通信情報保護學會誌
第3卷 第3號, 1993.9

DES의 선형근사

성 수 학*

요 약

DES를 linear 암호분석을 하기 위해서는 선형근사가 필요하다. 본 논문에서 우리는 선형근사의 성질과, 좋은 선형근사를 구성하기 위하여 반복가능한 선형근사를 연구한다.

1. 서 론

1993년 Matsui에 의해서 DES-like 반복 블럭 암호에 적용가능한 linear 암호 분석법이 제안되었다. 이 공격법은 DES에서 유일한 비선형 구조인 S-box를 적당히 선형화시켜 암호 분석하는 known plaintext attack으로 2^{21}개의 평문으로 8-라운드 DES를, 2^{47}개의 평문으로 16-라운드의 DES를 분석할 수 있다. Differential 암호분석과 유사하게 linear 암호 분석을 하기위해서는 확률이 최적인 선형근사가 필요하다.

본 논문에서 우리는 Matsui가 제안한 linear 암호분석법을 간단히 소개한다. 또한, linear 암호 분석법의 핵심인 선형근사의 성질과 반복 가능한 선형근사의 성질을 연구한다.

2. Linear 암호 분석

1993년 Matsui는 linear 암호 분석법으로 DES를 분석했다. Linear 암호 분석법은 DES에서 유일한 비선형 구조인 S-box를 적당히 선형화시켜 암호 분석하는 known plaintext 공격법으로 Biham과 Shamir가 제안한 chosen plaintext 공격법인 differential 암호분석 보다 좋은 방법이다.

Differential 암호 분석과 비슷하게 DES를 linear 암호 분석하기 위해서는 확률이 최적인 선형근사가 필요하다. 좋은 선형근사(선형근사의 확률이 0또는 1에 가까운 값을 가지는 선형근사)를 구하면 linear 암호 분석은 쉽지만, 반대로 좋은 선형근사를 구할 수 없으면 linear 암호분석은 어렵다.

본 논문에서는 DES의 초기치환과 역초기치환은 linear 암호 분석에 아무런 영향을 주지 않으므로 초기치환과 역초기치환이 없는 DES를 생각하기로 한다.

[정의] N-라운드 DES의 평문과 대응되는 암호문, 그리고 키가 확률 $p(p\neq 1/2)$로 아래의 선형 근사식을 만족할때 N-라운드 DES는 선형근사 되었다고 정의한다.

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

* 배재대학교 응용수학과 조교수

단, A[i]는 A의 i번지 비트값이고 $A[i,j,\cdots,k]$ = $=A[i]\oplus A[j]\oplus\cdots\oplus A[k]$이다. 선형근사의 확률 p가 0 또는 1에 가까운 값($|p-\frac{1}{2}|$ 이 최대)일때 최적의 선형근사라고 한다.

Linear 암호 분석에서 f함수의 입력번지, 출력번지, 그리고 키의 번지를 나타낼때 오른쪽 첫번째가 0번지이고 왼쪽으로 갈수록 번지가 증가한다.

N-라운드 DES의 선형근사를 구성하기 위해서 DES의 유일한 비선형 구조인 S-box를 선형화시킨다. S-box는 6개의 입력 비트와 4개의 출력 비트로 구성되어 있다. 몇 개의 입력 번지에 대응되는 입력 비트들의 XOR한 값을 몇 개의 출력 번지에 대응되는 출력 비트들의 XOR한 값으로 근사시킨다. 구체적인 정의는 아래와 같다.

[정의] S-box에 0부터 63까지의 입력 x를 작용하였을때, 입력과 출력 번지를 각각 나타내는 α와 β ($1\le\alpha\le63$, $1\le\beta\le15$, α를 이진수로 표현했을때 1 비트값이 나타나는 번지가 입력번지이다)에 대해서

$$NS(\alpha,\beta)=\#\{x\mid 0\le x\le63,\ \oplus_{s=0}^{5}(x[s]\cdot\alpha[s]) = \oplus_{t=0}^{3}(S(x)[t]\cdot\beta[t])\}$$

로 정의한다. 즉, NS는 S-box의 출력값의 XOR와 입력 값의 XOR가 같은 횟수를 나타낸다.

[예] α=33이면 입력번지는 0번지와 5번지이다. $x[0]\oplus x[5]=0$이면, S(x)는 {0, 1, ⋯, 15}상의 2개의 치환이 된다. 따라서, 임의의 β에 대해서 $\oplus_{t=0}^{3}(S(x)[t]\cdot\beta[t])=0$ 되는 가능성은 1/2이므로 그러한 x는 16개이다. 같은 방법으로, $x[0]\oplus x[5]=1$일때 $\oplus_{t=0}^{3}(S(x)[t]\cdot\beta[t])=1$되는 x의 갯수는 16개이다. 그러므로, $NS(33,\beta)=32$이다.

[정의] I를 f함수의 입력 X의 번지의 집합, A를 입력번지 I에 대응되는 키 K의 번지의 집합, 그리고 O를 f함수의 출력 f(X, K)의 번지의 집합일때

$$I\to O \quad \text{또는} \quad O\leftarrow I$$

로 나타낸다. 또, 입력 X가 랜덤할때 $X[I]\oplus K[A]=f(X,K)[O]$의 확률이 p이면 다음과 같이 쓴다.

$$I\to O \quad \text{확률 p 또는} \quad O\leftarrow I \text{ 확률 p}$$

특히, $I=\emptyset$(공집합)일때 $\emptyset\to\emptyset$ 확률 1로 쓴다.

S-box의 선형근사를 이용하여 f함수의 선형근사를 쉽게 얻을 수 있다. 예를들면, $NS_5(16,15)=12$이므로 16은 S_5의 입력 4번지, 15는 S_5의 출력 0, 1, 2, 3번지이다. S_5의 입력 4번지는 f함수의 입력 X의 15번지, X의 15번지에 대응되는 키 K의 번지는 22, 그리고 S_5의 출력 0, 1, 2, 3번지는 f함수의 출력 f(X, K)의 29, 7, 18, 24번지에 대응된다. 따라서, f함수의 입력 X가 랜덤할때 $X[15]\oplus K[22]=f(X,K)[7,18,24,29]$의 확률은 12/64이다. 즉, [15]→[7, 18, 24, 29](확률 12/64)이다.

f함수의 선형근사로 부터 N-라운드 DES의 선형근사를 구성할 수 있다. 선형근사의 확률을 계산하기 위해서 Piling-up Lemma가 필요하다.

보조정리(Piling-up Lemma) 독립인 확률변수 X_i ($1\le i\le n$)가 0을 취할 확률이 p_i, 1을 취할 확률이 $1-p_i$일때, $X_1\oplus X_2\oplus\cdots\oplus X_n=0$이 될 확률은 $2^{n-1}\prod_{i=1}^{n}(p_i-\frac{1}{2})+\frac{1}{2}$이다.

증명 : $p=P(X_1\oplus X_2\oplus\cdots\oplus X_{n-1}=0)$라고 두면,

$$\begin{aligned}&P(X_1\oplus X_2\oplus\cdots\oplus X_n=0)\\ &=P(X_1\oplus X_2\oplus\cdots\oplus X_{n-1}=0,\ X_n=0)\\ &\quad+P(X_1\oplus X_2\oplus\cdots\oplus X_{n-1}=1,\ X_n=1)\\ &=P(X_1\oplus X_2\oplus\cdots\oplus X_{n-1}=0)P(X_n=0)\\ &\quad+P(X_1\oplus X_2\oplus\cdots\oplus X_{n-1}=1)P(X_n=1)\\ &=pp_n+(1-p)(1-p_n)\\ &=2(p_n-\tfrac{1}{2})(p-\tfrac{1}{2})+\tfrac{1}{2}\end{aligned}$$

이다. 따라서, 수학적 귀납법에 의해서

$$P(X_1\oplus X_2\oplus\cdots\oplus X_n=0)=2^{n-1}\prod_{i=1}^{n}(p_i-\tfrac{1}{2})+\tfrac{1}{2}$$

이다.

[예] 3-라운드 선형근사

$$[7,18,24,29]\leftarrow[15]$$
$$\emptyset\leftarrow\emptyset$$
$$[7,18,24,29]\leftarrow[15]$$

첫째 라운드에서 $NS_5(16,15)=-20+32$이므로,

$X_1[15]\oplus K_1[22]$
$=f_1(X_1,K_1)[7,18,24,29]$ 확률 $\frac{-20}{64}+\frac{1}{2}$ (1)

셋째 라운드에서 $NS_5(16,15)=-20+32$이므로,

$X_3[15]\oplus K_3[22]$
$=f_3(X_3,K_3)[7,18,24,29]$ 확률 $\frac{-20}{64}+\frac{1}{2}$ (2)

이다. 한편,

$f_1(X_1,K_1)[7,18,24,29]$
$=PH[7,18,24,29]\oplus X_2[7,18,24,29]$
$f_3(X_3,K_3)[7,18,24,29]$
$=CH[7,18,24,29]\oplus X_2[7,18,24,29]$

이다. 여기서, X_i, K_i, $f(X_i,K_i)$는 각각 i-라운드 f함수의 입력, 서브 키, 출력이다. 또, PH, PL, CH, CL은 각각 평문의 왼쪽 반, 평문의 오른쪽 반, 암호문의 왼쪽 반, 암호문의 오른쪽 반이다. 이 두 식을 (1)과 (2)식에 대입하여 X_2항을 소거하면, Piling-up 보조정리에 의해서 확률 $2(\frac{-20}{64})(\frac{-20}{64})+\frac{1}{2}$인 3-라운드 선형근사를 얻을 수 있다.

$$PH[7,18,24,29]\oplus CH[7,18,24,29]\oplus PL[15]\oplus CL[15]=K_1[22]\oplus K_3[22]$$

식을 간단히 표현하기 위해서 i-라운드의 f함수의 입력번지들의 집합을 I_i, 출력 번지들의 집합을 O_i, 키의 번지들의 집합을 A_i라고 하자. 이젠, 선형근사를 이용하여 linear 암호분석의 과정을 살펴보자.

정리 2.1. (Linear 암호 분석 방법) $N-1$라운드의 선형근사를 이용하여 N-라운드 DES를 linear 암호분석할 수 있다.

증명 : $N-1$라운드의 선형근사식은 다음과 같다(정리 3.1 참조).

$$PH[O_1]\oplus PL[I_1]\oplus PL[O_2]\oplus X_N[O_{N-1}]\oplus X_{N-1}[O_{N-2}]\oplus X_{N-1}[I_{N-1}]=K_1[A_1]\oplus K_2[A_2]\oplus\cdots\oplus K_{N-1}[A_{N-1}]$$

한편, $X_N[O_{N-1}]=CL[O_{N-1}]$, $X_{N-1}[O_{N-2}]=f_N(CL,K_N)[O_{N-2}]\oplus CH[O_{N-2}]$, $X_{N-1}[I_{N-1}]=f_N(CL,K_N)[I_{N-1}]\oplus CH[I_{N-1}]$이다. 따라서,

$$PH[O_1]\oplus PL[I_1]\oplus PL[O_2]\oplus CL[O_{N-1}]\oplus CH[O_{N-2}]\oplus CH[I_{N-1}]=f_N(CL,K_N)[O_{N-2},I_{N-1}]\oplus K_1[A_1]\oplus K_2[A_2]\oplus\cdots\oplus K_{N-1}[A_{N-1}]$$

이다. 위의 식이 성립할 확률은 바로 선형근사의 확률이다. 마지막 라운드의 정확한 키 K_N과 정확한 $K_1[A_1]\oplus K_2[A_2]\oplus\cdots\oplus K_{N-1}[A_{N-1}]$값에 대해서는 평문과 대응되은 암호문의 px100%가 위의 식을 만족하지만 임의의 K_N과 $K_1[A_1]\oplus K_2[A_2]\oplus\cdots\oplus K_{N-1}[A_{N-1}]$에 대해서는 50% 정도 성립한다. $N-1$라운드의 선형근사의 확률이 0 또는 1에 가까운 값일수록 마지막 라운드의 키 K_N을 쉽게 찾을 수 있다.

3. 선형근사의 성질

N-라운드 DES를 linear 암호 분석하기 위해서는 $N-1$라운드의 선형근사가 필요하다. 선형근사가 될 조건은 아래의 정리와 같다.

정리 3.1. $O_i=I_{i-1}\Delta O_{i-2}(3\le i\le N)$인 조건을 만족하는 N-라운드 DES는 선형근사이다. 단, $A\Delta B=A\cup B-A\cap B$이다. 이때, N-라운드 DES의 선형근사식은 다음과 같다.

$$PH[O_1]\oplus PL[I_1]\oplus PL[O_2]\oplus CH[O_N]\oplus CL[O_{N-1}]\oplus CL[I_N]=K_1[A_1]\oplus K_2[A_2]\oplus\cdots\oplus K_N[A_N]$$

증명 : 각 라운드의 f함수의 입력번지, 출력번지, 키의 번지로 부터 다음 식을 얻을 수 있다.

$$\begin{aligned}X_1[I_1]\oplus K_1[A_1]&=PH[O_1]\oplus X_2[O_1]\\X_2[I_2]\oplus K_2[A_2]&=PL[O_2]\oplus X_3[O_2]\\X_3[I_3]\oplus K_3[A_3]&=X_2[O_3]\oplus X_4[O_3]\\&\vdots\\X_{N-1}[I_{N-1}]\oplus K_{N-1}[A_{N-1}]&=X_{N-2}[O_{N-1}]\oplus X_N[O_{N-1}]\\X_N[I_N]\oplus K_N[A_N]&=X_{N-1}[O_N]\oplus CH[O_N]\end{aligned}$$

한편, $O_i=O_{i-2}\Delta I_{i-1}$이므로 $X_i[I_i]\oplus X_i[O_{i-1}]=X_i[O_{i+1}](i\ge 2)$이다. 따라서,

$$X_1[I_1]\oplus X_N[I_N]\oplus K_1[A_1]\oplus\cdots\oplus K_N[A_N]=PH[O_1]\oplus PL[O_2]\oplus X_N[O_{N-1}]\oplus CH[O_N]$$

이다. $X_1[I_1]=PL[I_1]$, $X_N[I_N]=CL[I_N]$, $X_N[O_{N-1}]=CL[O_{N-1}]$을 위의 식에 대입하면 된다.

위의 정리를 이용하여 쉽게 선형근사와 선형근사식을 얻을 수 있다. 앞의 2장에서 본 예를 적용해 보자.

$$[7,18,24,29] \leftarrow [15]$$
$$\emptyset \leftarrow \emptyset$$
$$[7,18,24,29] \leftarrow [15]$$

$I_1=\{15\}$, $O_1=\{7,18,24,29\}$, $I_2=O_2=\emptyset$, $I_3=\{15\}$, $O_3=\{7,18,24,29\}$이므로 $I_2\Delta O_1=\{7,18,24,29\}=O_3$이다. 따라서, 위의 3-라운드 구조는 선형근사이다. 또한, 쉽게 선형근사식과 선형근사의 확률을 구할 수 있다.

4. 반복 가능한 선형근사

N-라운드 DES의 linear 암호분석을 효과적으로 하기위해서는 확률이 최적인 $N-1$라운드의 선형근사를 찾아야 한다. 선형근사의 확률 p가 최적 ($|p-\frac{1}{2}|$ 이 최대)일수록 linear 암호 분석을 하기가 쉽고, 역으로 선형근사의 확률이 1/2에 가까운 값일수록 암호분석을 하기가 어렵다. 특히, 선형근사의 확률이 1/2이면 linear 암호분석은 불가능하다. 라운드의 수 N이 클 경우 확률이 최적인 선형근사를 찾기위해서는 작은 라운드의 반복 가능한 선형근사를 찾는 것이 효과적이다.

[정의] $I_2=O_1$, $O_2=I_1$인 2-라운드 선형근사를 2-라운드 반복 가능한 선형근사라고 한다.

A를 $I_1\rightarrow O_1$, B를 $O_1\rightarrow I_1$, -를 $\emptyset\rightarrow\emptyset$라고 하면 AB-BA-AB-…, 또는 BA-AB-BA-…로 연결함으로서 큰 라운드의 선형근사를 얻을 수 있다.

정리 4.1. 확률이 최적인 DES의 2-라운드 반복 가능한 선형근사는 $I_1=[5]$, $O_1=[0]$, $I_2=[0]$, $O_2=[5]$이고, 선형근사의 확률은 $2(\frac{4}{64})(\frac{-2}{64})+\frac{1}{2}$이다.

[정의] $I_1=O_2=I_3$, $O_3=O_1\Delta I_2$인 3-라운드 선형근사를 3-라운드 반복 가능한 선형근사라고 한다.

A를 $I_1\rightarrow O_1$, B를 $I_2\rightarrow I_1$, C를 $I_1\rightarrow O_1\Delta I_2$, -를 $\emptyset\rightarrow\emptyset$라고 하면, ABC-CBA-ABC-CBA-…로 연결함으로서 큰 라운드의 선형근사를 얻을 수 있다.

정리 4.2. 확률이 최적인 3-라운드 반복 가능한 선형근사는

$I_1=[15]$, $O_1=[7,18,24,29]$, $I_2=[29]$,
$O_2=[15]$, $I_3=[15]$, $O_3=[7,18,24]$

이고, 선형근사의 확률은 $2^2(\frac{-20}{64})(\frac{-2}{64})(\frac{10}{64})+\frac{1}{2}$이다.

5. 결 론

DES-like 암호를 linear 암호 분석하기 위해서는 확률이 최적인 선형근사를 구해야 한다. 라운드의 수가 클 경우 2, 3, 4-라운드 반복 가능한 선형근사를 이용하여 선형근사를 구하는 것이 효과적이다.

참 고 문 헌

[1] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Wiezmann Institute of Science, Israel, 1990.

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

[3] E. Biham and A. Shamir, Differential cryptanalysis of the full DES, Technical report, Israel Institute of Technology, 1991.

[4] L.R. Knudsen, Cryptanalysis of LOKI, Asiacrypt '91, 1991.

[5] L.R. Knudsen, Iterative characteristics of DES and s^2-DES, Crypto '92, 1992.

[6] M. Matsui, Linear cryptanalysis method for DES cipher, Eurocrypt '93, 1993.

□ 著者紹介

成 洙 學(正會員)

1982年 慶北大學校 數學科(學士)
1985年 KAIST 應用數學科(碩士)
1988年 KAIST 應用數學科(博士)
1988年～1991年 韓國電子通信研究所 先任研究員
1991年～현재 培材大學校 應用數學科 助教授