韓國 컴퓨터情報學會 論文誌
第12卷 第2號, 2007. 5.

2007-12-2-1-8

암호화 강도 향상을 위한 새로운 교차구조기반의 DB-DES 알고리즘

이 준 용*, 김 대 영**

A New Crossing Structure Based DB-DES Algorithm for Enhancing Encryption Security

Lee Jun Yong*, Kim Dae Young**

요 약

DES는 64비트의 평문을 64비트의 암호문으로 암호화하는 블록 사이퍼 암호 시스템으로 1976년 표준으로 채택되어 20년 동안 전세계적으로 널리 쓰여왔다. 그러나 하드웨어와 암호 해독 기술의 발달로 인해 취약점이 드러난 DES는 더 이상 안전하지 않기 때문에 암호화 강도를 높인 새로운 암호 시스템이 요구되었다. 이에 따라 여러 가지 방법이 제안되었으며, 그 중에서 NG-DES[1]에서는 키 길이의 확장과 비선형 f함수를 사용하여 기존 DES보다 암호화 강도를 높일 수 있었다. NG-DES는 기존의 DES를 64비트에서 128비트로 확장하면서 각 라운드에 사용되는 Fiestel 구조 또한 확장하였는데, 이 구조는 각 평문 비트 변화가 전체 암호문 비트에 영향을 미치지 못하는 단점을 가지고 있다. 본 논문에서는 NG-DES에서 제안된 확장 Fiestel 구조에서 라운드 간의 입출력 연결을 효과적으로 교차시킴으로써 혼돈과 확산을 증가시켜 암호화 강도를 높인 암호 시스템을 제안한다.

Abstract

The Data Encryption Standard (DES) is a block cipher that encrypts a 64 bit block of plaintext into a 64 bit block of ciphertext. The DES has been a worldwide standard for 20 years since it was adopted in 1976. strong. But, due to the rapid development of hardware techniques and cryptanalysis, the DES with 64-bit key is considered to be not secure at the present time. Therefore it became necessary to increase the security of DES. The NG-DES(New Generation DES)[1] is an encryption system which upgrades the encryption security of DES by the key extension and the usage of non-linear f function. It extends not only the size of plaintext and

• 제1저자 : 이준용
• 접수일 : 2007.4.11, 심사일 : 2007.4.18, 심사완료일 : 2007. 5.20.
* 홍익대학교 컴퓨터공학과 교수 ** 홍익대학교 컴퓨터공학과 박사과정
※ 이 논문은 2004년도 홍익대학교 교내연구비에 의하여 지원되었음

ciphertext to 128 bit but also the Fiestel structure used in each round. This structure has a weak point that the change of each bit of plaintext does not affect all bits of ciphertext simultaneously. In this paper, we propose a modified Fiestel structure of DES and thus increased confusion and diffusion by effectively cross-connecting between outputs in a round and inputs in next round.

▸ Keyword : 하드웨어 설계(Hardware design), 컴퓨터 구조(Computer Architecture), 암호화 알고리즘(Encryption Algorithm), DES(Data Encryption Standard), 암호화 프로세서(Encryption processor)

Ⅰ. 서 론

오늘날 정보 통신 기술의 발전과 더불어 사회의 전반적인 활동이 고속 통신망을 이용하여 이루어지고 있으며 최근 인터넷을 기반으로 한 정보의 처리 및 교환이 활발해짐에 따라 정보보호에 대한 관심이 높아지게 되었다. 정보화 시대에 있어서 정보의 가치는 개인이나 기업체의 중요한 자산으로 인식되어질 수 있을 뿐만 아니라, 더 나아가서 국가의 안보와도 밀접한 관계를 맺고 있다. 그러한 정보의 올바른 사용과 관리를 지향하기 위한 기술적, 제도적 장치는 정보혁명 시대에 있어서 필수적으로 구축되어야할 사항일 것이다. 이러한 정보보호의 필요성에 따라 오래 전부터 암호학과 암호기술에 많은 발전이 이루어져왔다.[5][6][7] 최근에는 셀룰라 프로그래밍[10]을 이용한 난수 생성에 관한 연구도 진행되고 있으며, 진화론적 계산을 기반으로 하는 암호화 알고리즘도 많이 제안되고 있다.[11]

1970년대 중반 미국 표준국(NBS)에 의해서 민간 분야에서 사용될 암호시스템의 표준으로 DES가 등장하게 되었고 DES 암호화 기법은 그 이후로 가장 널리 사용되게 되었다. DES는 64bit의 키를 적용하여 64bit의 평문을 암호화시키는 대칭형 블락 암호이다.[2][3] 최근 하드웨어와 암호분석 기술의 발달로 인해로 인해 64bit의 키를 사용하는 DES는 DC(Differential Cryptanalysis)와 병렬처리 기술에 의해 짧은 시간에 쉽게 해독될 수 있다. NG DES[1]에서는 DES의 암호화 강도를 높이고자 키와 평문의 길이를 전수 공격(exhaustive key search)에 대응할 수 있을 만큼 128bit로 확장하였고, DES 알고리즘에서 가장 취약한 부분인 f함수의 선형을 보완하기 위해 f함수를 비선형적인 함수로 변경하였다.

NG-DES는 기존의 DES를 64비트에서 128비트로 확장하면서 각 라운드에 사용되는 Fiestel 구조 또한 확장하였는데, 이 구조는 각 평문 비트 변화가 전체 암호문 비트에 영향을 미치지 못하는 단점을 가지고 있다. 본 논문에서는 NG-DES에서 제안된 확장 Fiestel 구조에서 라운드 간의 입출력 연결을 변경하여 암호화의 강도를 결정짓는 요소 중 혼돈과 확산을 증가시킴으로써 암호 해독 공격에 더 안전한 암호 시스템을 소개하고자 한다.

Ⅱ. 관련 연구

2.1 DES

DES는 64비트의 키(실제는 56비트, 8비트는 parity bit)를 적용하여 64비트의 평문을 64비트의 암호문으로 암호화시키는 대칭형 블록 암호이다. DES 알고리즘에서는 대체(substitution)와 치환(permutation)이라는 2개의 기본적인 암호화 함수가 반복적으로 16회 적용된다.[8]

2.2 암호/복호화 과정

DES의 암호화 과정은 다음과 같이 크게 3단계로 나눌 수 있다.

첫째, 64비트의 평문이 치환된 입력을 생성하기 위해 비트열의 순서를 재조정하는 초기 순열(IP : Initial Permutation) 단계

둘째, 순열과 치환의 기본적인 암호화 함수가 64비트 평문에 동일하게 16회 반복되어 적용되는 단계

셋째, 16번 반복 처리된 64비트의 출력을 좌우로 교환하고 초기 순열의 역인 역초기 순열(IP-1 또는 FP : Final Permutation)을 통과하는 단계

그림 1은 DES 암호화와 복호화의 전 과정을 보여주고 있다. DES의 복호화 과정은 암호화 과정과 동일하다. 단지, 각 라운드마다 생성되어 적용되는 부분키 ki를 역으로 적용시키는 것만 다를 뿐이다. 그림 2는 라운드마다 평문에 적용되는 암호화와 복호화의 공식을 나타낸 것이다.

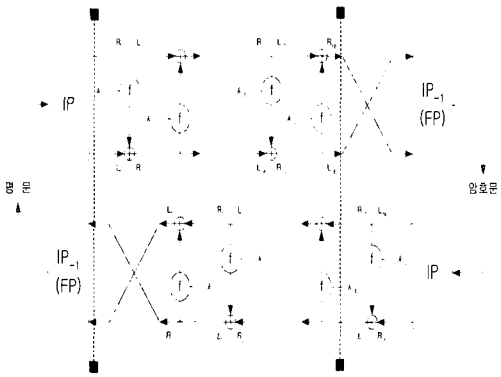

그림 1. DES의 암호화와 복호화 과정
Fig 1. Encryption and decryption process of DES

암호화 : $L_i = R_{i-1}$

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

복호화 : $R_{i-1} = L_i$

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

(L_i, R_i : 32비트 평문 블록, K_i : round i 에 대한 48비트 키, f : 데이터와 키를 조합하는 함수)

그림 2. DES의 암호화와 복호화 공식
Fig 2. Encryption and decryption formula of DES

초기 치환을 통해서 얻어진 64비트의 평문 블록은 그림 3과 같은 한 라운드를 16번 반복한 후에 암호문 블록으로 바뀌게 된다. 더 자세히 살펴보면 초기 치환을 거친 64비트가 두개의 32비트 L0과 R0으로 분할되고 여기에 64비트 키로부터 생성된 부분키 k1(48비트)이 적용되어 역시 32비트의 L1과 R1을 생성한다. 이 과정이 16회 반복된다.

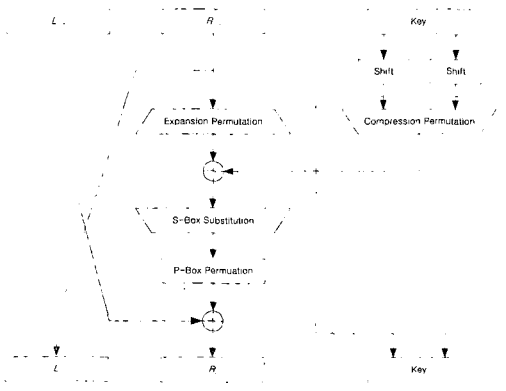

그림 3. DES의 한 라운드(round)
Fig 3. One round of DES

2.2 NG-DES

2.2.1 암복호화 구조

NG-DES[1]는 전수 공격(exhaustive key search)에 대응할 수 있도록 DES 키의 길이를 64비트에서 128비트로 확장하였고 이에 따라 평문의 길이 또한 128비트로 확장하였다. 기존 DES의 각 라운드에서는 64비트만 처리할 수 있기 때문에 128비트를 처리하기 위해 Fiestel 구조를 다음과 같이 확장하였다. 128비트의 평문 블록을 4개의 32비트 서브 블록으로 나눈 뒤, 한 쌍의 32비트 평문 블록을 기존의 DES와 같은 구조의 입력으로 사용하고 나머지 한 쌍은 그 앞의 구조와 대칭되는 구조의 입력으로 사용한다. 그림 4는 NG-DES의 한 라운드의 구조를 보여주고 있다.

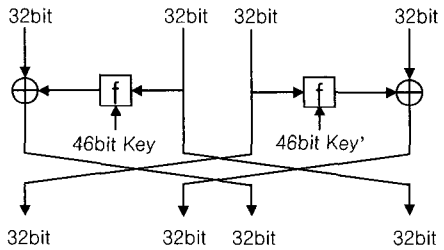

그림 4. NG-DES의 한 라운드
Fig 4. One round of NG-DES

각 라운드가 끝날 때마다 오른쪽의 64비트 결과와 왼쪽의 64비트 결과를 교환하는데, 단 암호화와 복호화의 구조를 동일하게 하기 위해 마지막 라운드가 끝난 뒤에는 교환하지 않는다.

2.2.2 서브키

f함수에 사용되는 2개의 48비트 서브키는 서로 다른 키를 사용하는데 다음과 같은 수식을 만족해야 한다.

48비트 서브키 Ki와 K'i는 다음과 같이 3개의 16비트 키로 구성된다.

$$K_i = (k_{i1}, k_{i2}, k_{i3})$$

$$K'_i = (k'_{i1}, k'_{i2}, k'_{i3})$$

$$k_{i1} \odot k'_{i1} = 1$$

$$k_{i2} \odot k'_{i2} = 1$$

$$k_{i3} \odot k'_{i3} = 1$$

i : 라운드 수

⊙ : 비 부호 16비트 정수로 취급되는 입력과 출력에 대한 정수 법 216+1(mod 65537)

(예) x ⊙ y = (x × y) mod 216 + 1

단, 곱셈 연산(multiplication operation)의 입력 중 16비트 모두가 '0'인 경우에는 216으로 취급한다.

2.2.3 NEW_f 함수

NG-DES에서 사용되는 f 함수는 기존의 DES와 같은 구조를 가지고 있다. 단지, 그림 3의 선형적인 XOR 함수 부분을 비선형적인 NEW_f 함수로 대체함으로써 차분 암호 해독(differential cryptanalysis)과 같은 암호 공격에 대응할 수 있도록 암호화 강도를 높인 것이 특징이다. NEW_f 함수는 두 개의 입력(48비트 expansion permutation의 결과와 48비트 서브키)을 받아들여 48비트의 출력을 만드는 함수이다. 그림 5는 NEW_f 함수의 구조를 보여주고 있다.

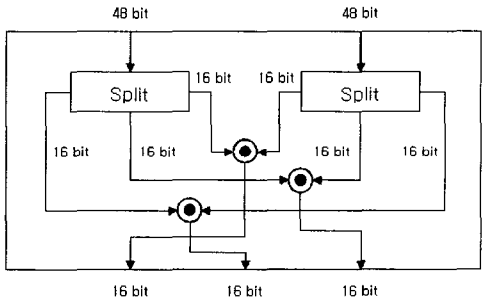

그림 5. NEW_f 함수
Fig 5. New_f function

각각의 입력 48비트를 3개의 16비트로 나눈 뒤 그림 5와 같이 곱셈 연산(multiplication)을 적용한다. 그리고 출력된 3개의 16비트 결과값을 적절히 48비트의 비트열에 위치시킴으로 해서 확산의 효과를 얻는다.

III. Double DES (DB-DES)

NG-DES에서 각 라운드가 끝날때마다 교환(swapping)되는 32비트는 다음 라운드에서 다른 수식의 입력으로 들어가 암호학적 강도에 사용되는 확산을 제공하며, f함수의 비선형성은 혼돈을 제공하는 역할을 한다. 혼돈과 확산의 정의는 다음과 같다.

혼돈(confusion) : 어떻게 암호문의 통계적 성질이 평문의 통계적 성질에 의존하는 지에 대한 결정을 복잡하게 하는 것.

확산(diffusion) : 각 평문의 비트와 키의 비트는 암호문의 모든 비트에 영향을 주어야 한다.

여기서 NG-DES의 암호화 구조는 64비트로 나누어진 두 개의 서브 블락(sub-block)이 라운드마다 서로 위치가 교환되는 구조를 갖고 있어서, 두 개의 서브 키 값이 두 서브 블락에 모두 적용되므로 키값에 의한 확산은 제공되지만, 두 서브 블락의 평문이 서로 섞이지는 않기 때문에 평문에 의한 확산은 제한된 단점을 갖고 있다. 본 논문에서 제안한 Double DES는 NG-DES의 이러한 단점을 보완하기 위해 각 라운드마다 교환되는 입출력 연결을 변경하여 평문에 의한 확산이 증대되도록 개선하였다. 그림 6은 Double DES의 한 라운드와 구조를 보여준다.

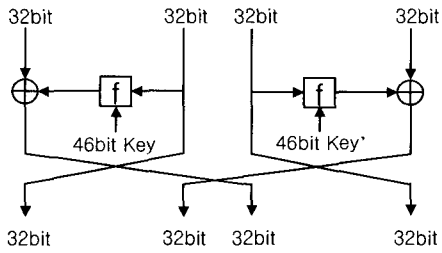

그림 6. Double DES의 한 라운드
Fig 6. One round of Double DES

앞에서도 설명했듯이 128비트로 확장된 NG-DES의 경우, 128비트를 두 개의 64비트 서브 블락으로 나누어 각 64 비트를 기존의 DES와 같은 방식으로 처리하게 된다. NG-DES의 경우에는 오른쪽 서브 블락(64비트 모두)이 다음 라운드의 왼쪽 서브 블락의 입력으로 왼쪽 서브 블락은 다음 라운드의 오른쪽 서브 블락으로 교차하여 들어간다. 물론, 서브 블락내에서는 입력 되는 수식이 라운드가 바뀔 때마다 서로 교차하는 형태이므로 각 64비트 서브 블락내에서는 확산이 일어난다. 하지만 왼쪽 서브 블락과 오른쪽 서브 블락은 16라운드를 거치는 동안 서로 섞이지 않기 때문에 평문에 의한 확산이 각 블락의 64비트 내로 제한되게 된다. 즉, 블락 내 교차(inter-block exchange)는 발생하지만 블락 간 교차(intra-block exchange)는 발생하지 않는다. 그림 7은 NG-DES와 DB-DES의 평문에 의한 확산 효과를 도식화 한 것이다. 평문을 P, 암호문을 C, 왼쪽(상

위) 블락을 L, 오른쪽(하위) 블락을 R이라고 표기하면, 그림에서 보듯이 평문의 왼쪽 블락(PL)에 속한 비트 하나가 0에서 1로 바뀌게 되었을 때 NG-DES의 암호화 구조상 이 평문 한 비트의 변화는 전체 암호문에 영향을 미치지 못하고 암호문의 왼쪽 블락(CL)내에서만 영향을 미치게 된다. 따라서 확산의 효과가 전체 블락의 절반으로 제한되는 단점이 존재한다. 하지만 DB-DES의 경우에는 평문 중에서 어떤 한 비트가 변화하더라도 이 비트의 변화 효과가 전체 암호문 블락에 영향을 미치게 된다. 이는 그림 4의 NG-DES와 그림 6의 Double DES의 라운드간 입출력 연결을 비교해 보면 쉽게 알 수 있다. DB-DES에서는 한 라운드의 출력이 다음 라운드의 입력으로 들어갈 때 한 블락(64비트)의 두 개의 출력 중 하나(32비트)씩 양쪽 블락간에 서로 교차되는 구조를 갖고 있기 때문이다. 즉, 라운드 수행 시마다 이전과 다른 수식으로 들어갈 뿐만 아니라(inter-block exchange) 하나의 출력은 다른 블락으로 들어가는(intra-block exchange) 구조를 갖고 있어 평문에 의한 확산을 증가시키는 효과를 가지고 있다.

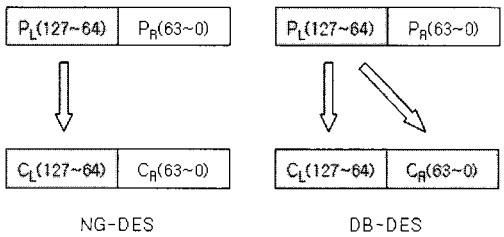

그림 7. NG-DES와 DB-DES의 평문에 의한 확산 효과 비교
Fig 7. Comparison of diffusion effect of NG-DES and DB-DES by plain text

그림 8은 DB-DES의 전체 암호화 구조를 보여준다. 각 라운드에 사용되는 키는 NG-DES와 동일한 방식으로 생성되며 왼쪽 블락에 사용되는 키를 Low Key, 오른쪽 블락에 사용되는 키를 High Key라고 표기하였다. 라운드간 입출력 연결을 변경하였기 때문에 키 배열을 NG-DES와 달리 라운드마다 동일한 블락의 입력으로 들어간다.

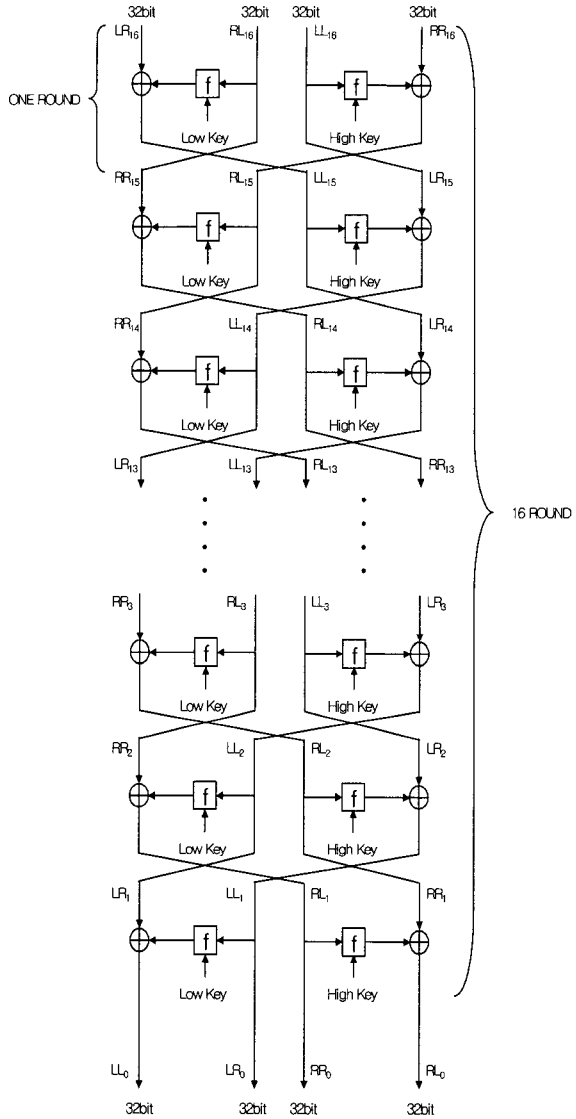

그림 8. Double DES의 암호화 구조
Fig 8. Encryption structure of Double DES

그림에서 볼 수 있듯이 각 32비트 입력은 4라운드를 주기로하여 4개의 수식을 모두 통과하며 2개의 키값이 모두 적용되는 구조를 갖고 있다. 따라서 키값에 의한 확산 뿐만 아니라 평문에 의한 확산이 효과적으로 일어나는 구조를 갖고 있다. 암호화와 복호화의 구조를 동일하게 하기 위해 NG-DES와 같이 마지막 라운드 후에는 교환을 하지 않는다.

IV. 성능 평가

DB-DES의 암호화 강도를 측정하기 위해 Visual C++을 이용하여 NG-DES와 DB-DES를 구현하여 키와 평문에 변화에 따른 암호문의 변화를 분석하였다. 128비트 크기의 키와 평문을 각각 100개씩 생성하여 실험한 후 그 평균치를 구하여 비교 분석하였다.

먼저 그림 9는 평문에서 0~63번째 위치에 있는 각 한 비트씩을 변화시켰을 때, 암호문 전체 비트의 변화 개수를 100개의 평문에 대하여 실험한 후 평균을 구한 값이다. 이는 그림 7에서 설명한 대로 NG-DES의 경우에는 평문의 반쪽 블락내에서의 변화가 암호문의 절반에만 영향을 미치는 반면 DB-DES의 경우에는 전체 암호문에 영향을 미치기 때문에, DB-DES가 NG-DES에 비해 전체적으로 높은 변화량을 보여주고 있어 확산의 효과가 더 큼을 확인할 수 있다. 평문 한 비트의 변화에 따른 암호문 비트의 평균 변화율은 DB-DES의 경우 6.66비트, NG-DES의 경우는 3.75비트를 나타내었다.

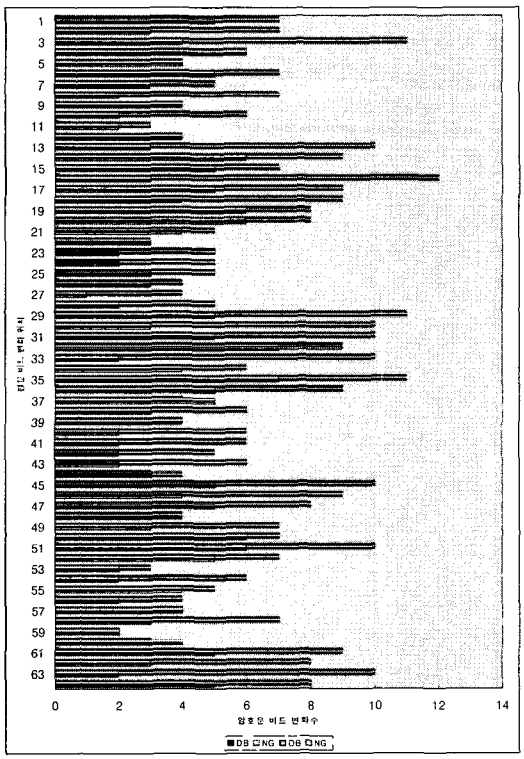

그림 9. 평문 한 비트의 변화에 따른 암호문 비트의 변화량 비교
Fig 9. Comparison of change of encryption text bits by plaintext change

그림 10은 0~63번째 위치에 있는 평문 비트가 1개부터 64개까지 변화하였을 때 DB-DES와 NG-DES의 전체 암호문의 비트 변화량을 보여준다. 그림에서 보듯이 DB-DES의 확산 정도가 NG-DES에 비해 월등히 나음을 알 수 있다. 평균적으로 NG-DES는 24.125, DB-DES는 34.875의 비트 변화량을 나타내었다. 그림 11은 0~127번째 위치에 있는 평문 비트가 65개에서 128개까지 변화하였을 때의 결과이다. 이 경우에는 NG-DES도 평문의 변화가 암호문 전체에 영향을 주기 때문에 DB-DES와 암호문의 비트 변화수가 DB-DES와 대동소이하다. 따라서, 평문 비트의 변화가 왼쪽과 오른쪽 중 어느 한쪽 블락내에 치우져 있을 경우에는 DB-DES가 NG-DES보다 확산에 의한 암호화 강도가 더 높다는 결론을 내릴 수 있다.

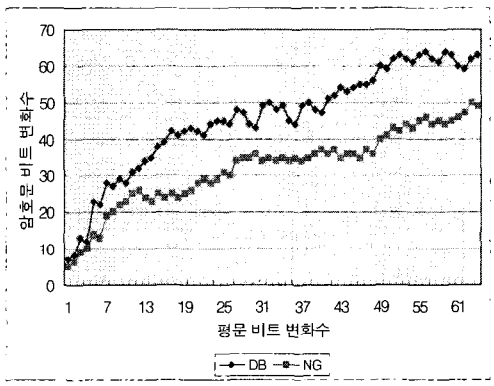

그림 10. 평문 비트 변화 개수(1~64)
Fig 10. Number od bit change in plain text(1~64)

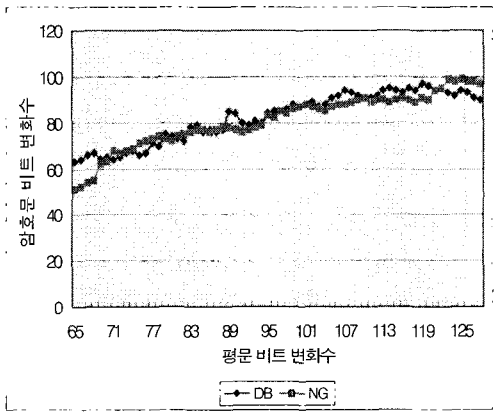

그림 11. 평문 비트 변화 개수(65~128)
Fig 11. Number od bit change in plain text(65~128)

그림 12는 키 비트의 변화에 따른 암호문의 변화량을 비교한 것이다. DB-DES와 NG-DES의 키 적용 방식은 유사하지만 라운드 간의 입출력 구조가 다르기 때문에 암호문 비트의 변화에는 다소 차이가 있다. 하지만 평균적인 비트 변화량은 DB-DES의 경우 31.55, NG-DES의 경우 31.16으로 키값에 의한 확산의 정도는 서로 비슷한 것을 확인할 수 있다.

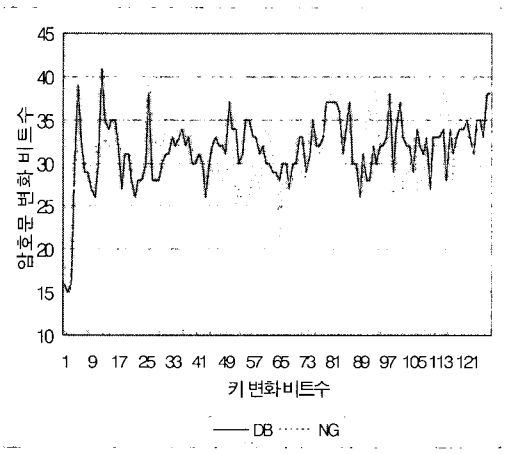

그림 12. 키 비트의 변화에 따른 암호문 비트의 변화량 비교
Fig 12. Comparison of change of encryption text bits by key bit change

결론적으로, 키의 변화에 따른 암호문의 확산 효과는 DB-DES와 NG-DES가 비슷하지만, 평문의 변화에 따른 엄호문의 확산 효과는 DB-DES가 NG-DES에 비해 대략 1.5배 정도 큰 것을 확인할 수 있었다.

V. 결론

NG-DES는 하드웨어와 암호 해독 기술의 발달로 인해 취약점이 드러난 DES를 키 길이의 확장과 비선형 f함수를 사용하여 암호화 강도를 높인 암호 시스템이다. NG-DES는 기존의 DES를 64비트에서 128비트로 확장하면서 각 라운드에 사용되는 Fistel 구조 또한 확장하였는데, 이 구조는 각 평문 비트 변화가 전체 암호문 비트에 영향을 미치지 못하여 암호화 강도를 판단하는 요소중 확산의 효과가 떨어지는 단점을 가지고 있다. 본 논문에서는 NG-DES에서 제안된 확장 Fistel 구조에서 라운드 간의 입출력을 연결할 때 왼쪽 64비트 블락과 오른쪽 64비트 블락을 효과적으로 교차시킴으로써 확산을 증가시켜 암호화 강도를 높인 암호 시스템(Doubld Des)을 제안하고, Visual C++로 두 시스템을 구현하여 비교 분석하였다. 분석 결과 평문의 변화에 따른 암호문의 변화율이 기존의 NG-DES에 비해 대략 1.5배 높은 것으로 나타나 DB-DES가 확산에 의한 암호화 강도가 더 높음을 확인할 수 있었다. 따라서, 제안된 시스템을 하드웨어로 구현할 경우 기존의 시스템과 동일한 자원과 속도를 유지하면서도 암호화 강도는 향상되는 장점을 지닌다.

참고문헌

[1] 지훈, 이준용 "DES를 기반으로 하는 새로운 암호기법에 대한 연구, NG(NewGeneration)- DES", CAD 및 VLSI 설계연구회 학술발표회 논문집, pp 89-95, 1999.

[2] NBS, "Data Encryption Standard," FIPS Pub. 46, U.S, National Bureau of Standards, Washington DC, Jan. 1997

[3] Barker, W. Introduction to the Analysis of the Data Encryption Standard(DES), Laguna Hills, CA: Aegean Park Press, 1991.

[4] William Stallings, "Network and Internetwork Security-Principles and Practice", Prentice-Hall, 1995.

[5] 이민섭, "현대 암호학", 敎友社, 1999.

[6] Bruce Schneier, "Applied Cryptography," 3rd. ed.

[7] 박창섭, "암호 이론과 보안", 大英社, 1999.

[8] E.Biham and A.Shamir, "Differential cryptanalysis of the full 16-round DES," Proc. of crypto'92. 1992..

[9] Eli Biham, "On Matsui's Linear Cryptanalysis," Technion-Computer Science Dep. 1994.

[10] Sheng-Uei Guan and Shu Zhang, "Evolutionary Approach to the Design of Controllable Cellular Automata Structure for Random Number Generation," IEEE Trans. on

evolutionary computation, Vol. 7, No. 1, pp. 23-36, 2003.

[11] P. Isasi and J. C. Hernandez, "Introduction to the applications of evolutionary computation in Computer Security and cryptography," Computational Intelligence, Vol. 20, No. 3, pp. 445-449, 2004.

저 자 소 개

이 준 용

1996 : 미네소타 주립대 컴퓨터공학박사

1996·1997 : 미국 IBM 연구원

1997~ 현재: 홍익대학교 교수

관심분야 : 컴퓨터구조, 임베디드시스템, 정보보안

김 대 영

1998 : 홍익대학교 컴퓨터공학과 학사

2001 : 홍익대학교 전자계산학과 석사

2001~ 현재 : 홍익대학교 컴퓨터공학과 박사과정