DES 암호화기법의 확장속성과 암호 성능에 관한 연구

이경원(한밭대학교 컴퓨터공학과 통신서비스연구실) kwlee@hanbat.ac.kr
김정호(한밭대학교 컴퓨터공학과 통신서비스연구실) jhkim@hanbat.ac.kr

요 약

최근 인터넷 등의 컴퓨터 네트워크가 급속히 보급되고, 이러한 컴퓨터 네트워크의 개방화, 세계화에 따라 안정성에 대한 위협이 커다란 문제로 지적되고 있다. 특히 인터넷을 비즈니스에 응용하려는 상업화 움직임에 따라 정보 보호의 필요성이 더욱 커지고 있으며, 정보를 어떻게 보호할 것인가의 문제가 정보화의 발전을 좌우하는 커다란 과제로 대두되고 있다.

이에 따라 개인의 프라이버시 보호, 기밀성, 무결성, 인증, 부인봉쇄 등의 서비스를 제공하는 정보보호의 유효한 기술로서 암호에 대한 연구가 활발히 이루어지고 있다.

현재 가장 보편적으로 사용되고 있는 대표적인 암호 알고리즘인 DES(Data Encryption Standard)는 평문, 암호문, 키 모두 64비트 사이즈를 가진 블록암호이다. DES가 보유하고 있는 56비트의 키는 하드웨어의 기술수준이 높아짐에 따라 그 안전성이 위협받을 가능성은 매우 높아진다. 이로 인하여 56비트 키 길이를 갖는 DES는 exhaustive 공격과 테이블 look up 공격 그리고 time-memory trade off 공격 등에 대해서 암호강도가 감소된다. 따라서 암호강도의 향상을 위해서는 DES의 키 길이에 대한 확장 알고리즘이 요구된다.

본 연구에서는 DES의 성능을 증가시키기 위해서 아래와 같은 조건들을 만족시키도록 확장된 DES를 설계하였다

1) 현재의 56비트 키 길이를 112비트 길이로 확장시켰다.
2) S-box 내의 엔트리를 일정하게 수정하여 SAC과 상관계수 조건에 맞게 S-box를 선정하였다.
3) Differential Cryptoanalysis 공격에 대한 대응방안으로 라운드 특성이 구성될 확률을 낮추기 위해 16 라운드 동안의 F함수 반복 횟수를 2회 증가시키도록 한다.

그러므로 1), 2), 3) 조건을 만족시키기 위한 암호 알고리즘 설계는 DES알고리즘과 같이 입력데이터의 한 블럭을 64 비트씩 읽어들여 이를 2개의 32비트 서브 블록 (L, R)으로 나누어 암호함수를 적용하는 것이 아니라 입력데이터의 한 블록단위를 96비트로 읽어드려 이를 3개의 서브 블럭(A, B, C)이 16 라운드를 반복 수행하도록 하였다.

먼저 DES의 대칭적 특징인 암호화 과정과 복호화 과정의 식은 다음과 같다.

암호화 :

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

복호화 :

$R_{i-1} = L_i$

$L_{i-1} = R_i \oplus f(R_{i-1}, K_i)$

$= R_i \oplus f(L_i, K_i)$

DES의 56비트 키 길이를 112비트로 확장하고, S-box를 수정한 확장된 DES 암호 알고리즘의 식은 다음과 같다.

암호화 :

$A_i = B_{i-1}$

$B_i = C_{i-1} \oplus f(B_{i-1}, K_{2,i})$

$C_i = A_{i-1} \oplus f(B_{i-1}, K_{1,i})$

복호화 :

$A_{i-1} = C_i \oplus f(A_i, K_{2,i})$

$B_{i-1} = A_i$

$C_{i-1} = B_i \oplus f(A_i, K_{1,i})$

$f_1(B_{i-1}, K_{1,i}) = P(S_1(D_1), \cdots\cdots\cdots, S_8(D_8))$

$f_2(B_{i-1}, K_{2,i}) = P(S_9(D_9), \cdots\cdots\cdots, S_{16}(D_{16}))$

$D_1D_2D_3,\ldots\ldots,D_8 = E(B_{i-1}) \oplus K_{2,i}$

$D_9D_{10}D_{11},\ldots\ldots,D_{16} = E(B_{i-1}) \oplus K_{1,i}$

$f_1(B_{i-1}, K_{1,i})$, $f_2(B_{i-1}, K_{2,i})$: f function

$P(S_1, \ldots\ldots)$: P-box

S_i : i번째 S-box

D_i : Si의 입력 6 bit

$E(B_{i-1})$: expansion permutation

암호시스템의 분석에는 여러 가지 방법이 있다. 이 연구에서는 제안한 확장된 DES 알고리즘을 DC(differential cryptanalysis)와 상관계수(correlation coefficient)에서 성능을 평가하고자 한다.

DC로 공격하기 위해서, DES의 16라운드 순환 특성(characteristic)은 추가된 하나의 라운드와 2라운드 반복 특성(iterative characteristic)에 기반을 둔 15라운드의 순환 특성으로 구성된다. DC의 공격에 대응하기 위해 DES의 모든 16라운드는 $(1/234)^6 = 2^{-47.2}$만큼의 순환 특성을 가져야 한다. DC 공격은 $2^{47.2} = 1.6\times10^{16}$(8비트)의 선택평문 메시지가 필요하다. 만약 제안한 확장된 DES 알고리즘에서 DC를 적용한다면, 16라운드 특성은 하나의 추가 라운드와 3라운드 반복 특성과 2R-attack을 위한 2-round에 기반을 둔 13라운드 순환 특성으로 구성된다. DES의 F함수와 마찬가지로 F1과 F2가 같다면, 확장된 DES의 변형에서 13라운드의 순환 특성의 확률은 약 $(1/234)^8$이기 때문에 확장된 DES는 모든 16라운드에서 DC 공격에 대응하기 위해 $(1/234)^8 = 2^{-6294}$의 16라운드 순환 특성을 필요로 한다. 따라서, 확장된 DES가 DC에 대응하기 위한 순환 특성의 확률은 DES보다 증가된다. 이것은 DC의 공격에서 확장된 DES가 DES보다 강력하다는 것을 의미한다. 또한 DC 대응하기 위해서 확장된 DES는 $2^{62.96} = 8.97*10^{18}$(12바이트)의 많은 양의 선택평문 메시지가 필요하다.

Webster와 Trvares는 완전함(completeness)의 개념과 쇄도효과(avalanche effect)를 결합하기 위해서 SAC(Strict Avalanche Criterion, p_{ij})를 소개했다. 일반적인 S-box는 Z_2^n에서 Z_2^m(n>m)까지의 부울함수로 간주된다.

하나의 입력 비트가 보수화되고, 각각의 출력 비트가 모든 입력 비트에 의해 결정될 때 출력 비트의 평균은 변한다. 만일 모든 입력 비트가 바뀐다면 f함수의 각각의 출력 비트는 변할 확률이 있다. i번째 입력 비트가 보수화되었을 때 $p_{i,j}$는 j번째 출력 비트가 변화할 확률을 나타낸다. $p_{i,j}$가 0.5로 가까이 접근할수록 S-box는 SAC를 더욱 만족시킬 수 있다. [표-1]에서는 확장된 DES에서 S-box의 $p_{i,j}$가 DES의 $p_{i,j}$보다 0.5에 근접함을 나타내고 있다. 이것은 DES보다 확장된 DES가 SAC을 만족한다는 것을 의미한다.

$p_{i,j}(k)$는 쇄도 백터 V_k의 I번째 입력 비트와 j번째 출력 비트 사이의 상관관계를 나타낸다. S-box 출력의 각각의 비트 사이에서 상관계수는 독립적이어야 하고, 상관계수($-1\leq|p_{i,j}(k)|\leq1$)가 0에 가까워질수록 더 나은 설계라고 할 수 있다.

[표-2]는 확장된 DES에서 S-box의 상관계수가 DES의 상관계수보다 0에 근접하다는 것을 보여준다. 결과적으로, 이러한 SAC과 상관계수를 가지는 S-box를 디자인했을 때, DES의 S-box보다 확장된 DES의 S-box가 보다 나은 안정성을 가질 수 있다.

[표-1] DES와 확장된 DES의 S-box의 SAC($p_{i,j}$)

S-box	DES	확장된 DES
S_1	0.620	0.500
S_2	0.633	0.500
S_3	0.661	0.497
S_4	0.665	0.508
S_5	0.663	0.500
S_6	0.651	0.500
S_7	0.656	0.495
S_8	0.625	0.508
S_9		0.505
S_{10}		0.500
S_{11}		0.505
S_{12}		0.508
S_{13}		0.518
S_{14}		0.497
S_{15}		0.508
S_{16}		0.505

[표-2] DES와 확장된 DES의 S-box의 상관계수

S-box	DES	확장된 DES
S_1	-0.195	-0.048
S_2	-0.188	-0.030
S_3	-0.165	-0.049
S_4	-0.232	-0.040
S_5	-0.184	-0.035
S_6	-0.183	-0.037
S_7	-0.153	-0.037
S_8	-0.176	-0.034
S_9		-0.039
S_{10}		-0.014
S_{11}		-0.043
S_{12}		-0.045
S_{13}		-0.007
S_{14}		-0.030
S_{15}		-0.043
S_{16}		-0.085

본 연구에서는 확장된 DES 기법에 대한 성능표현을 제안하고, DC 공격에 대한 안전성 검증을 수행하였다. 확장된 DES는 DC에 대응하기 위한 16라운드 순환 특성을 증가하기 위해서, 각각의 서브블럭이 모든 16라운드를 수행하는 동안에 F함수의 반복 횟수가 다르도록 DES 알고리즘을 확장시켰다. 확장된 DES를 DES와 비교할 때의 성능 표현에서 다음의 개선 효과를 얻었다.

첫째 DC에 대응하기 위해 확장된 DES의 특성의 확률은 DES의 확률보다 낮게 감소된다. 둘째 96비트의 입력 데이터 블록을 각각 32비트의 3개의 서브 블록으로 나누어 실행시켰다(F함수 적용). 셋째 S-box를 S^1-S^{16}으로 확장시킨 결과 SAC에 있어서 확장된 DES의 p_{ij}는 DES의 p_{ij}보다 더욱 0.5에 근접하게 되었으며, 상관계수에 있어서 확장된 DES의 p_{ij}는 DES의 p_{ij}보다 더욱 0에 근접하게 된다.

따라서 본 연구에서 DC에 대한 하나의 대응방안으로 S-box의 엔트리를 재구성하여 XOR 분포를 균일하도록 하고 SAC와 상관관계의 조건에 알맞은 S-box를 선정함으로써 성능표현에서 개선된 효과를 얻었다.