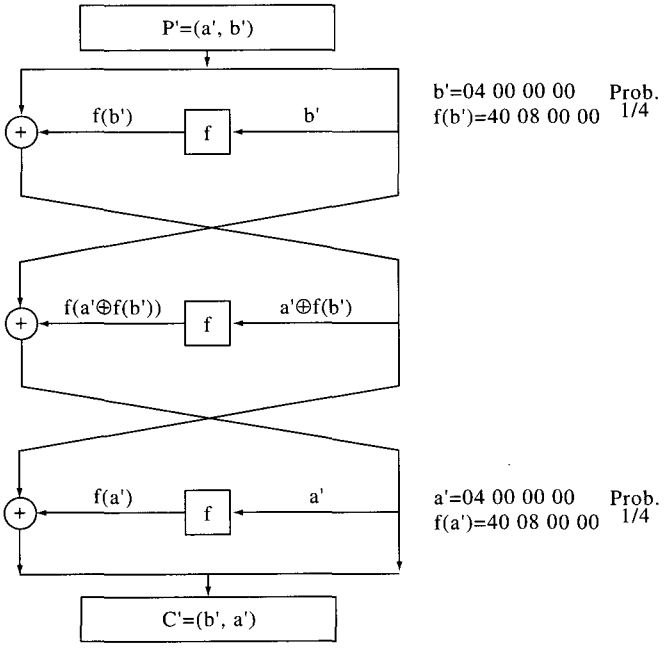


그림 4. 3 라운드 특성

인 경우 3 라운드 반복 가능한 특성이 존재할 조건식은 f(b')=b'이고 특성의 확률은 f(b')=b'의 확률의 제곱으로 $(16/64)^6$이하이다. (2) a'=b' (a'≠0)인 경우의 3 라운드 반복 가능한 특성이 존재할 조건식은 f(a' f(a'))=0으로, a'⊕f(a')=0인 경우와 a'⊕f(a')≠0인 경우로 나누어 생각할 수 있다. a' f(a')=0인 경우 DES의 3 라운드 반복 가능한 특성의 확률은 f(a')=a'의 확률의 제곱으로 $(16/64)^6$이하이고, a'⊕f(a')≠0인 경우의 DES의 3 라운드 반복 특성의 확률은 (1/234)*(a'->f(a')의 확률)^2 이하로 (1/234)* $(16/64)^2$ 이하이다.

제안된 암호함수의 3 라운드 특성도 a' 또는 b'이 0인 경우와 a'=b'(a'≠0)인 경우를 생각할 수 있다. (1) a' 또는 b'이 0인 경우의 3 라운드 반복 특성이 존재할 조건식은 a'=0이라고 할 때 f(b')=b'이다. (a) f(b')=b'의 확률이 x/64라고 가정하자. 그러면, 하나의 S_i-box의 입력 XOR값 X_i'는 00??00이고 나머지 S_j-box들의 입력 XOR값 X_j'(j≠i)는 000000이다. 따라서 Y_i(=??00)와 S_i-box의 출력 XOR값(S-box의 XOR 확률분포 특성(iii)에 의해 0이 아님)은 network permutation에 의해서 Y_{i+1}'블록과 Y_{i+2}'블록으로 이동하게 된다. 따라서 f(b')≠b'이다. (b) f(b')=b'의 확률이 (x1/64)*(x2/64)라고 가정하자. 이 때는 S-box의 XOR 분포의 확률이 $x_1/64$, $x_2/64$인 두 개의 S-box가 인접할 경우와 떨어져 있을 경우로 나누어 생각할 수 있다. 즉, 두 개의 S-box가 떨어져 있을 때 두 개의 S-box를 S_i와 S_j(|i-j|≥2)라고 하면 S_i-box와 S_j-box의 입력 XOR은 각각 X_i'=00??00이고, X_j'(j≠i)=00??00으로 Y_i와 Y_j는 ??00이며, Y_{i+1}은 S_i-box의 출력 XOR이고, Y_{j+1}은 S_j-box의 출력 XOR으로 network permutation에 의해 오른쪽으로 한 블록 쉬프트 하므로 f(b')≠b'이다. 두 개의 S-box가 인접되어 있을 때에도 (a)와 같이 network permutation에 의해 f(b')≠b'이다. 따라서 (a)와 (b)에 의해 제안된 암호함수의 3 라운드 반복 특성이 존재하기 위해서는 $Y_1, Y_2, \ldots, Y_8$이 모두 같은 값을 가져야 한다. 즉, $S_i(X_i')\oplus x_{i+1}$(i=1,2, . ,8)이 일정한 값(α)을 가져야 한다. 예로 b'=0110 0000 0110 0000 0110 0000 0110 0000이라면 $S_i(X_i')\oplus x_{i+1}=\alpha$, (i=1,2, . ,8)에서 f(b')=b'의 확률은 $(16/64)^4$(=(x_1/64)*1*(x_3/64)*1*(x_5/64)*1*(x_7/64)*1)이고 3 라운드 반복 특성이 존재할 확률은 f(b')=b'의 확률의 제곱으로 $(16/64)^8$이하이다.

(2) a'=b'(a'≠0)인 경우의 3 라운드 반복 가능한 특성이 존재할 조건식은 f(b'⊕f(b'))=0으로, b'⊕f(b')=0인 경우와 b'⊕f(b')≠0인 경우로 나누어 생각할 수 있다. (가) 만일 b'⊕f(b')=0이면 3 라운드 반복 가능한 특성의 확률은 f(b')=b'의 확률의 제곱으로 (a) f(b')=b'의 확률이 x/64라고 가정하면 하나의 S_i-box의 입력 XOR값 X_i'는 00??00이고 나머지 S_j-box들의 입력 XOR값 X_j'(j≠i)는 000000이다. 따라서 Y_i는 ??00이고 Y_{i+1}은 S_i-box의 출력 XOR값으로 network permutation에 의해서 Y_i블록이 Y_{i+1}'블록으로 이동하고, Y_{i+1}블록은 Y_{i+2}'블록으로 이동하게 된다. 따라서 f(b')≠b'이다. (b) f(b')=b'의 확률이 (x1/64)*(x2/64)라고 가정하면, 이 때는 S-box의 XOR 분포의 확률이 $x_1/64$, $x_2/64$인 두 개의 S-box가 인접할 경우와 떨어져 있을 경우로 나누어 생각할 수 있다. 즉, (i) 두 개의 S-box가 떨어져 있을 때 두 개의 S-box를 S_i와 S_j(|i-j|≥2)라고 하면 S_i-box와 S_j-box의 입력 XOR은 각각 X_i'=00??00이고, X_j'(j≠i)=00??00이다. 따라서 Y_i와 Y_j는 ??00이고

Y_{i+1}은 S_i-box의 출력 XOR이고, Y_{j+1}은 S_j-box의 출력 XOR으로 network permutation에 의해 Y_i블록과 Y_{i+1}블록은 Y_{i+1}'블록과 Y_{i+2}'블록으로 이동하게 되고, Y_j블록과 Y_{j+1}블록은Y_{j+1}'블록과 Y_{j+2}'블록으로 쉬프트함으로 f(b')≠b'이다. (ii) 두 개의 S-box가 인접되어 있을 때에도 (a)와 같이 network permutation에 의해 f(b')≠b'이다. 따라서 (a)와 (b)에 의해 제안된 암호함수의 3 라운드 반복 특성이 존재하기 위해서는 Y_1, Y_2, . . . , Y_8이 모두 같은 값을 가져야 한다. 즉, $S_i(X_i')\oplus x_{i+1}$(i=1,2, . ,8)이 일정한 값을 가져야 한다. 따라서 f(b')=b'의 확률은 (1)에서와 같이 $(16/64)^4$이고 3 라운드 반복 특성이 존재할 확률은 f(b')=b'의 확률의 제곱으로 $(16/64)^8$이하이다.

(나) 만일 b'⊕f(b')≠0이면 3 라운드 반복 가능한 특성의 확률은 (b'->f(b')의 확률)^2*(b'⊕f(b')->0이 될 확률)로 $(16/64)^2*(16/64)^8$ 이하이다.

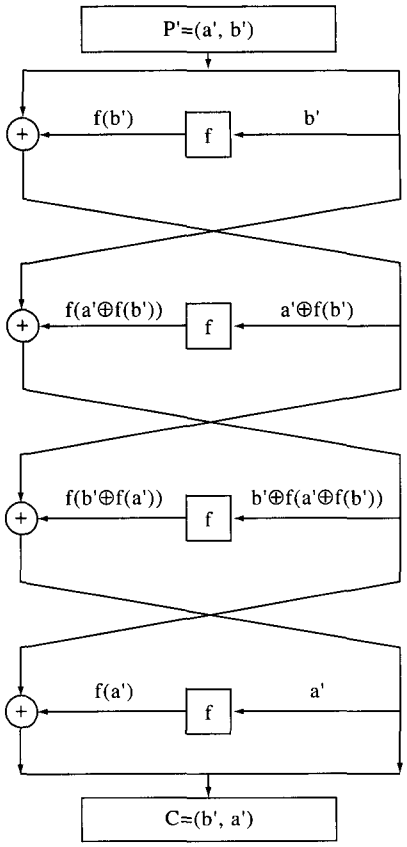


그림 5. 4-라운드 특성

5.3 4 라운드 반복 가능한 특성

DES의 4 라운드 반복 특성이 존재하기 위해서는 f(a')=f(a'⊕f(b')), f(b')=f(b'⊕f(a'))을 만족하는 a', b'이 존재해야 한다. 4 라운드 반복 가능한 특성은 그림 5에서 a' 또는 b'이 zero인 경우와 a'=b'(a'≠0)인 경우로 나누어 생각할 수 있다.

(1) a' 또는 b'이 zero인 경우 4 라운드 반복 가능한 특성이 존재할 조건은 a'=0 이라고 가정할 때 0=f(f(b'))과 f(b')=f(b')으로 바뀐다. 따라서 f(f(b'))=0일 확률을 계산하면 된다. 만일 f(b')=0이면 4 라운드 반복 가능한 특성이 아니고 2 라운드 반복 가능한 특성을 두 번 연결한 것이 된다. 따라서 f(b')≠0인 경우에 대해서만 고려해 보면 a'=0이고, f(b')≠0일 때 4 라운드 반복 가능한 특성의 확률은 (b'->f(b')의 확률)2과, f(b')->0의 확률의 곱으로 $(16/64)^4*(1/234)$ 이하이다.

(2) a'=b'(a'≠0)인 경우 4 라운드 반복 가능한 특성이 존재할 조건은 f(b'⊕f(b'))=f(b')으로 (f(b'⊕f(b'))=f(b'))이 만족될 때 b'->f(b')의 확률)^{2}과 (b' f(b')->f(b')의 확률)^{2}의 곱으로 $(16/64)^8$ 이하이다.

제안된 암호함수의 4 라운드 반복 특성도 a' 또는 b'이 zero인 경우와 a'=b'(a'≠0)인 경우로 나누어 생각할 수 있다.

(1) a'=0, f(b')≠0인 경우에 b'->f(b')의 확률을

x/64라고 가정하면 적당한 S_i-box의 입력 XOR만이 zero가 아니고 그 형태는 00??00이다. 그러나 i 번째 출력 블록 $Y_i(=x_i \oplus S_{i+7}(X_{i+7}')=??00)$는 network permutation에 의해 Y_{i+1}' 블록으로 옮겨가고, S_i-box의 출력 XOR(S-box의 XOR 확률분포 특성(iii)에 의해 0이 아님)인 $Y_{i+1}(=x_{i+1} S_i(X_i'))$블록은 Y_{i+2}' 블록으로 이동하므로 $f(b')\neq 0$이 아닌 블록이 존재하고 블록내의 1비트 값은 두 개 이상이다. 따라서 암호함수의 입력이 f(b')일 때 S-box의 입력 XOR이 011000이거나 6개의 비트중 1비트 값이 한 개인 S-box가 존재하지만 새로이 제안된 암호함수에서 f(f(b'))=0이 될 수 없다. 제안된 암호함수의 f(f(b'))=0이 되기 위해서는 모든 S-box의 입력 XOR이 non-zero가 되야 하므로 b'->f(b')의 확률은 $(x/64)^4$이 되야 하고, 암호함수의 입력이 f(b')일 때 f(f(b'))=0이 되는 확률은 2 라운드 특성에서처럼 $(16/64)^8$이하이다. 그러므로 $f(b')\neq 0$일 때 제안된 암호함수의 4 라운드 반복 특성은 다음과 같다.

(b'->f(b')의 확률)^{2}과 f(b')->0의 확률의 곱으로 $(16/64)^8*(16/64)^8$ 이하이다.

(2) $a'=b'(a'\neq 0)$인 경우 4 라운드 반복 가능한 특성이 존재할 조건은 $f(b'\oplus f(b'))=f(b')$으로 b'->f(b')의 확률을 x/64라고 가정하면 적당한 S_i-box의 입력 XOR만이 zero가 아니고 그 형태는 00??00이다. 그러나 i 번째 출력 블록 $Y_i(=x_i \oplus S_{i+7}(X_{i+7}')=??00)$는 network permutation에 의해 Y_{i+1}' 블록으로 옮겨가고, S_i-box의 출력 XOR(S-box의 XOR 확률분포 특성(iii)에 의해 0이 아님) $Y_{i+1}(=x_{i+1} \oplus S_i(X_i'))$블록은 Y_{i+2}' 블록으로 이동하므로 $f(b')\neq 0$이 아닌 블록이 존재하고 블록내의 1비트 값은 두 개 이상이다. 따라서 암호함수의 입력이 $b'\oplus f(b')$일 경우 S-box의 입력 XOR 011001이거나 011000이거나 6 개의 비트중 1비트 값이 한 개인 S-box가 존재하지만 제안된 암호함수에서 $f(b'\oplus f(b'))=f(b')$이 될 수 없다. $f(b'\oplus f(b'))=f(b')$이 되기 위해서는 모든 S-box의 입력 XOR이 non-zero가 되야 하므로 b'->f(b')의 확률은 $(x/64)^4$이 되야 하고, 암호함수의 입력이 $b'\oplus f(b')$일 때 $f(b'\oplus f(b'))=f(b')$이 되는 확률은 $(16/64)^8$이하이다. 그러므로 $a'=b'(a'\neq 0)$일 때 제안된 암호함수의 4 라운드 반복 특성은 다음과 같다.

(b'->f(b')의 확률)^{2}과 $b'\oplus f(b')$->f(b')의 확률의 곱으로 $(16/64)^8*(16/64)^8$ 이하이다.

5.4 13 라운드의 DC 공격

DES의 13 라운드 특성은 2 라운드 반복 특성을 6번 반 사용하여 구하여 지므로 DES의 13 라운드 특성이 주어질 확률은 $(16/234)^6$이하로 약 $2^{-43.2}$이다. 제안된 암호함수의 13 라운드 특성도 2 라운드 반복 특성을 6번 반 사용하므로 $((1/2)16)^6$으로 2^{-96}이다.

5.5 16 라운드의 DC 공격

라운드의 수가 클 경우 DC 공격은 2 라운드 반복 가능한 특성을 이용하여 큰 라운드의 특성을 구성하는데, 1992년 Biham과 Shamir는 1990년 처음 발표된 DC 공격 방법을 발전시켜 16 라운드 DES를 2^{37}의 복잡도로 공격할 수 있는 새로운 DC 공격 방법을 제안하였다[7]. 제안된 방법은 그림 6와 같은 구조로 맨 앞 2 라운드에서 $(1/234)^6$의 확률을 갖는 13 라운드 반복특성을 사용하였다.

P를 임의의 64비트 평문이라 하고, $v_0, \ldots,$ v_{4095}는 첫 라운드의 S_1, S_2, S_3 box에만 non-zero가 입력될 때 발생될 수 있는 2^{12}개의 32비

트라고 하면, 2^{24}의 평문쌍이 존재하며, 이들 평문쌍들의 XOR은 언제나 (v_k,q)의 형태를 가지며, v_k는 2^{12}번 발생한다. 입력될 수 있는 평문쌍$(P_i, \overline{P_i})$과 이에 대한 암호문쌍$(T_i, \overline{T_i})$은 다음과 같이 정의할 수 있다.

$$P_i=P\oplus(v_i,0), P_i=(P\oplus(vi,0))\oplus(0,q),\ 0\le i<2^{12}$$
$$T_i=DES(P_i,K), T_i=DES(P_i,K) \quad (5)$$

이들 평문쌍들에 의한 XOR값들 중에 2^{12}쌍은 첫 라운드 암호함수의 출력 XOR값과 일치

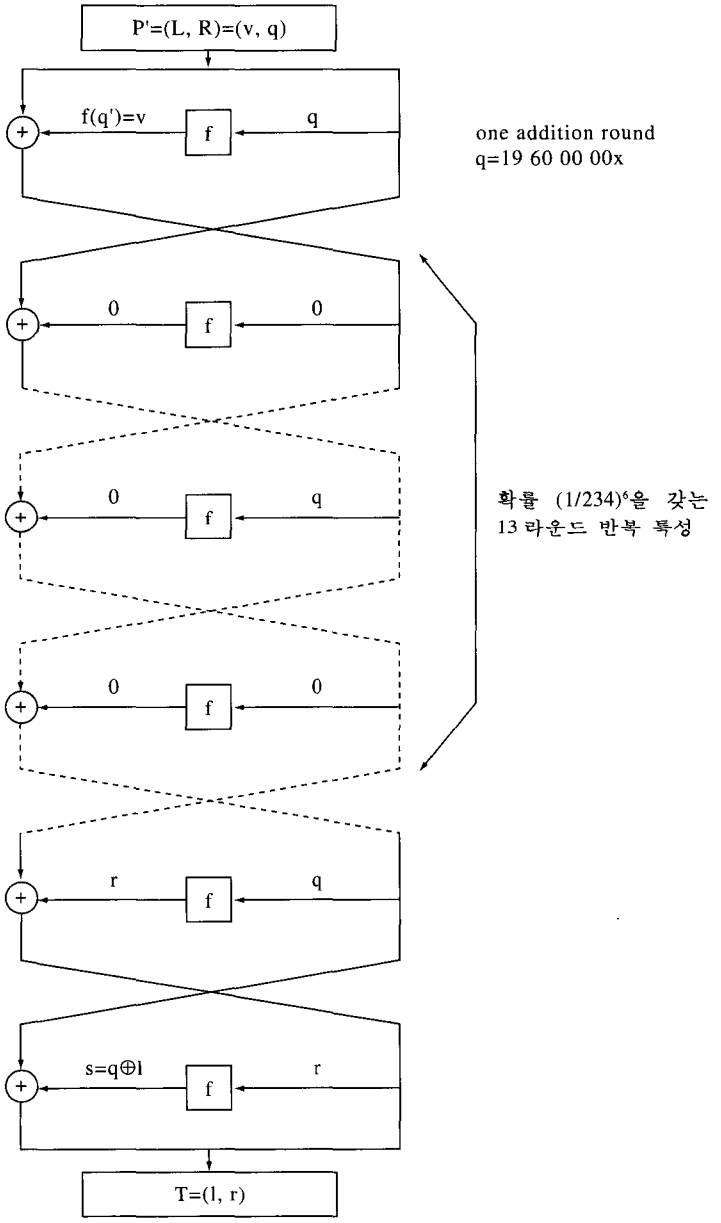


그림 6. 16 라운드 DES 공격

하므로 두 번째 라운드에 (q, 0)가 입력되는 반복 특성을 얻을 수 있다. 따라서 16 라운드 반복 특성을 만족하는 암호키를 찾을 수 있는 평문쌍(right pair)을 얻을 수 있는 확률은 $2^{12}*(1/234)^6 = 2^{-35.2}$가 되고 16 라운드 DES의 공격은 2^{36}개의 암호문쌍을 2^{37}번 분석함으로서 공격이 가능하다.

제안된 암호함수의 16 라운드 DC의 확률은 2^{-84}이하 ($2^{12}*((1/4)^8)^6 = 2^{-84}$)이다.

6. 결 론

본 논문에서는 DES에 대한 DC의 대응방안으로서 DES의 일부를 수정하여 N-1 라운드 특성이 구성될 확률을 낮추는 방법을 사용하였다. 제안된 암호함수는 기존의 DES 암호함수 분석방법과 최근 발표된 DC 공격 분석을 통해 기존 DES와 비교 평가하였다. 그 결과 DES보다 제안된 암호함수가 DC 공격에 대한 높일 수 있었고 결과를 아래 표 4에 나타내었다. 따라서 제안된 암호함수는 국제 표준으로 공인된 DES를 수정하여 DC 공격에 대한 비도를 높일 수 있었고 DES와 같은 수준에서 안전성을 평가하였으므로 DES 이상의 비도 및 안전성이 보장되며 실용적 가치가 있을 것으로 판단된다.

표 4. DES와 제안된 암호함수의 DC 공격에 대한 복잡도

	제안된 암호함수	기존 암호함수
2-round	2^{-16}	$2^{-7.2}$
3-round	2^{-16}*, 2^{-20}**	2^{-12}*, $2^{-11.2}$**
4-round	2^{-32}*, 2^{-32}**	$2^{-43.2}$
16-round	2^{-84}	$2^{35.2}$

* 는 조건식에서 a' 또는 b'이 0인 경우

**는 조건식에서 a'=b'(a'≠0)인 경우

참 고 문 헌

[1] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptanalysis," Journal of CRYPTOLOGY, Vol.4, No.1, 1991.

[2] E. Biham and A. Shamir, "Differential Cryptanalysis of FEAL and N-hash," technical report, Weizmann Institute of Science, Israel, 1991.

[3] M.H. Dawson and S.E. Tavares, "An Expanded Set of S-box Design Criteria based on information theory and its relation to differential-like attacks," proc. of EUROCRYPT91, Springer-Verlag, 1991

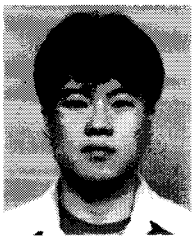
[4] L. Brown, M. Kwan, J. Pieprzyk and J. Seberry, "Improving Registance to Differential Cryptanalysis and the Redign of LOKI," Abtract of ASIACRYPT'91, 1991.

[5] Kaisa Nyberg, "Generalized Feistel Network," advances in Cryptology ASIACRYPT' 96

[6] 남길현, "확장된 DES-like 암호 알고리즘의 안전성 분석과 Differential Cryptanalysis에 관한 연구", 한국전자통신연구소 데이터 보호 기반 기술 연구 (I), 1992

[7] E. Biham and A. Shamir, "Differential Cryptanalysis of the full 16-round DES," Proc. of CRYPTO92.

□ 著者紹介



김 구 영

1995년 동국대학교 전자공학과 졸업
현 동국대학교 전자공학과 대학원 석사 과정

원 치 선

1982년 고려대학교 전자공학과 졸업
1986년 매사추세츠대 (엠허스트) 석사
1990년 매사추세츠대 (엠허스트) 박사
1989 ~ 1992년 LG전자 (현)영상미디어 연구소 선임연구원
1992년 ~ 현재 동국대학교 전자공학과 부교수

※ 주관심 분야 : 디지털 영상처리, 디지털 비디오 전송 시스템