通信情報保護學會誌
第3卷 第3號, 1993. 9

DES의 선형 해독법에 관한 해설(Ⅰ)

김 광 조*

요 약

본 해설은 1993년 1월 28일 부터 1월 30일까지 일본의 전자통신정보학회 산하 정보 시큐리티 연구회가 연례적으로 개최하는 SCIS'93(Symposium on Cryptography and Information Security)에서 우수 논문상을 수상한 미쓰비시 전기㈜의 마쓰이가 발표한 DES에 관한 새로운 해독 방법 즉, 선형 해독법에 관하여 이번호와 다음호 2부로 나누어 번역하여 소개한다.

1. 서 론

Biham과 Shamir에 의해 Differential Cryptanalysis[1]를 발표한 이래 DES-like의 비밀키 암호방식에 관한 해독법 연구가 상당히 진보되었다고 생각된다. 그들은 이어서 논문[2]에서 FEAL 암호를 31단까지 선택 평문 공격에 의해 해독하고, 최근의 논문[3]에는 16단의 DES 암호문 선택평문공격에 성공함을 제시하였다.

Differential Cryptanalysis는 본질적으로 선택 평문 공격법이나, 해독자가 조작해야 하는 것은 평문이 아니라, 2개의 평문쌍의 Exclusive Or값이므로 해독자에게 충분한 량의 평문이 주어진다는 조건아래에서 기지 평문 공격(Known Plaintext Attack)이 적용된다고 말할 수 있다.

그러나, 위의 기지평문 공격법은 n비트 블럭 암호의 경우 단수에 관계없이 적어도 $2^{n/2}$개의 기지 평문이 필요로 하나(예를들어, DES-8의 경우 2^{38}개[3], FEAL-8의 경우 2^{37}개[2]), 단수가 작은 암호의 경우에는 보다 효율적인 해독 방법이 연구되고 있다. FEAL 암호에 관하여 이런 방법에서의 연구 결과로서 Tardy-Corfdir, Gilbert는 F 함수를 바이트 단위로 선형 근사함으로서 FEAL-6을 20,000개의 기지 평문으로 해독하고[4] 마쓰이와 야마기시는 주어진 평문에서 부터 적당한 것을 추출하여 암호 알로기즘을 선형화하는 방식을 이용하여 FEAL-8을 2^{15}개의 기지 평문으로 키의 전수 검사 보다 빠른 해독 방법을 제시하였다[5]. 이런 방법은 가산 연산 중 발생하는 carry를 해독자가 제어하는 방식을 이용하여 암호 알고리즘 중에서 단순화한 산술 연산의 특성을 이용한 것으로, DES 암호와 같이 변환 테이블을 사용하는 암호 알고리즘에는 직접 적용이 곤란하다.

본 연구에는 이러한 아이디어를 DES 암호의 기지 평문 공격으로도 사용 가능하도록 새로운 선형해독법(Linear Cryptanalysis)을 제안한다. 이 방법은 주어진 암호 알고리즘에 대하여 그 평문과 암호문의 관계를 비트 단위로 선형 근사시킴을 목표로 한다.

이것을 실현하기 위하여 우선 DES 암호의 비선형

* 한국전자통신연구소 실장

요소인 8개의 S-box의 입출력간의 선형 근사식을 유도하는 것으로 부터 출발한다. 그리고 이 근사식을 F 함수에서부터 알고리즘 전체로 확장하고, 최종적으로 평문에서 암호문에 이르는 일련의 확률적 선형 비트 경로를 구성하고 그 경로에 영향을 주는 키 비트를 전수 검사로 구하는 방법이다. 이 방법을 이용하여 기지평문 공격에 의한 DES 암호 해독은 컴퓨터 시뮬레이션 결과 DES-8은 2^{21}개의 기지 평문으로 40초, DES-12는 2^{33}개의 기지 평문으로 50시간에 키를 찾아 내었다. 사용한 컴퓨터는 HP 9750(PA-RISC/66MHz)이고 C 언어로 구현하였다.

본 논문에서는 이 방법을 DES-16에 적용한 경우, 해독에 필요한 기지 평문 수는 2^{47}개임을 제시하고 제안한 기지 평문 공격 방식은 대단히 간단하고 평문을 저장하는 메모리를 필요로 하지 않는다. 이것은 DES-16에 대한 키 전수 검사 보다 고속인 기지 평문 공격의 최초의 결과이다.

또한 본 해독법은 키의 도출에 평문의 특정 비트만을 사용하므로 기지평문 조건을 완화시킬 수 있다. 즉, 해독에 필요한 평문 수를 증가시켜서 평문의 적당한 비트 위치의 확률 정보만을 사용하여 키를 구할 수 있는 특징을 가지고 있다. 이것은 본 해독법이 COA(Ciphertext Only Attack)에서도 적용 가능을 의미한다.

예를 들면, DES-8의 경우 미지의 평문이 랜덤한 ACSII 코드(16진의 00-7F)로 되어 있다면 2^{37}개의 암호문만으로 키를 구할 수 있으며 또한 평문이 영문으로 ASCII 코드로 표현되어 있다는 조건하에는 2^{29}개의 암호문으로 키의 도출이 가능하다.

더욱이 DES-16에 대해서도 평문이 1비트도 주어져 있지 않는 경우라도 그 평문의 확률 정보뿐으로 키의 전수 검사 보다도 고속으로 COA가 성립하는 상황이 존재하는 것도 가능하다.

2. 준 비

그림 1과 그림 2는 본고에서 취급하는 DES의 암호화 처리부 및 F 함수의 구성도이다. 암호화 처리부 중 초기 전치 IP 및 최종 전치 IP^{-1}는 1대 1 사상이므로 생략한다. 본고에서는 다음의 기호를 사용하며 특히 단수에 의존하지 않는 경우는 단수를 표시하는 첨자를 생략한다. 또한 각 그림에 있어서 오른쪽은 하위로 하고 특히 최하위 비트는 0번째 비트로 약속한다.

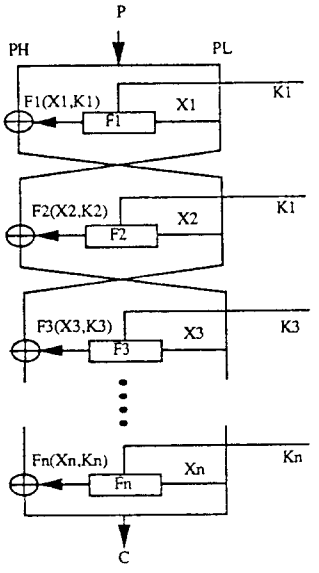

그림 1. DES 암호화 과정

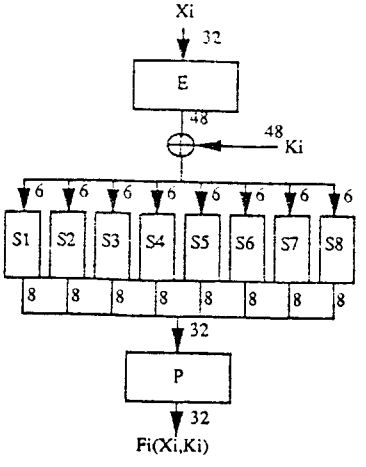

그림 2. DES의 F함수(숫자는 bit수)

- P : 평문 64 비트
- C : 암호문 64 비트
- P_H, P_L : 평문의 상위 32비트, 하위 32 비트

- C_H, C_L : 암호문의 상위 32비트, 하위 32 비트
- X_i : 제 i 단의 F 함수의 32 비트 입력
- K_i : 제 i 단의 확대키 48 비트
- $F_i(X_i, K_i)$: 제 i 단의 F 함수
- $A[i]$: A의 제 i 번째 비트
- $A[i, j, \cdots, k] : A[i] \oplus A[j] \oplus \cdots \oplus A[k]$

3. 해독 원리

선형 해독법의 목표는 랜덤하게 주어진 평문 P와 대응하는 암호문 C 및 키 K에 대하여 유의 확률 p로 다음식과 같은 형태의 선형 근사식을 구성하는 데 있다.

$$P[i_1, i_2, \cdots, i_a] \oplus C[j_1, j_2, \cdots, j_b] = K[k_1, k_2, \cdots, k_c] \quad (1)$$

여기서 $i_1, \cdots, i_a, j_1, \cdots, j_b, k_1, \cdots, k_c$는 고정된 비트 위치이고, 유의 확률이란 $p \neq 1/2$를 의미한다. 실제 이식의 구성에 성공하면 암호 해독자는 maximum likelihood법을 이용하여 키의 1 비트 $K[k_1, k_2, \cdots, k_c]$를 의미있게 추정할 수 있을 것이다. 즉,

[**Algorithm 1**]

step 1 : 주어진 모든 기지 평문과 대응되는 암호문의 쌍으로 부터 $P[i_1, i_2, \cdots, i_a] \oplus C[j_1, j_2, \cdots, j_b]$를 계산한다.

step 2 : 이 값이 0이된 평문수가 전체 평문의 반 이상이 되면 $K[k_1, k_2, \cdots, k_c]=0 (p>1/2)$ 일때), 또는 1 ($p<1/2$ 일때)로 추정한다. 이 값이 0이된 평문수가 전체 평문의 반 이하가 되면 $K[k_1, k_2, \cdots, k_c]=0 (p>1/2)$ 일때), 또는 ($p<1/2$ 일때)로 추정한다.

이 추정이 성공할 확률은 기지 평문수 N과 식(1)의 성공 확률 p로 결정되므로 N 또는 $|p-1/2|$ 가 클수록 당연히 이 확률이 커진다. 식 (1)의 형태를 갖는 선형 근사식 중, $|p-1/2|$ 가 최대가 되는 것을 최량 표현이라 부르고, 그 성립 확률을 최량 확률이라고 부르면 해독자의 관심은 다음과 같다.

P1 : 선형 근사식의 구체적 구성법

P2 : 해독 성공 확률을 N과 p에 의한 표현

P3 : 최량 표현과 최량 확률의 계산

위의 방법으로 FEAL 암호에 관하여 마쯔이와 야마기시의 결과[5]는 주어진 기지 평문 중에서 적당한 것을 선택하는 것 (**P1**)에 의해 식 (1)을 확률 1로 성립시키는 것 (**P2, P3**)이 해독이 완료됨을 의미한다.

DES 암호를 대상으로 하는 본고에서는 우선, (**P1**)을 구하기 위해 4절에서 S-box의 선형 근사식을 유도하는 것으로 부터 출발한다. 5절에는 이 근사식을 알고리즘 전체로 연장하여 식(1)의 형태로 도달하는 것을 목표로 하며 (**P2**)의 확률도 계산한다 (보조정리 2). (**P3**)에 관하여는 약간의 고찰과 컴퓨터에 의한 검색이 필요하므로 본고에는 그 결과만을 제시한다(부록 B).

실제 n단의 암호의 해독을 위하여 최적의 $n-1$단의 최량 표현을 사용한다. 즉, 최종단은 제 n단 F 함수에 입력되는 라운드키 K_n을 이용하여 복호된다는 점을 고려하여 근사식 중에 F 함수를 넣어 계산한다. 그 결과가 다음식과 같고 이식을 $n-1$단의 최량 확률로 성립시키도록 한다.

$$P[i_1, i_2, \cdots, i_a] \oplus C[j_1, j_2, \cdots, j_b] \oplus F_n(C_L, K_n)[l_1, l_2, \cdots, l_d] = K[k_1, k_2, \cdots, k_c] \quad (2)$$

그런데 지금, 이식에 잘못된 K_n를 대입하였다고 유의성은 명백히 감소한다. 즉, 식 (2)의 성립 확률이 거의 1/2인 경우이다. 따라서 해독자는 다음에 표시하는 maximum likelihood법을 이용하여 K_n 및 $K[k_1, k_2, \cdots, k_c]$를 의미있게 추정하는 것이 가능하다.

[**Algorithm 2**]

Step 1 : K_n의 각 후보값에 대한 카운터를 설정하여 0으로 초기화한다.

Step 2 : 주어진 각 기지 평문과 대응하는 암호문 쌍에 대하여 다음을 실행한다.

- K_n의 각 후보값에 대하여 식 (2)의 좌변을 계산하고, 그 결과가 0으로 된 키에 해당하는 카운터 값에 1을 증가시킨다.

Step 3 : 모든 카운터의 값에서 최대치 T_{max}와 최소치 T_{min}을 비교하여 기지 평문수 N에 대하여

• $|T_{max}-N/2| > |T_{min}-N/2|$ 이면 T_{max}에 대응하는 K_n을 선택하고, 식(2)의 우변은 $0(p>1/2$ 일때) 또는 $1(p<1/2$ 일때)로 추정한다.

• $|T_{max}-N/2| < |T_{min}-N/2|$ 이면 T_{min}에 대응하는 K_n을 선택하고, 식(2)의 우변은 $1(p>1/2$ 일때) 또는 $0(p<1/2$ 일때)로 추정한다.

이 해독법의 성공 확률은 보조정리 4로 주어진다. 그러나 본 방식에서는 식 (2)를 풀기 위해서는 평문의 a개 비트만이 사용되고 있다는 점을 주의한다. 따라서, 반드시 최량 표현은 아니지만, a의 값이 작은 별도의 관계식을 이용하여 **Algorithm 2**를 실행하면 해독에 필요한 기지 평문수를 증가시키는 대신에 평문에 관한 정보량을 감소시키는 것이 가능하다.

여기서 평문에 관한 적당한 확률 정보가 주어져 있다면 식 (2) 중 평문에 관한 항을 삭제하여도 그 유의성을 잃지 않을 가능성이 있다. 이것은 COA가 성립한다는 면을 시사하며 본고의 6절에는 DES 암호의 최량 근사식을 이용하여 기지평문 공격을 서술하고 COA는 별도로 구체적으로 보고한다.

4. S-box의 선형 근사

DES 암호는 8개의 S-box $S_1, \cdots, S_8$은 각각 6비트의 입력을 갖고 있으므로 입력 패턴의 총수는 $2^6=64$이다. 본 절에는 우선 각 S-box에 대하여 몇개의 입력 비트의 Exclusive Or값과 몇개의 출력 비트의 Exclusive Or값이 64개 중 몇개가 일치하는가를 우선 조사한다.

정의 1 *S-box* S_a ($a=1, 2, \cdots, 8$)에 있어서, S_a의 입력 64개 중에 $1\leq\alpha\leq63$으로 마스크된 입력 비트 위치와 $1\leq\beta\leq15$로 마스트된 출력 비트의 *Exclusive Or*값이 일치되는 경우의 수를 $NS_a(\alpha, \beta)$로 표현한다. 즉,

$$NS_a(\alpha, \beta) = \#\{x \mid 0\leq x<64, \bigoplus_{s=0}^{5} (x[s] \cdot \alpha[s]) = \bigoplus_{t=0}^{3} (S_a(x)[t] \cdot \beta[t])\}$$

여기서 • 는 비트 단위의 곱셈을 의미한다.

[예]

$$NS_5(16, 15)=12 \qquad (3)$$

이 값이 32가 되지 않는 경우 S-box의 입출력 비트간에 상관이 있다고 생각된다. 예를들면, 식 (3)에 의해서 S_5의 입력의 4번째 비트는 확률 12/64=0.19로 모든 출력비트의 Exclusive Or와 같아진다는 것을 의미한다. 이것은 F 함수 내부의 비트 확장 E와 P를 고려하면, 키 K를 임의로 고정하여 F 함수에 랜덤한 입력 X가 들어가면 다음식이 확율 0.19로 성립함을 의미한다.

$$X[15] \oplus F(X, K)[7, 18, 24, 29]=K[22] \qquad (4)$$

또한, 다음식이 1-0.19=0.81의 확률로 성립한다.

$$X[15] \oplus F(X, K)[7, 18, 24, 29]=K[22] \oplus 1 \qquad (5)$$

식(3)은 모든 S-box 중에 편차가 가장 큰 것, 즉 $|NS_a(i, j)-32|$ 를 최대로 하는 것으로 식 (4)은 F 함수의 최량 표현이다. 또한 S-box의 구성법에 의해 다음과 같은 사실을 쉽게 알 수 있다.

보조정리 1.

1. $NS_a(i, j)$는 짝수 값을 갖는다.
2. i값이 *1, 32* 또는 *33*의 경우, 임의의 *S-box*와 j에 $NS_a(i, j)=32$이다.

부록 A는 S_5에 대하여 $NS_5(i, j)-32$의 값을 모든 i와 j에 대하여 계산하였다. 여기서, 종축은 i, 횡축은 j을 나타내며 표중에 절대값이 클수록 그 입출력 비트간의 상관이 크다는 것을 나타낸다.

5. Involution의 선형 근사

5.1. 3단 DES

본 절에서는 전절에서 구성한 F 함수의 선형 근사식을 알고리즘 전체로 확장하는 방법에 대하여 예를 들면서 설명한다.

최초로 3단의 DES를 생각한다(그림 3). 제 1 단의 F 함수에 식 (4)을 적용하면 확률 12/64로 다음식이 성립한다.

$$X_2[7, 18, 24, 29] \oplus P_H[7, 18, 24, 29] \oplus P_L[15]=K_1[22] \qquad (6)$$

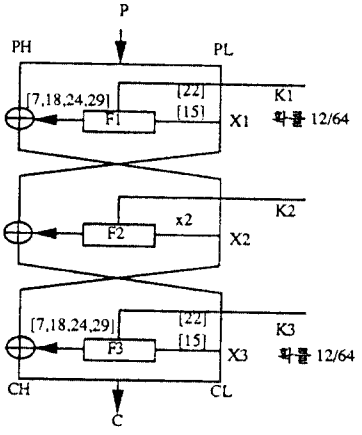

그림 3. 3단 DES

같은 방식으로 제 3 단의 F 함수에도 식(4)을 적용하면 역시 12/64의 확률로 다음 등식이 성립한다.

$$X_2[7, 18, 24, 29] \oplus C_H[7, 18, 24, 29] \oplus C_L[15]=K_3[22] \quad (7)$$

따라서 위의 2개 식에서 X_2를 삭제하면

$$P_H[7, 18, 24, 29] \oplus C_H[7, 18, 24, 29] \oplus P_L[15] \oplus C_L[15]=K_1[22] \oplus K_3[22] \quad (8)$$

을 얻을 수 있다.

여기서, 랜덤하게 주어진 평문과 대응하는 암호문에 대하여 식(8)이 성립하는 확률은 식(6)과 식(7)이 동시에 성립할 확률과 동시에 성립하지 않을 확률의 합이므로, $(12/64)^2+(1-12/64)^2=0.70$이 된다. 식(4)가 한개의 F 함수로 달성 가능한 최량 표현이라면, 식(8)는 3단 DES로 실현되는 최량 표현이 된다.

또한, 식(8)의 좌변이 해독자에게 알려진 값이라는 것으로 충분한 량의 기지 평문이 주어져 있다면, 식(8)에 **Algorithm 1**을 적용하여 해독자는 그식의 우변을 추정하는 것이 가능하다.

여기서 이 해독의 성공확률은 일반적으로 다음의 보조정리에 나타낸 바와 같으며, 증명은 이항 분포를 정규 분포에 근사시킴으로서 가능하다.

보조정리 2 : N개의 랜덤한 기지 평문을 이용하여 *Algorithm* 1을 실행할 때, 그 성공 확률은 다음과 같다.

$$\int_{-2\sqrt{N}|p-1/2|}^{\infty} \frac{2}{\sqrt{\pi}} e^{-x^2/2} dx \quad (9)$$

식 (9)의 계산값은 표 1과 같다.

표 1. Algorithm 1의 추정 성공 확률(%)

N	추정 성공 확률
$\frac{1}{4}\|p-1/2\|^{-2}$	84.1
$\frac{1}{2}\|p-1/2\|^{-2}$	92.1
$\|p-1/2\|^{-2}$	97.7
$2\|p-1/2\|^{-2}$	99.8

5.2. 5단 DES

다음은 5단 DES를 고찰한다(그림 4). 여기서 우선, 제 2 단 F 함수에 식(4)을 적용하고 제 1 단 F 함수에 다음식을 적용한다.

$$X[27, 28, 30, 31] \oplus F(X, K)[15]= K[42, 43, 45, 46] \quad (10)$$

식(10)에는 $NS_1(27, 4)=22$에서 얻은 것으로 그 성립확률은 $22/64=0.34$이다. 이 때, 전절에서와 같이 간단한 계산으로 다음의 근사식을 얻는다.

$$X_3[7, 18, 24, 29] \oplus P_H[15] \oplus P_L[7, 18, 24, 27, 28, 29, 30, 31] =K_1[42, 43, 45, 46] \oplus K_2[22] \quad (11)$$

또한, 같은 방법으로 제 4 단의 F 함수에 식(4), 제 5 단의 F 함수에 식 (10)을 적용하면,

$$X_3[7, 18, 24, 29] \oplus C_H[15] \oplus C_L[7, 18, 24, 27, 28, 29, 30, 31] =K_4[22] \oplus K_5[42, 43, 45, 46] \quad (12)$$

따라서, 이식들에서 X_3을 소거하고, 평문과 암호문을 연결하여 다음의 관계식을 구한다.

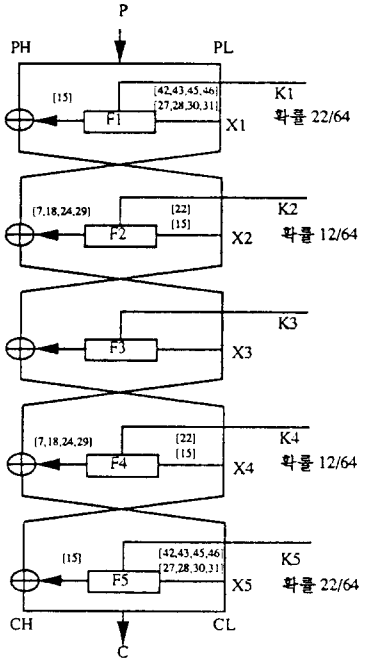

그림 4. 5단 DES

$$P_H[15] \oplus P_L[7, 18, 24, 27, 28, 29, 30, 31] \oplus C_H[15] \oplus C_L[7, 18, 24, 27, 28, 29, 30, 31] = K_1[42, 43, 45, 46] \oplus K_2[22] \oplus K_4[22] \oplus K_5[42, 43, 45, 46] \quad (13)$$

그러면 식(13)의 성립확률은 이것들의 합계 총 4회의 근사 중 짝수개가 성립하고 나머지가 성립않는 확률이므로 간단히 계산 가능하다. 여기서는 보다 일반적인 형태로 다음의 보조정리를 제시한다. 증명은 n에 관하여 귀납법으로 가능하다.

보조정리 3. [Piling-up Lemma]

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 식과 같이 얻어진다.

$$2^{n-1} \prod_{i=1}^{n} (p_i - 1/2) + 1/2 \quad (14)$$

따라서, 랜덤하게 주어진 기지 평문에 대하여 식(13)이 성립할 확률은 $2^3(-10/64)^2\ (-20/64)^2 + 1/2 = 0.519$가 되는 것을 알 수 있다. 따라서, 보조정리 2를 이용하면 $(1/0.019)^2 = 2800$개 정도의 기지평문을 이용하면 틀림없이 식(13)의 우변을 추정하는 것이 가능하다.

5.3. 임의 단의 DES에로 확장

임의 단의 DES에 있어서 선형 근사식의 구성은 그림 5에서 보듯이 5단의 근사로 부터 출발한다. 이것은 제 2 단의 F 함수에 식(4)를 적용하고 제 3 단과 제 4 단의 F 함수에는 각각 다음식을 적용한다.

$$X[29] \oplus F[X, K][15] = K[44] \quad (15)$$

$$X[15] \oplus F[X, K][7, 18, 24] = K[22] \quad (16)$$

이 식은 $NS_1(4, 4) = 30$ 및 $NS_5(16, 14) = 42$에서 유도한 것으로 각각의 성립 확률은 $30/62 = 0.469$, $42/64 = 0.656$이다. 이 때, 간단한 계산에 의해 X_1과 X_5를 연결하면 다음의 선형 근사식을 얻는다.

$$X_1[7, 18, 24, 29] \oplus X_5[7, 18, 24] = K_2[22] \oplus K_3[44] \oplus K_4[22] \quad (17)$$

여기서 식(17)이 성립된 확률은 Piling-up Lemma에 의해 $2^2(-20/64)(-2/64)(10/64) + 1/2 = 0.506$임을 알 수 있다. 이 확률은 5단 DES 암호의 근사한 값보다 낮으나, 식(17)은 평문과 암호문의 하위 32 비트만을 표현하고 있다는 특징을 가지고 있다. 따라서, 이관계식을 알고리즘 중에 반복하여 사용함으로서 임의 단의 DES 암호에서 평문과 암호문을 연결하는 의미있는 선형 근사식의 구성이 가능하다.

예를들면, 그림 6은 식(17)을 16단 DES 암호에 적용한 경우이다. 이 경우, 평문과 암호문간 다음의 선형 근사식이 성립한다.

$$P_H[7, 18, 24] \oplus P_L[12, 16] \oplus C_H[15] \oplus C_H[7, 18, 24, 27, 28, 29, 30, 31] = K_1[19, 23] \oplus K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \oplus K_8[44] \oplus K_9[22] \oplus K_{11}[22] \oplus K_{12}[44] \oplus K_{13}[22] \oplus K_{15}[22] \oplus K_{16}[42, 43, 45, 46] \quad (18)$$

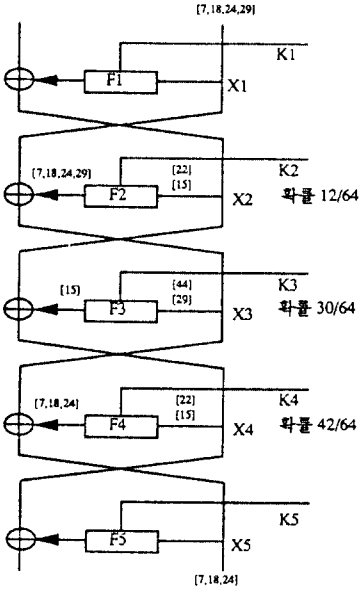

그림 5. 5단 DES의 근사

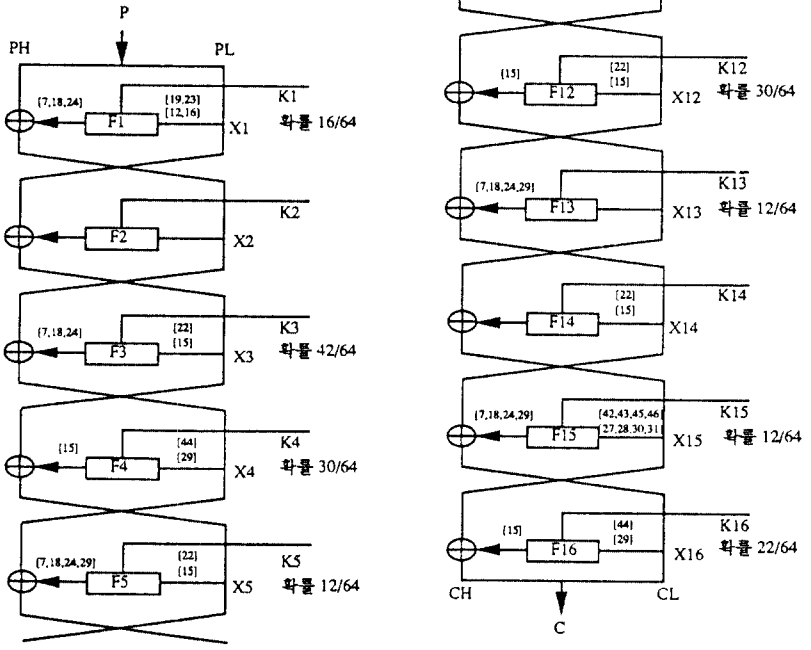

그림 6. 16단 DES의 최량표현

이 식은 제 1 단에는 $NS_5(34, 14)=16$에서 유도한 선형 근사식을 이용하고 제 3-5, 7-9, 11-13단에는 식(17), 또한, 15, 16단은 각각 식(4)와 (10)을 이용한 것이다.

$$X[7, 18, 24] \oplus F(X, K)[12, 16] = K[19, 23] \quad (19)$$

이 때, 식(18)의 성립 확률은 Piling-up Lemma에 의해

$$2^{11}(-20/64)^4(-10/64)(-2/64)^3(10/64)^3(-16/64)+1/2=-2^{23.5}+1/2$$

이고, 보조정리 2에 의해 2^{47}개의 기지 평문이 있으면, 식의 우변을 추정 가능하게 된다. 이것은 키의 전수 탐색 보다는 좋으며, 다음 절에 키의 효과적인 도출법을 설명한다.

5.4. 최량 표현의 계산

전술한 바의 3단, 5단, 16단 DES 암호의 근사식은 각 단에서 최량표현임을 증명 가능하다. 이 증명에는 약간의 이론적 고찰과 컴퓨터 시뮬레이션에 의해 가능하다(상세한 내용은 생략). 부록 B는 20단까지의 DES 암호에 있어서 최량 표현과 최량 확률을 나타내었으며 표에서 1열은 단수, 2열은 평문과 암호문을 연결하는 최량 표현, 3열은 그 성립 확률, 4열은 최량 표현을 구성하기 위한 필요 각단수로 F 함수의 근사식을 1단에서 부터 나타낸 것이다. 여기서, -의 기호로 표시한 단은 근사를 하지 않은 것을 나타내며 표에서 사용되는 기호는 밑에 기술하였다.

특히, 평문과 암호문의 대칭성에 의해 또다른 최량 표현을 찾을 수 있다(예를들면, P, C 및 K_i와 K_{n+1-i}를 서로 바꾸어서도 가능함). 이와 같은 방법으로 최량 표현이 2개를 얻을 수 있는 경우에는 부록의 표에는 *로 나타내었다. 또한, 표에 서술한 것이 각 단에서 구성 할 수 있는 최량 표현의 전부이다.

그러나, 이 선형 근사식은 모두 각단에 있어서 S-box를 1개만을 근사하여 얻은 것으로 일반적으로 1단에 2개 이상의 S-box를 근사하는 것도 가능하다. 이 경우 다음에 표시한 바와 같이 의미있는 관계식을 유도할 수 있다.

$$X[3,4] \oplus F(X, K)[0,10,20,25]=K[6,7] \quad (20)$$

$$X[3,4] \oplus F(X, K)[5,11,27]=K[4,5] \quad (21)$$

위의 관계식은 각각 $NS_7(3, 15)=40$ 및 $NS_8(48, 13)=20$을 이용하여 유도한 것으로 X 항이 공통으로 사용되었으므로 이를 삭제하면 확률 $2(8/64)(-12/64)+1/2=0.453$으로 성립하고 X를 포함하지 않는 다음의 근사식을 구할 수 있다.

$$F(X, K)[0, 5, 10, 11, 20, 25, 27] = K[4, 5, 6, 7] \quad (22)$$

이것은 F 함수에 랜덤한 입력이 주어졌을 때를 가정하고 그 출력만으로 키 $K[4, 5, 6, 7]$을 추정 가능하다는 의미이다. 보조정리 2에 의해 이 추정은 $1/(0.5-0.453)^2=450$개 정도의 입력으로 거의 틀림없이 성공한다.

이것은 F 함수가 확대 전치(E)를 갖고 있어, 키를 고정해도 단사가 되지 않음에서 기인한 것으로 이와 같은 관계식은 본질적으로 8개가 존재하고 따라서 키의 8비트를 구할 수 있다. 식(22)는 이관계 식으로 부터 얻은 최량의 성공 확률을 갖는 것이다.

또한, 식(22)을 2단 겹쳐서 임의 단의 DES의 선형 근사식을 구성하는 것도 가능하나, 간단한 계산 결과 부록 B 보다 유의성이 낮은 것을 확인하였다.

6. DES의 기지평문공격

6.1. 8단 DES

전술한 방법에 의해 일반적으로 DES의 암호화 키 중 1비트를 구할 수 있으나, 여기서는 8단 DES에서 모든 키비트를 보다 효율적으로 구할 수 있는 방법을 서술한다.

이를 위해 최초로 8단 DES 암호를 7단의 최량 표현을 이용하여 근사시켜 본다. 즉, 8단은 K_8에 의해 복호된다는 점을 이용하여 7단의 암호로 보고 이것을 부록 B를 이용한 최량 표현으로 근사시키는 것이 가능하다(그림 7). 이 결과, 확률 $1/2+1.95\times2^{-10}$으로 성립하는 다음의 관계식을 구할 수 있다.

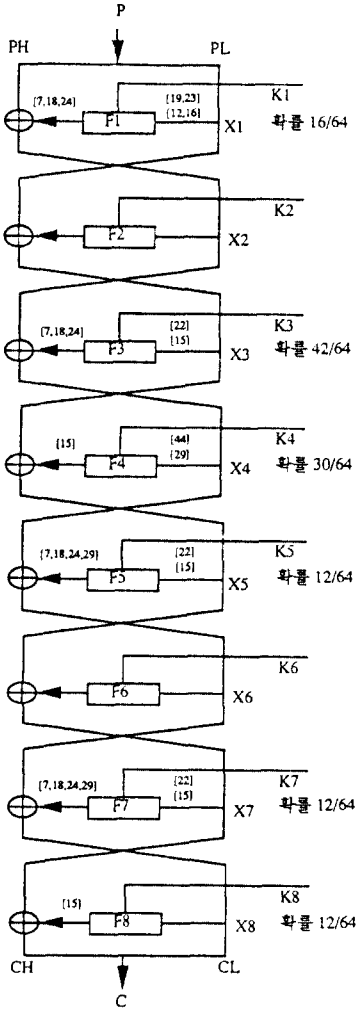

그림 7. 8단 DES의 기지평문공격(1)

$$P_H[7,\ 18,\ 24] \oplus P_L[12,\ 16] \oplus C_H[15] \oplus C_L[7,\ 18,\ 24,\ 29] \oplus F_8(C_L,\ K_8)[15] = K_1[19,\ 23] \oplus K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \quad (23)$$

여기서 $F_8(C_L, K_8)$에 영향을 주는 입력 정보는 S-box S_1에의 입력 정보 즉, $K_8[42]$~$K_8[47]$과 $C_L[26]$~$C_L[31]$뿐이다. 따라서 식 (23)의 성립 확률은 영향을 주는 키 비트 $K_8[42]$~$K_8[47]$과 식 (23)의 우변의 1 비트로 합계 7비트이다. $K_8[42]$~$K_8[47]$ 중 1비트라도 틀린 값을 식(23)에 삽입하면 그 유의성이 상실된다.

그리하여 $K_8[42]$~$K_8[47]$에 대응하는 2^6개의 카운터를 이용하여 Algorithm 2를 실행하면 이 7비트를 추정하는 것이 가능하지만, 이 경우 Algorithm 2를 다음과 같이 고속화가 가능하다.

[**Algorithm 2**(고속판)]

step 1 : $P_H[7,\ 18,\ 24] \oplus P_L[12,\ 16] \oplus C_H[15] \oplus C_L[7,\ 18,\ 24,\ 29]$ 및 $C_L[26]$에서 $C_L[31]$까지 합계 7비트 정보에 대응하는 2^7개의 카운터를 준비하고 초기화한다.

step 2 : 주어진 각 기지 평문과 암호문의 쌍에 대해 **Step 1**에 대응하는 카운터의 값에 1을 증가시킨다.

step 3 : K_8의 (64개중) 각 후보 k에 대하여 식 (23)의 좌변을 0으로 하는 **Step 1**의 7비트 정보에 대응하는 카운터 값의 합계를 T_k로 한다.

step 4 : 64개의 T_k의 최대값을 T_{max}, 최소값을 T_{min}로 하고 기지 평문 수 N에 대하여

- $|T_{max}-N/2| > |T_{min}-N/2|$ 이면 T_{max}에 대응하는 $K_8[42]$~$K_8[47]$를 채택하고 식 (23)의 우변은 0으로 추정한다.
- $|T_{max}-N/2| < |T_{min}-N/2|$ 이면 T_{min}에 대응하는 $K_8[42]$~$K_8[47]$를 채택하고 식 (23)의 우변은 1로 추정한다.

이 알고리즘의 연산 시간은 **Step 2**에만 의존하고 그 계산량은 XOR 연산 $9N$회, 카운터 증가 N회이다. 실행에 필요한 메모리는 무시될 정도로 작다.

다음은, **Algorithm 2**의 해독 성공 확률은 다음과 같이 일반적으로 평가한다. 우선 식(2)에 있어서 임의의 K에 대해서 다음의 식이 성리하는 K와 K'은 동치라 부른다.

$$F(X,\ K)[l_1,\ l_2,\ \cdots,\ l_d] = F(X,\ K')[l_1,\ l_2,\ \cdots,\ l_d] \quad (24)$$

이식은 확실한 동치 관계이며, 여기서 동치류의 대표원소의 집합을 K_1, K_2, …로 놓고 옳바른 K에 대하여 $F(X, K)[l_1, l_2, \cdots, l_d] = F(X, K_i)[l_1, l_2, \cdots, l_d]$가 성립하는 확률을 q_i로 한다. 이것은 동치류의 대표

원소의 값에 의존하지 않는 값으로 K와 K_i가 동일한 class에 속한다면, q_i=1이다. 따라서, 이 방법은 **Algorithm 2**를 정확하고 옳바른 K를 포함한 동치류 및 식(2)의 우변을 결정하는 방법이라고 말할 수 있다.

이상의 결과로 보조정리 2를 일반화하여 다음의 사실을 알 수 있으며 증명은 보조정리 2와 같이 이항 분포를 정규 분포로 근사시킴으로서 가능하다.

보조정리 4 N개의 랜덤한 기지 평문을 이용하여 **Algorithm 2**를 실행 할 때, 그 해독 성공 확률(키 K의 동치류와 식(2)의 우변을 바르게 추정할 확률)은 적어도 다음의 식으로 주어진 값의 이상이다.

$$\int_{x=-2\sqrt{N}|p-1/2|}^{\infty} \left(\prod_{K_i=K} E_i(x)\right) \frac{2}{\sqrt{\pi}} e^{-x^2/2} dx \quad (25)$$

여기서, $\prod$는 K를 포함하지 않는 모든 동치류의 대표 원소에 대한 것으로, $E_i(x)$는 다음의 식으로 정의되는 함수이다.

$$E_i(x)=\int_{-x-4\sqrt{N(p-1/2)q_i}}^{x+4\sqrt{N(p-1/2)(1-q_i)}} \frac{2}{\sqrt{\pi}} e^{-y^2/2} dy \quad (26)$$

그러면, 식(23)을 여기에 적용하면, 이 경우 K_8의 후보의 동치류는 43번째부터 48번째까지 6비트에 대응하는 64가지를 대표하고, q_i는 임의로 주어진 X에 대하여 다음 식이 성공할 확률이다.

$$F(X, K_8)[15]=F(X, K_i)[15] \quad (27)$$

여기서 각 q_i의 값은 K_8에 의존하지만, 그 분포는 K_8에 의존하지 않는다는 점을 주의하자. 실제 간단한 수치 계산에 의해 q_i의 분포는 표 2와 같으며,

표 2. 식 (27)의 성립 확률의 분포

q_i	$\frac{64}{64}$	$\frac{44}{64}$	$\frac{40}{64}$	$\frac{36}{64}$	$\frac{32}{64}$	$\frac{28}{64}$	$\frac{24}{64}$	$\frac{20}{64}$
i의 갯수	1	2	6	12	17	16	8	2

이것을 이용하여 식(25)의 계산치는 표 3과 같다.

이 경우 $8|p-1/2|^{-2}=8|1.95\times2^{-10}|^{-2}=1.05\times2^{21}$이므로 약 2^{21}개의 평문이 있으면 Algorithm 2에 의해 해독은 대부분의 경우 가능하다고 예상된다.

표 3. 식 (25)의 계산치

N	식(25)의 계산치
$4|p-1/2|^{-2}$	0.77
$8|p-1/2|^{-2}$	0.96
$16|p-1/2|^{-2}$	1.00

이것을 확인하기 위해 컴퓨터로 7비트의 해독 실험을 한 결과가 표 4와 같다.

표 4. 7비트의 해독 성공 확률

평문의 수	식(25)의 계산치	성공률의 실험치
2^{20}	77%	88%
2^{21}	96%	99%
2^{22}	100%	100%

이 결과는 성공률의 실험치가 식(25)의 계산치보다 좋다는 것을 나타낸다(실험치가 계산치 보다 확률이 높은 것은 일반적으로 각 K의 후보에 대응하는 식(2)의 성립 확률이 서로 독립적이 아님에 기인한다). 결국 $8|p-1/2|^{-2}$개의 평문이 주어진다면 거의 틀림없이 7비트의 해독에 성공한다는 것을 알 수 있다.

그러면, 이상의 방법은 최종단의 키를 도출하는데 있으며 평문과 암호문의 관계를 서로 교환하여도 같은 방법으로 제 1 단의 키를 구할 수도 있다. 즉, 제 2 단 이후 7단까지의 최량 근사식을 선형 근사한 다음의 관계식을 이용하는 것이다.

$$\begin{aligned} &P_H[15] \oplus P_L[7, 18, 24, 29] \oplus C_H[7, 18, 24] \\ &\oplus C_L[12, 16] \oplus F_1(P_L, K_1)[15] \\ &=K_2[22] \oplus K_4[22] \oplus K_5[44] \oplus K_6[22] \\ &\oplus K_8[19, 23] \end{aligned} \quad (28)$$

위식의 성립 확률은 식 (23)과 동일하며 이식으로 K_1의 제 43~48 비트 및 식(28)의 우변의 1비트를 결정할 수 있다. 이 해독 과정은 최초의 7비트의 도출과 병렬로 실행할 수 있으므로 라운드키 중 14비트는 메모리의 사용없이 구할 수 있다. 이 14비트는 라운드키 발생부를 고려하면 암호화키의 56비트 중 다음의 12비트에 상당한다(이하 암호화키 56 비트는 PC-1을 통과 한 후의 키 정보를 의미함).

$$28, 31, 37, 38, 41, 44, 46, 50, 53, 54,$$
$$0 \oplus 8 \oplus 14 \oplus 20 \oplus 24,$$
$$1 \oplus 2 \oplus 22 \oplus 23 \oplus 26 \oplus 52$$

이어서 라운드키를 구하기 위하여, 이번에는 제 2 단부터 제 7 단까지의 F 함수만을 선형 근사를 위하여 다음의 관계식을 이용한다. 이식은 제 1 단과 제 8 단이 각각 K_1 및 K_8을 이용하여 암호화, 복호화한 것으로 보고 6단 근사를 한 결과이다(그림 8).

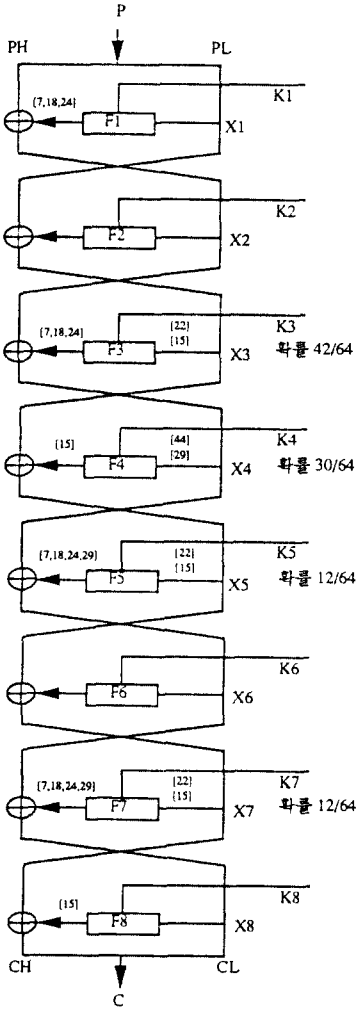

그림 8. 8단 DES의 기지평문공격(2)

$$P_H[7, 18, 24] \oplus F_1(P_L, K_1)[7, 18, 24] \oplus C_H[15] \oplus C_L[7, 18, 24, 29] \oplus F_8(C_L, K_8)[15] = K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \quad (29)$$

이식의 성립 확률은 Piling-up Lemma에 의해 $1/2-1.95\times2^{-9}$임을 알 수 있다. 이식에는 F 함수가 2개가 있으므로 그중 $F_8(C_L, K_8)$은 해독자에게 이미 알려진 값으로 미지수는 $F_1(P_L, K_1)[7, 18, 24]$에 영향을 주는 키 비트, 즉, S-box S_5에의 입력인 K_1의 18 비트부터 23 비트까지의 6비트이다. 재차 **Algorithm 2**에 의해 6비트와 식(29)의 우변 1 비트해서 합계 7비트를 도출할 수 있다.

식(29)에 있어서 평문과 암호문의 관계를 서로 바꾸어 다음의 관계식도 확률 $1/2-1.95\times2^{-9}$로 성립하므로 이것에서 K_8의 제 18~23 비트까지의 6비트 및 우변의 1비트, 전부 7비트를 구할 수 있다. 식(29)와 (30)을 풀기 위하여는 필요한 기지 평문 수는 최초의 1/4정도라도 좋다.

$$P_H[15] \oplus P_L[7, 18, 24, 29] \oplus F_1(P_L, K_1)[15] \oplus C_H[7, 18, 24] \oplus F_8(C_L, K_8)[7, 18, 24] = K_2[22] \oplus K_4[22] \oplus K_5[44] \oplus K_6[22] \quad (30)$$

이상으로 라운드키 28 비트를 구하는데 성공했다. 이것에서 라운드키 발생부를 고려하면 암호화 키 56 비트 중 다음의 23 비트에 해당한다(5비트는 중복해서 구하는 것이 가능).

$$0, 1, 3, 5, 8, 11, 14, 15, 18, 20, 23, 24$$
$$28, 31, 37, 38, 41, 44, 46, 50, 53, 54,$$
$$2 \oplus 22 \oplus 26 \oplus 52$$

위와 같이하여 라운드키를 순서로 구할 수 있으나 상세한 내용은 생략한다. 마지막으로 8단 DES를 컴퓨터에 의한 해독 결과를 정리한다. 실험 방법은 랜덤하게 발생한 평문과 대응하는 암호문의 쌍으로

표 5. 8단 DES의 해독 실험 결과

기지 평문의 수	해독 성공률(%)	해독 시간(초)
2^{20}	53	20
2^{21}	98	40
2^{22}	100	80

부터 암호화 키 56비트를 전부 추정한 결과로 그 성공 확률과 해독 시간의 실험치는 표 5와 같다.

6.2. 12단 DES

12단 DES의 기지 평문 공격에 의한 해독은 8단의 경우와 동일하게 실행 가능하다. 즉, 11단의 최량표현을 이용하여 다음의 관계식을 이용한다 (그림 9).

$$P_H[7, 18, 24, 29] \oplus P_L[15] \oplus C_H[15]$$

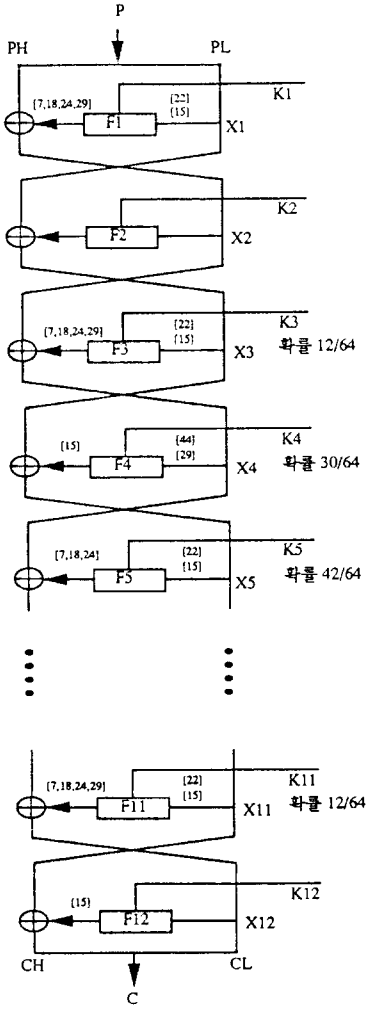

그림 9. 12단 DES의 기지평문공격

$$\oplus C_L[7, 18, 24, 29] \oplus F_{12}(C_L, K_{12})[15]$$
$$= K_1[22] \oplus K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \oplus K_8[44] \oplus K_9[22] \oplus K_{11}[22] \quad (31)$$

위 식의 성립 확률은 $1/2+1.91\times2^{-16}$이고 표 4의 결과에 의해 $8\,|\,1.91\times2^{-16}|^{-2}=1.10\times2^{33}$개의 기지 평문이 있으면, K_{12}의 제 42 부터 47 비트까지의 6 비트 및 식(31)의 우변의 1비트로 7비트를 구하는 것이 가능하다.

같은 방법으로, 제 2 단 이후의 11단을 근사하여 다음의 관계식을 구하여 여기에서 K_1의 제 42 부터 47비트까지의 6비트와 우변의 1비트를 도출한다.

$$P_H[15] \oplus P_L[7, 18, 24, 29] \oplus F_1(P_L, K_1)[15] \oplus C_H[7, 18, 24, 29] \oplus C_L[15]$$
$$= K_2[22] \oplus K_4[22] \oplus K_5[44] \oplus K_6[22] \oplus K_8[22] \oplus K_9[44] \oplus K_{10}[22] \oplus K_{12}[22] \quad (32)$$

식(29)와 (30)에 대응하는 관계식은 각각 다음과 같이 표현된다. 이 등식의 성립 확률은 $1/2-1.53\times2^{-15}$이고 여기서 K_1, K_8의 제 18에서 23비트까지의 6비트와 각식의 우변의 1비트가 도출된다.

$$P_H[7, 18, 24, 29] \oplus F_1(P_L, K_1)[7, 18, 24, 29] \oplus C_H[15] \oplus C_L[7, 18, 24, 29] \oplus F_{12}(C_L, K_{12})[15]$$
$$= K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \oplus K_8[44] \oplus K_9[22] \oplus K_{11}[22] \quad (33)$$

$$P_H[15] \oplus P_L[7, 18, 24, 29] \oplus F_1(P_L, K_1)[15] \oplus C_H[7, 18, 24, 29] \oplus F_{12}(C_L, K_{12})[7, 18, 24, 29]$$
$$= K_2[22] \oplus K_4[22] \oplus K_5[44] \oplus K_6[22] \oplus K_8[22] \oplus K_9[44] \oplus K_{10}[22] \quad (34)$$

이상으로 라운드키의 28비트를 구하였으며 이 비트는 라운드키 발생부를 고려하면 암호화키 56 비트 중 25 비트에 해당된다(3비트는 중복하여 구해진다). 나머지의 31 비트는 동일한 방법으로 또는 전수 검사에 의하여 구할 수 있다.

컴퓨터 실험 결과 랜덤하게 발생한 2^{33}개의 기지 평문을 이용하여 50시간에 암호화 키 56 비트를 구하는데 성공하였다.

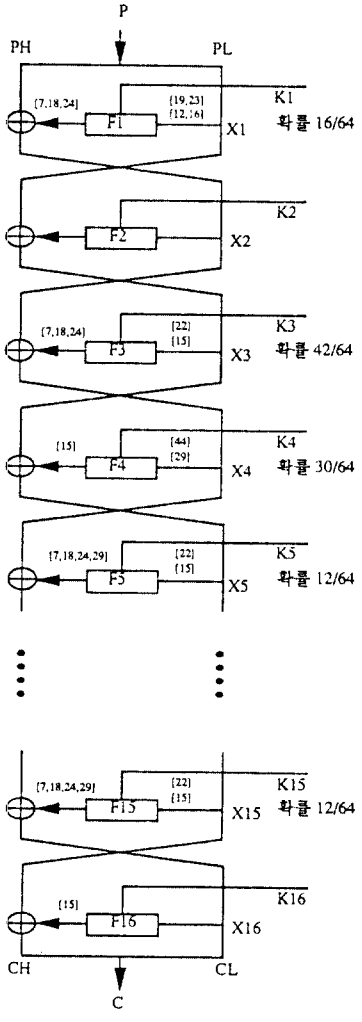

그림 10. 16단 DES의 기지평문공격

6.3. 16단 DES

표준 규격인 16단 DES의 기지 평문 공격도 8단 및 12단의 경우와 동일하게 실행 가능하다. 즉, 15단의 최량 표현에서 도출한 다음의 2개의 선형 근사식을 이용하여 라운드키 14 비트가 구해진다 (그림 10).

$$P_H[7,\ 18,\ 24] \oplus P_L[12,\ 16] \oplus C_H[15] \oplus C_L[7,\ 18,\ 24,\ 29] \oplus F_{16}(C_L,\ K_{16})[15] = K_1[19,\ 23] \oplus K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \oplus K_8[44] \oplus K_9[22] \oplus K_{11}[22] \oplus K_{12}[44] \oplus K_{13}[22] \oplus K_{15}[22] \quad (33)$$

$$P_H[15] \oplus P_L[7,\ 18,\ 24,\ 29] \oplus C_H[7,18,24] \oplus C_L[12,\ 16] \oplus F_1(P_L,\ K_1)[15] = K_2[22] \oplus K_4[22] \oplus K_5[44] \oplus K_6[22] K_8[22] \oplus K_9[44] \oplus K_{10}[22] \oplus K_{12}[22] \oplus K_{13}[44] \oplus K_{14}[22] \oplus K_{16}[19,\ 23] \quad (36)$$

위 두 식의 성립 확률은 $1/2+1.19\times2^{-22}$이고 표 3의 결과에 의해 $8\,|\,1.19\times2^{-22}\,|^{-2}=1.41\times2^{46}$개의 기지 평문이 주어지면 메모리를 사용치 않고 K_1 및 K_{16}의 제 42 에서 47비트까지 각 6비트와 식(35)와 (36)의 우변 1 비트를 높은 확률로 구할 수 있다. 이 14 비트는 암호화키 56 비트 중 다음의 14 비트이다.

31, 32, 38, 39, 41, 42, 44, 45, 50, 51, 54, 55
$0 \oplus 5 \oplus 8 \oplus 9 \oplus 13 \oplus 14 \oplus 17 \oplus 20 \oplus 24 \oplus 46$,
$2 \oplus 7 \oplus 9 \oplus 11 \oplus 18 \oplus 22 \oplus 26 \oplus 37 \oplus 52$

지금의 경우 계산량은 $N=1.41\times2^{46}$이라 할 때 비트 XOR 연산 $18N$회, 카운터 값의 증가 횟수 $2N$회이다. 나머지 42비트의 미지의 키는 전수 검사에 의해 구하여도 좋고 식(33)과 (34)에 대응되는 식을 풀어서 미지의 키 비트를 감소시켜도 좋을 것이다.

이 경우, 식(33)과 (34)에 대응하는 식의 성립 확률은 $1/2-1.19\times2^{-21}$이므로 해독에 필요한 평문의 수는 $N/4$이다. 또한, 이 결과 얻어지는 암호화 키 비트를 합계하면 다음의 26 비트가 된다.

0, 1, 3, 4, 8, 9, 14, 15, 18, 19, 24, 25
31, 32, 38, 39, 41, 42, 44, 45, 50, 51, 54, 55
$5 \oplus 13 \oplus 17 \oplus 20 \oplus 46$,
$2 \oplus 7 \oplus 11 \oplus 22 \oplus 26 \oplus 37 \oplus 52$

결국 $N+N/4=1.76\times2^{46}$개의 기지 평문이 있으면, 무시할 정도의 메모리 량으로 키의 26 비트를 구하는 것이 가능하다. 나머지의 미지 키 30 비트는 이제는 전수 검사가 용이하다.

7. 결 론

본고에서는 DES 형태의 암호 방식의 새로운 해독법으로서 선형 해독법을 제안하고 이것을 이용하여 DES 암호의 기지 평문 공격을 행하였으며 이는 전수 검색법 보다 빠른 기지평문 공격으로서는 최초의 결과이다.

본 방식에서는 암호 알고리즘의 비트 단위로 선형 근사하는 것으로 마쓰이가 이미 FEAL 암호의 기지 평문 공격에 의한 해독법을 보다 일반화한 것이다.

또한, 이 해독법은 블럭 암호에 대하여 범용적인 암호문 단독 공격법을 처음으로 제시한 결과이다. 이 결과 16단의 DES 암호에 대하여 전수 탐색법 보다 고속인 COA가 가능한 상황이 존재하는 것을 제시하는 것도 가능하며 COA에 대하여 상세한 내용은 본 해설의 2부에 소개한다.

참 고 문 헌

1. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", J. of Cryptology, Vol.4, pp.3-72, 1991.

2. E. Biham and A. Shamir, "Differential Cryptanaylsis of FEAL and N-Hash", Advances in Cryptology-Eurocrypt'91, Lecture Notes in Computer Science, Vol.547, pp.1-16, 1991.

3. E. Biham and A. Shamir, "Differential Cryptanaylsis of the full 16-round DES", Crypto'92 Extended Abstracts, pp.12.1-12.5, 1992.

4. A. Tardy-Corfdir and H. Gilbert, "A Known Plaintext Attack of FEAL-4 and FEAL-6", Advances in Cryptology-Crypto'91, Lecture Notes in Computer Science, Vol.576, pp.172-182, 1991.

5. M. Matsui and A. Yamagishi, "A New Method for Known Plaintext Attack of FEAL Cipher", Eurocrypt'92 Extended Abstracts, pp. 77-87, 1992.

6. M. Matsui, "Linear Cryptanalysis of DES Cipher(II)", to appear.

□ 著者紹介

金 光 兆(正會員)

1980年 延世大學校 電子工學科(學士)
1983年 延世大學校 大學院 電子工學科(碩士)
1990年 요꼬하마 國立大學 大學院 電子情報工學科(博士)
現 在 : 韓國電子通信研究所 室長

關心分野 : 暗號學 및 應用分野, M/W通信

부록 A : $S_5(i, j)-32$

Sbox5	(j)1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
(i) 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	4	−2	2	−2	2	−4	0	4	0	2	−2	2	−2	0	−4
3	0	−2	6	−2	−2	4	−4	0	0	−2	6	−2	−2	4	−4
4	2	−2	0	0	2	−2	0	0	2	2	4	−4	−2	−2	0
5	2	2	−4	0	10	−6	−4	0	2	−10	0	4	−2	2	4
6	−2	−4	−6	−2	−4	2	0	0	−2	0	−2	−6	−8	−2	0
7	2	0	2	−2	8	6	0	−4	6	0	−6	−2	0	−6	−4
8	0	2	6	0	0	−2	−6	−2	2	4	−12	2	6	−4	4
9	−4	6	−2	0	−4	−6	−6	6	−2	0	−4	2	−6	−8	−4
10	4	0	0	−2	−6	2	2	2	2	−2	2	4	−4	−4	0
11	4	4	4	6	2	−2	−2	−2	−2	−2	2	0	−8	−4	0
12	2	0	−2	0	2	4	10	−2	4	2	−8	−2	4	−6	−4
13	6	0	2	0	−2	4	−10	−2	0	−2	4	−2	8	6	0
14	−2	−2	0	−2	4	0	2	−2	0	4	2	−4	6	−2	−4
15	−2	−2	8	6	4	0	2	2	4	8	−2	8	−6	2	0
16	2	−2	0	0	−2	−6	−8	0	−2	−2	−4	0	2	10	−20
17	2	−2	0	4	2	−2	−4	4	2	2	0	−8	−6	2	4
18	−2	0	−2	2	−4	−2	−8	4	6	4	6	−2	4	−6	0
19	−6	0	2	−2	4	2	0	4	−6	4	2	−6	4	−2	0
20	4	−4	0	0	0	0	0	−4	−4	4	4	0	4	−4	0
21	4	0	−4	−4	4	−8	−8	0	0	−4	4	8	4	0	4
22	0	6	6	2	−2	4	0	4	0	6	2	2	2	0	0
23	4	−6	−2	6	−2	−4	4	4	−4	−6	2	−2	2	0	4
24	6	0	2	4	−10	−4	2	2	0	−2	0	2	4	−2	−4
25	2	4	−6	0	−2	4	−2	6	8	6	4	10	0	2	−4
26	2	2	−8	−2	4	0	2	−2	0	4	2	0	−2	−2	0
27	2	6	−4	−6	0	0	2	6	8	0	−2	−4	−6	−2	0
28	0	−2	2	4	0	−6	2	−2	6	−4	0	2	−2	0	0
29	4	−2	6	−8	0	−2	2	10	−2	−8	−8	2	2	0	4
30	−4	−8	0	−2	−2	−2	2	−2	2	−2	6	4	4	4	0
31	−4	8	−8	2	−6	−6	−2	−2	2	−2	−2	−8	0	0	−4
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	−4	−2	2	−2	2	−4	8	−4	0	−6	6	2	−2	−16	−12
35	0	−2	−2	6	−2	−4	4	0	0	−2	−2	−2	6	4	−4
36	−2	6	4	0	6	−2	4	4	−6	−2	4	0	14	2	0
37	6	2	0	0	6	2	0	−4	−6	2	−8	0	−2	6	−4
38	2	4	−2	−2	0	2	−4	4	−2	−4	−2	6	0	−2	0
39	−10	0	−2	6	4	6	−4	0	6	−12	2	2	0	6	−4
40	4	−2	−2	0	4	−6	2	2	−6	4	0	6	−2	−4	0
41	0	2	6	0	0	6	2	2	−2	−8	0	−2	−6	0	0
42	0	−4	−8	6	6	6	−6	6	2	−2	−2	−8	4	−4	4
43	8	0	4	6	−2	−6	6	2	6	−2	6	−4	0	4	4
44	2	4	−6	0	−6	0	6	−2	−4	2	4	−2	4	6	0
45	−2	−4	−2	0	−2	−8	2	−2	0	−6	−8	−2	0	−2	4
46	6	2	−4	6	4	4	−2	−10	−8	0	−2	4	−2	2	0
47	6	−6	−4	6	−4	4	−2	2	4	4	−6	0	2	−2	−4
48	2	−2	0	−4	−6	2	−4	4	2	2	0	0	2	2	4
49	2	−2	0	0	−2	2	0	0	−2	−2	−4	0	2	2	4
50	6	0	−2	−2	8	2	4	0	10	0	2	−2	4	2	0
51	−6	0	10	2	0	−2	−4	0	6	0	−10	2	4	−2	0
52	0	−12	4	−4	0	4	−8	−4	0	−4	0	−4	−4	0	0
53	−8	0	0	8	−4	4	0	0	−4	−4	0	4	4	−4	4
54	4	−2	−6	−2	−2	8	0	4	−4	−2	−2	6	2	−4	0
55	−8	−6	−6	−6	6	0	4	12	0	2	−2	2	2	4	−4
56	2	4	−6	0	−2	4	−2	−6	4	−6	0	6	4	−2	0
57	−2	8	2	−4	6	−4	−6	−2	−4	2	4	−2	0	2	0
58	6	−10	0	2	4	0	−2	6	−4	0	2	4	−2	−2	−4
59	−2	−6	−4	−10	0	−8	−2	−10	4	4	−2	0	2	−2	4
60	−8	−6	−2	0	−4	2	2	−6	2	4	0	10	−2	4	4
61	4	2	2	4	4	−2	2	−2	10	0	0	2	2	4	0
62	−4	4	−4	2	2	−2	2	2	−2	−2	−2	4	−4	0	4
63	−4	−4	−4	14	6	−6	−2	2	−2	6	−2	0	0	−4	0

부록 B : DES의 최량 표현과 최량 확률

*2	$P_L[\alpha] \oplus C_H[\alpha] \oplus C_L[15]$ $=K_2[22]$	$1/2-1.25\times2^{-2}$	-A
3	$P_H[\alpha] \oplus P_L[15] \oplus C_H[\alpha] \oplus C_L[15]$ $=K_1[22] \oplus K_3[22]$	$1/2+1.56\times2^{-3}$	A-A
*4	$P_H[\alpha] \oplus P_L[15] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $=K_1[22] \oplus K_3[22] \oplus K_4[\gamma]$	$1/2-1.95\times2^{-5}$	A-AB
5	$P_H[15] \oplus P_L[\alpha, \beta] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $=K_1[\gamma] \oplus K_2[22] \oplus K_4[22] \oplus K_5[\gamma]$	$1/2+1.22\times2^{-6}$	BA-AB
*6	$P_L[\delta] \oplus C_H[\alpha] \oplus C_L[15]$ $=L_2 \oplus K_6[15]$	$1/2-1.95\times2^{-9}$	-DCA-A
*7	$P_H[\delta] \oplus P_L[12, 16] \oplus C_H[\alpha] \oplus C_L[15]$ $=K_1[19, 23] \oplus L_3 \oplus K_7[22]$	$1/2+1.95\times2^{-10}$	E-DCA-A
*8	$P_H[\delta] \oplus P_L[12, 16] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $=K_1[19, 23] \oplus L_3 \oplus K_7[22] \oplus K_8[\gamma]$	$1/2-1.22\times2^{-11}$	E-DCA-AB
*9	$P_H[15] \oplus P_L[\beta, \delta] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $=K_1[\gamma] \oplus K_2[22] \oplus L_4 \oplus K_8[22] \oplus K_9[\gamma]$	$1/2-1.91\times2^{-14}$	BD-DCA-AB
*10	$P_L[\alpha] \oplus C_H[\alpha] \oplus C_L[15]$ $=L_2 \oplus L_6 \oplus K_{10}[22]$	$1/2-1.53\times2^{-15}$	-ACD-DCA-A
11	$P_H[\alpha] \oplus P_L[15] \oplus C_H[\alpha] \oplus C_L[15]$ $=K_{11}[22] \oplus L_3 \oplus L_7 \oplus K_{11}[22]$	$1/2+1.91\times2^{-16}$	A-ACD-DCA-A
*12	$P_H[\alpha] \oplus P_L[15] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $=K_1[22] \oplus L_3 \oplus L_7 \oplus K_{11}[22] \oplus K_{12}[\gamma]$	$1/2-1.19\times2^{-17}$	A-ACD-DCA-AB
13	$P_H[15] \oplus P_L[\alpha, \beta] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $=K_1[\gamma] \oplus L_2[22] \oplus L_4 \oplus L_8 \oplus K_{12}[22] \oplus K_{13}[\gamma]$	$1/2+1.49\times2^{-19}$	BA-ACD-DCA-AB
*14	$P_L[\beta] \oplus C_H[\alpha] \oplus C_L[15]$ $=L_2 \oplus L_6 \oplus K_{10} \oplus K_{14}[22]$	$1/2-1.19\times2^{-21}$	-DCA-ACD-DCA-A
*15	$P_H[\delta] \oplus P_L[12, 16] \oplus C_H[\alpha] \oplus C_L[15]$ $=K_1[19, 23] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}[22]$	$1/2+1.19\times2^{-22}$	E-DCA-ACD-DCA-A
*16	$P_H[\delta] \oplus P_L[12, 16] \oplus C_H[15] \oplus C_L[\alpha, \beta]$ $=K_1[19, 23] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}[22] \oplus K_{16}[\gamma]$	$1/2-1.49\times2^{-24}$	E-DCA-ACD-DCA-AB
*17	$P_H[15] \oplus P_L[\beta, \delta] \oplus C_H[15] \oplus C_L[\alpha, \delta]$ $=K_1[\gamma] \oplus K_2[22] \oplus L_1 \oplus L_8 \oplus L_{12} \oplus K_{16}[22] \oplus K_{17}[\gamma]$	$1/2-1.16\times2^{-26}$	BD-DCA-ACD-DCA-AB
*18	$P_L[\alpha] \oplus C_H[\alpha] \oplus C_L[15]$ $=L_2 \oplus L_6 \oplus K_{10} \oplus K_{14} \oplus K_{18}[22]$	$1/2-1.86\times2^{-28}$	-ACD-DCA-ACD-DCA-A
19	$P_H[\alpha] \oplus P_L[15] \oplus C_H[\alpha] \oplus C_L[15]$ $=K_1[22] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus L_{15} \oplus K_{19}[22]$	$1/2+1.16\times2^{-28}$	A-ACD-DCA-ACD-DCA-A
*20	$P_H[\alpha] \oplus P_L[15] \oplus C_H[\alpha] \oplus C_L[\alpha, \beta]$ $=K_1[22] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus L_{15} \oplus K_{19}[22] \oplus K_{20}[\gamma]$	$1/2-1.46\times2^{-30}$	A-ACD-DCA-ACD-DCA-A

A : $X[15] \oplus F(X, K)[7, 18, 24, 29]=K[22]$ *Prob.* 0.189 α : 7, 18, 24, 29

B : $X[27, 28, 30, 31] \oplus F(X, K)[15]=K[42, 43, 45, 46]$ *Prob.* 0.344 β : 27, 28, 30, 31

C : $X[29] \oplus F(X, K)[15]=K[44]$ *Prob.* 0.469 γ : 42, 43, 45, 46

D : $X[15] \oplus F(X, K)[7, 8, 24]=K[22]$ *Prob.* 0.656 δ : 7, 18, 24

E : $X[12, 16] \oplus F(X, K)[7, 18, 24]=K[19, 23]$ *Prob.* 0.250 L_i : $K_i[22] \oplus K_{i+1}[44] \oplus K_{i+2}[22]$