정보처리에 적합한 내장형 데이터 암호블록 설계

송제호*, 방준호*, 김태형*, 이우춘*, 김환용**
*전북대학교 IT응용시스템공학과, 원광대학교 전자 및 제어공학부
e-mail:songjh@jbnu.ac.kr

Design of inner Data Crypto-Block adapted Information Processing

Je-Ho Song*, Jun-Ho Bang*, Tae-Hyung Kim*, Woo-choun Lee*, Hwan-Yong Kim**
*Dept. of IT Applied System Eng. Chonbuk National University
**Div. of Electronic and control Engineering. WonKwang University

요 약

본 논문에서는 기존 암호알고리즘과 호환성을 갖는 비밀키 암호알고리즘에 기반을 둔 새로운 데이터 암호알고리즘을 제안 하였다. 그러므로 정보처리에 적합한 새로운 내장형 암호 블록을 설계하고 검증하는데 Synopsys 툴로 설계하였고 40MHz의 시스템 속도환경에서 Altera MAX+PlusⅡ툴로 모의실험 및 검증한 결과 단일 라운드로 640Mbps의 데이터 처리율을 확인하였다. 따라서, 제안된 암호시스템에 적용할 경우 실시간 정보보안 및 정보처리에 적용할 수 있다고 사료된다.

1. 서론

1949년 발표된 Shannon의 논문에서 현대 암호는 기원하며 1960년 대는 컴퓨터와 통신시스템의 발달로 디지털 형태의 자료 및 보안서비스를 제공할 필요성이 증가함에 따라, 1977년에 미국 표준 암호알고리즘으로 DES (Date Encryption Standard)를 선정하여 현재까지 세계 표준 암호로써 금융망과 상업용 네트워크를 중심으로 널리 사용되는 대표적인 비밀키 암호알고리즘(private key cryptoalgorithim)이 되었다[1,2]. 암호로서 기본적인 기능으로는 기밀성(confidentiality), 인증(authentication), 무결성(integrity), 부인방지(nonrepudiation), 전달방지(replay prevention), 접근제어(access control), 유용성(availability)등을 갖추어야 하며 보안 설계에 있어서 매우 중요하다. 암호 방식은 데이터 암호부분에서 사용되는 기법으로 Feistel 및 SPN(Substitution Permutation Networks) 구조를 사용하였다 [3,4]. 일반 블록 암호시스템은 최소 16회 정도 반복 수행하지만 본 논문에서는 F 암호함수를 이용하여 단지 1회의 라운드에서만 수행하도록 한 결과 단순 키 기능과 인증 및 비대칭형 개념을 가진 킷값으로 비도를 높일 수 있었다[3,4,5].

본 논문에서 설계 환경은 40MHz의 시스템 속도와 Synopsys 툴을 사용하였다. 따라서, 새로운 시스템 구조 및 암호알고리즘이 적용된 범용 데이터 암호블록은 128 비트 데이터를 가지고 범용 Synopsys로 설계하였고 Altera MAX+PlusⅡ 타임 시뮬레이션(time simulation)으로 640Mbps의 처리속도 및 인증에 대하여 검증하였다.

2. 범용 블록 암호알고리즘 구조

비밀키 암호시스템은 변환하는 방법에 따라 데이터를 블록 단위로 처리하는 블록 암호알고리즘(block cryptoalgorithm)과 평문의 작은 단위인 비트단위로 처리하는 스트림 암호알고리즘(strea cryptoalgorithm)으로 나눈다[5]. 블록 암호방식은 크게 DES와 같은 형태인 Feistel 방식과 치환(substitution)과 재배열(perm -utation)을 반복하여 사용하는 S-P 네트웍 방식 등이 있다. Feistel 방식은 한 라운드에 평문의 일부만 처리하여 병렬처리 효율이 낮은 반면 라운드 함수 설계의 융통성과 암·복호화 과정이 동일하다는 장점을 가진다[6,7]. S-P 네트웍 방식은 한 라운드에서 전체 평문을 암호화하므로 병렬처리가 가능하여 속도가 빠르지만 복호화를 고려하여 암호

화 과정을 설계하므로 설계의 폭이 좁다.

블록 암호의 동작 모드는 다음과 같다[8,9].

ECB 모드(Electronic Code Book)는 각각의 평문을 블록 단위로 독립적인 암・복호화 과정을수행한다.

긴 평문 $M = M_1 \| M_2 \| \cdots \| M_n$을 전송해서 $C = E_k(M_1) \| E_k(M_2) \| \cdots \| E_k(M_n)$라는 암호문을 만든다. 수식으로 표현하면 식 (1)과 같다.

$$C_i = E_k(M_i) \tag{1}$$

$$M_i = D_k(C_i)$$

CBC 모드(Cipher Block Chaining)는 일반적인 암호 모듈에서 IV(Initialization Vector)값을 사용하는데 응용 프로그램인 임의숫자 생성기(random number generator)를 사용하여 자동으로 생성된다.

$$C_i = E_k(M_i \oplus C_{i-1}) \tag{2}$$

$$M_i = D_k(C_i) \oplus C_{i-1}$$

CFB 모드(Cipher Feedback)는 의사난수데이터(pseudo random data)를 생성하기 위해 사용되며, 암호문을 생성하기 위하여 평문(M_i)과 XOR 연산하고 출력된 암호문은 다음 블록에 대한 의사난수데이터를 만들기 위하여 블록 암호화로 귀환된다. 식 (3)에서 암・복호화 대하여 나타낸다.

$$C_i = M_i \oplus E_k(C_{i-1}) \tag{3}$$

$$M_i = C_i \oplus E_k(C_{i-1})$$

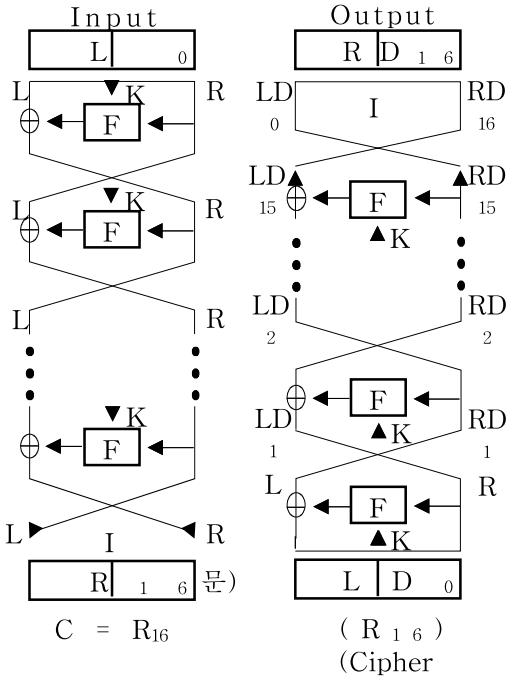
OFB 모드(Output Feedback)는 독립적인 수열 테이터 블록(sequence data block) S를 자체 동기(self synchronizing) 스트림 암호문으로 변환하는 과정이다. 평문(M_i)는 이전에 S_{i-1}을 암호화한 S_i와 XOR 연산한 후 암호문 블록이 되는 것은 식 (4)로 표현된다.

$$S_i = E_k(S_{i-1}), \quad C_i = M_i \oplus S_i \tag{4}$$

$$S_i = E_k(S_{i-1}), \quad M_i = C_i \oplus S_i$$

3. 내장형 블록 암호알고리즘 설계

본 논문에서 제안된 알고리즘은 데이터 암호부분에서 Feistel 및 SPN구조를 사용하였다. Feistel 암호화는 평문을 우측과 좌측 반씩 두 개(L_0, R_0)로 나누고 라운드 함수 F는 서브키(K_i)를 우측 반에만 적용하고, F 출력은 좌측의 반과 XOR 연산을 한 후 우측으로 위치가 교환된다. 복호화 과정은 암호화 과정의 대칭관계이며 암호화의 첫번째 라운드는 그림 2에서 상세히 나타내고 수식은 식 (5)로 표현된다[10,11].



(a) 암호화 과정 (b) 복호화 과정

[그림 1] Feistel 구조

$$L_1 = R_0 \tag{5}$$

$$R_1 = L_0 \oplus F(R_0, K_1)$$

$$C = R_1 \| L_1 = L_0 \oplus F(R_0, K_1) \| R_0$$

i번째 라운드에서 암호화 및 복호화 수식은 식 (6), 식 (7)로 나타낸다.

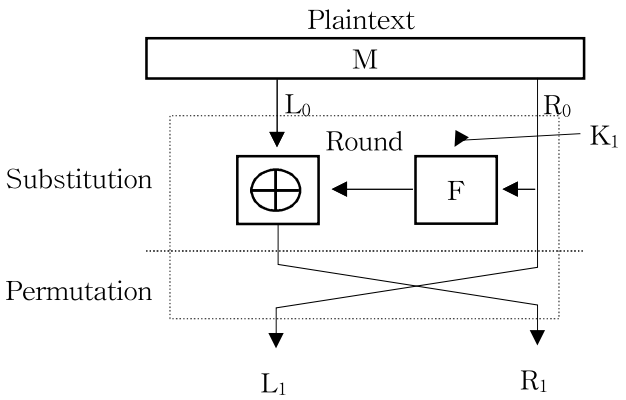
$$L_i = R_{i-1} \tag{6}$$

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

$$C = R_i \| L_i = L_{i-1} \oplus F(R_{i-1}, K_i) \| R_{i-1}$$

$$LD_i = RD_{i-1} \tag{7}$$

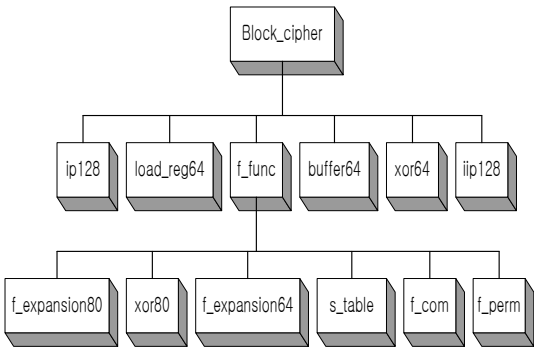
$$RD_i = LD_{i-1} \oplus F(RD_{i-1}, K_{n-i+1})$$



[그림 2] Feistel 암호화의 첫번째 단계

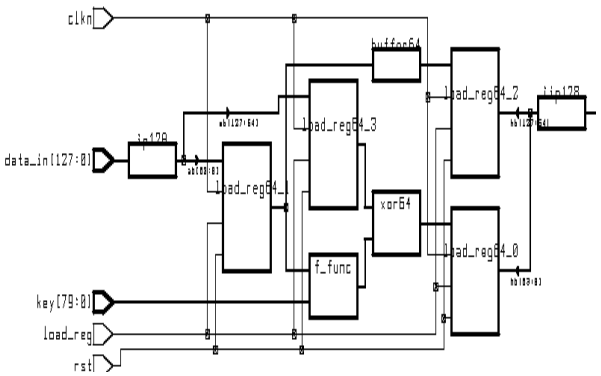
본 논문에서 제안한 정보처리용 암호시스템에서 데이터를 암호화하는 블록이다. 암호화를 수행하는데 사용되는 하부 블록은 6개의 기능 블록으로 구성되어있다.

정보처리에 적합한 내장형 데이터 암호시스템에서 데이터를 암호화하는 블록은 그림 3과 같다. 암호화를 수행하는데 사용되는 하부 블록은 6개의 기능 블록으로 구성되어있다.



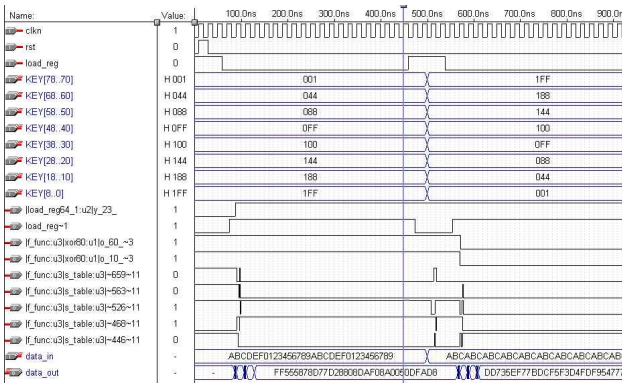
[그림 3] 정보처리용 내장형 데이터 암호 기능 블록도

정보처리용 데이터 암호 블록도는 그림 4와 같다.



[그림 4] 정보처리용 내장형 데이터 암호 블록도

그림 5는 데이터를 암호화하는 내장형 데이터 암호블록에 대한 모의실험 결과다. 입력 데이터는 “ABCDEF0123456789ABCDEF0123456789”이며 암호화된 데이터는 “FF555878D77D28808DAF08A00 50FAD8”이다.



[그림 5] 정보처리용 내장형 데이터 암호 블록의 모의실험 결과

5. 결론

현대 사회는 정보 통신 및 정보화 기술의 급속한 발전으로 실생활의 많은 부분들이 사이버 세계에서 이루어 지면서 정보 보호에 대한 인식이 점차 확산되어가고 있다.

본 논문에서 정보처리에 적합한 내장형 데이터 암호블록은 비밀키 암호알고리즘에서 블록 암호화 방식을 기준으로 시스템을 구성하였다. 그리고 데이터 암호부분에서 사용되는 기법은 Feistel 및 SPN 구조를 혼합하여 사용하였다. 데이터 암호화는 단일 라운드를 사용하여 단지 1회의 라운드에서만 수행하여도 단순 키 기능과 인증 및 비대칭형 개념을 가진 키값으로 비도를 높일 수 있도록 F 암호함수를 사용한 결과 일반 블록 암호시스템에서 최소 16회 정도 반복 수행 한 것과 같은 비선형화를 시켰다. 본 논문에서 내장형 데이터 블록 암호시스템을 Synopsys 툴로 설계하였고 40MHz의 시스템 속도환경에서 Altera MAX+PlusⅡ툴로 모의실험 및 검증한 결과 단일 라운드로 640Mbps의 데이터 처리율을 확인하여 정보처리 및 암호화에 적용할 수 있을것으로 사료된다.

참고문헌

[1] 서광석, 김창한, 암호학과 대수학, 북스힐,1999.
[2] 이병관, 전자상거래 보안, 남두도서, 2002.

[3] 이임영, 송유진 역, 현대암호, 생능출판사,1999.
[4] 권용진, 박종서, 조성준 역, 현대암호이론, 인터비젼, 2001.
[5] D. R. Stinson, Cryptography Theory and Practice, Chapman & Hall/CRC, 2002.
[6] VISA Open Platform Overview, 1999.
[7] J. Bruer, "On Nonlinear Cimbinations of Linear shift Register Sequences,"
[8] L. Brown and J. Seberry, Key scheduling in DES type Cryptosystems, Abstract of AUSCRYPT90, 1990.
[9] E. Biham and A. Shamir, Differential Cryptanalysis of the Full 16-Round DES, Proc. of CRYPTO92, 1992.
[10] W. Diffie and M. E. Hellman, Exhaustive Cryptanalysis of the NBS Data Encryption Standard, IEEE Vol. 10. No. 6, 1977.
[11] E. F Brickell, J. H. Moor and M. R. Purtill, Structure in the S-Boxes of DES, Proc. of CRYPTO86, 1986.