1999年度 大韓電子工學會 秋季綜合學術大會 論文集 第22卷 第2號 99/11

VHDL을 이용한 개선된 Isolated 2중 DES의 설계 및 구현

이 재 철, 홍 진 표, 강 민 섭
안양대학교 정보통신·컴퓨터공학부
전화 : (0343) 467-0990 / 팩스 : (0343) 467-0800

Design and Implementation of Modified Isolated Double DES Using VHDL

Jae-Chul Lee, Jin-Pyo Hong and Min-Sup Kang
Division of Computer & Electronic Engineering, Anyang University
E-mail : jclee@cs2.anyang.ac.kr

Abstract

Conventional double DES has been not only shown to have a vulnerable drawback to attack method called 'Meet-in-the-Middle', but also to be hard to use that it is because software implementation has a number of problem in real time processing.

This paper describes the design and implementation of modified Isolated double DES algorithm using VHDL for resolving the above problems. In this approach, we also discuss an efficient method for increasing cipher strength through expansion of key length.

1. 서 론

컴퓨터 통신망은 종합정보통신 시스템이 구축되어 사용자에게 요구되는 각종 서비스를 제공해주고 있다. 그러나 실제 통신장치, 통신 선로 등으로 구성되는 통신망에서는 도청자가 통신중인 정보를 도청하여 해독함으로써 정보가 누출되거나 데이터를 변조, 삽입 및 삭제 등이 가능하기 때문에 이를 방지하기 위한 컴퓨터나 통신 시스템상에서 정보보호를 위한 암호화 연구가 활발히 진행되고 있다[1-5].

현재 가장 보편적으로 실용화되어 사용되는 암호 알고리듬은 IBM의 Lucifer 알고리듬을 기반으로 개발한 DES(Data Encryption Standard)이다[1,2]. 그러나 DES는 키 길이가 짧은 것이 문제점으로 지적되어 왔다[5]. 1990년에 Biham과 Shamir는 평문의 입력과 암호문의 차이를 분석한 차분 암호 해독(differential cryptanalysis) 공격방법을 발표하여 2^{55}미만의 복잡도로 DES(Data Encryption Standard)를 해독할 수 있음을 보였고[6], 1993년에 Matsui는 선형 해독법을 발표하여 56 비트의 단일 DES 알고리듬이 기지의 평문과 암호문 쌍을 이용한 공격방법에 취약성이 있음을 지적하였다[3].

단일 DES의 짧은 키 길이를 보완한 알고리듬으로 다중 암호 방식인 2중 DES(double DES)는 키 길이를 112비트로 확장할 수 있어 비도를 높일 수는 있으나 중간 결과에 의한 공격(Meet-in-the-Middle)에 취약하다[4].

소프트웨어적으로 구현된 이러한 암호 알고리듬들[3-5]은 명령어 인출(fetch), 디코딩 그리고 실행하는데 많은 Machine Cycle이 필요하므로 혁신적인 병렬처리 기술이 개발되지 않는 한 현재까지는 하드웨어에 의한 구현 속도에는 미치지 못하고 있는 실정이다.

이러한 문제를 해결하기 위해서 하드웨어적인 접근방식으로서 FPGA(Field Programmable Gate array)/ASIC(Application Specific IC)을 이용한 암·복호 알고리듬의 구현에 대한 연구가 계속되고 있다[8].

한편, 중간 결과에 의한 공격을 보완하기 위한 Isolated 2중 DES이 제안되었으나[7], 하드웨어적인 구현에 관한 연구는 아직 공개되지 않았다.

이 연구는 반도체설계교육센타로부터 부분적인 지원을 받아 이루어 졌음.

본 논문에서는 중간 결과에 의한 공격을 보완할 수 있는 Isolated 2중 DES를[7] 기반으로 킷값과 데이터를 확장시킨 개선된 Isolated 2중 DES를 제안한다.

제안된 암호 시스템은 기존의 Isolated 2중 DES보다 암호강도를 강하며, 수행시간을 단축시키기 위하여 VHDL(VHSIC Hardware Description Language)을 이용하여 하드웨어로 구현하였다.

2. 기존 DES 알고리듬

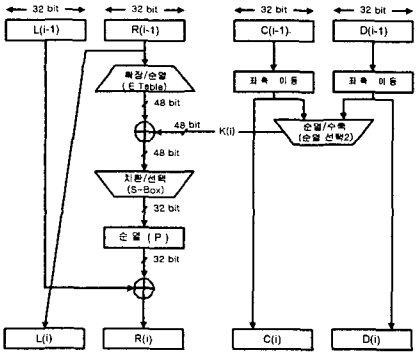
2.1 확장된 DES(HDES) 알고리듬

단일 DES는 암호화, 복호화 알고리즘이 대칭적이며 치환(permutation)과 대치(substitution) 그리고 S_box로 구성된 블록 암호화 시스템으로 64 비트의 평문 블록은 초기 치환(IP: initial permutation)후에 32 비트씩 좌(L_0), 우(R_0)부분으로 나뉘게되어 16라운드의 계산을 거치게 된다. 16라운드 후에는 역 초기 치환(IP^{-1}: inverse initial permutation)을 거쳐 암호문(ciphertext)이 생성된다[1]. 본질적으로 대치된 64 비트 입력은 16라운드를 거치며 매 라운드의 결과로 64 비트의 중간 값을 생성한다. 각 64 비트 중간 값의 좌우 절반은 분리된 32 비트 값으로 취급되며 L(왼쪽)과 R(오른쪽)로 분류된다. 각 라운드의 전체적인 처리는 다음 공식으로 요약된다.

$$L_i = R_{i-1}$$

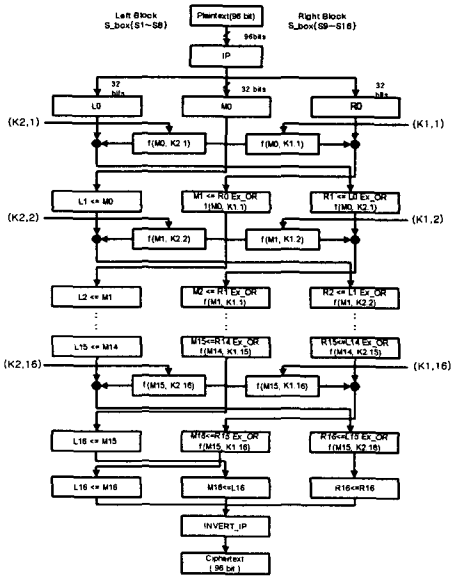
$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

여기서 ⊕은 비트 단위 XOR함수를 의미한다. 한 라운드의 구조는 <그림 1>과 같다[5].



<그림 1> 단일 DES의 한 라운드 구조

<그림 2>는 단일 DES를 기본으로한 확장된 DES(HDES)의 암호 알고리듬을 나타낸다[9]. HDES는 DES의 키(key) 길이 56 비트를 112 비트로 확장시켰고, S_box를 S_1 - S_{16}으로 확장시켰으며, 입력데이터의 한 블록단위를 96 비트로 읽어서 이를 3개의 서브 블록(L, M, R)이 16라운드를 반복 수행한다.



<그림 2> 확장된 DES(HDES) 암호 알고리듬

그러나 이 알고리듬은 DES에 비해서 암호강도는 증가되지만, 해킹 수법의 발전으로 인하여 아직도 공격에 취약한 문제점을 가지고 있다.

2.2 Isolated 2중 DES 알고리듬

단일 DES의 보안성을 강화하기 위해 다중 키를 이용한 다중 암호 방식(multiple encryption)인 2중 DES는 2번의 암호화 단계와 2개의 키를 갖는데 하나의 평문 P(64 bit)와 두 암호키 K_1(56 bit) 및 K_2(56 bit)가 주어졌을 경우 암호문 C와 복호화된 평문 P는 각각 식 (1)과 (2)와 같이 정의된다.

$$C = E_{K2}[E_{K1}[P]] \quad (1)$$

$$P = D_{K1}[D_{K2}[C]] \quad (2)$$

2중 DES는 56(비트) × 2(K_1, K_2) = 112 비트 크기의 키가 되어 암호의 강도가 단일 DES 보다 현저히 증가되나 중간 결과에 의한 공격 방법에 취약하다[4].

2중 DES의 중간결과에 의한 공격을 보완하기 위한 Isolated 2중 DES 알고리듬은 기존의 2중 DES의 2단계의 암호화 단계에서 첫 번째 암호화 단계가 끝난 후 나온 중간 결과와 중간키를 XOR 연산을 하여 다음 단계의 입력으로 전해주는 것이다.

3. VHDL을 이용한 개선된 Isolated 2중 DES의 설계

3.1 개선된 Isolated 2중 DES 알고리듬

제안한 알고리듬은 중간결과에 의한 공격을 보완하기 위하여 Isolated 2중 DES를 사용하며, 높은 비도를 얻기 위해서 각 암호화 단계에서 HDES를 사용한다.

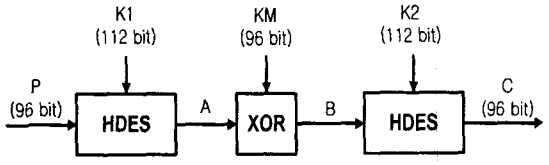
즉, 96 비트의 평문과 킷값 112 × (K_1, K_2) = 224와 중간 키(KM) 96 비트, 총 320비트의 키를 사용하여 64 비트의 평문과 킷값 112 비트와 중간 키 56 비트 총 168 비트의 키를 사용한 기존의 Isolated 2중 DES에 비해서 높은 암호화 강도를 얻을 수 있다.

제안한 알고리듬의 암호화와 복호화는 식 (3)과 (4)와 같이 정의된다.

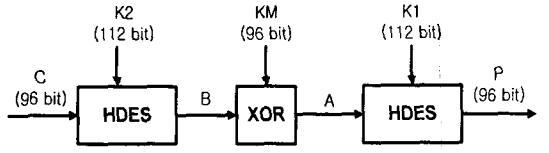
$$C = E_{K2}[KM \text{ XOR } [E_{K1}[P]]] \quad (3)$$

$$P = D_{K1}[KM \text{ XOR } [D_{K2}[C]]] \quad (4)$$

식 (3)에서 96 비트의 평문과 키 K_1으로 첫 번째 암호화 (E_{K1})을 수행하여 중간문 A를 생성하고, 중간문 A를 중간키(KM)와 XOR하여 두 번째 중간문 B를 생성하고, 다시 키 K_2로 암호화(E_{K2})를 수행하여 최종 암호문을 생성한다(<그림 3>). 복호화시에는 암호화 과정과 비슷하나 킷값을 역순으로 수행하면 평문을 생성한다. <그림 3>은 제안한 알고리듬의 전체적인 암호 구조를 나타낸 것이다.



(가) 암호화



(나) 복호화

<그림 3> 개선된 Isolated 2중 DES의 암호 구조

3.2 VHDL 모델링

본 논문에서 제안한 개선된 Isolated 2중 DES회로는 크게 암·복호처리부, 키 생성부 그리고 제어부로 구성된다.

3.2.1 암·복호처리부

제어부에서 보내는 신호에 따라 96비트 데이터의 암·복호화 처리를 수행하는 블록이다. 데이터의 입·출력에는 구애받지 않고, 암·복호할 수 있고, 암·복호화 수행시에는 키 생성부로부터 각 라운드에 대한 킷값을 입력받아 동작하게 된다.

암·복호처리부의 내부 블럭은 초기치환을 하는 IP_BOX, 96비트의 블록 데이터를 나누는 reg_dec, 실제적인 암·복호화를 수행하는 F 함수 블록, XOR연산을 하는 vector_xor, 최종 치환을 하는 IP_INV_BOX, 중간키(KM)과 XOR 연산을 하는 key_xor 그리고, 각 라운드의 중간값과 결과에 대해 다음 라운드의 입력을 조절하고, 라운드의 전체적인 입·출력을 조절하는 select_reg 블록으로 구성되어 있다.

3.2.2 F 함수 블록

F 함수 블록 DES에서 비도를 결정하는 중요한 부분으로써 비선형 치환을 하는 16개의 S_box(Sk, k = 1, 2 .. 16), 확장 치환을 하는 E_box, 키와 E_box의 출력을 XOR 연산하는 E_XOR, 그리고 1 : 1 치환을 하는 p_box로 구성되어 있다.

3.2.3 키 생성부

각 라운드에 필요한 킷값을 생성하는 부분으로 제어신호에 따라 암·복호화 수행시 shift 연산을 수행하는 블록으로 128 비트 중 패리티 비트를 제거하는 EP_BOX, 패리티 비트를 제거한 112 비트를 키 값으로 입력받아 매 라운드마다 1 비트 또는 2 비트씩 시프트 하는 key_reg(<표 1>), 그리고 그 출력을 압축 치환하는 EP(1,2)_BOX로 구성된다. 그러나 복호화시에는 <표 1>의 역순으로 수행된다.

<표 1> 암호화시 왼쪽으로 이동하는 비트수

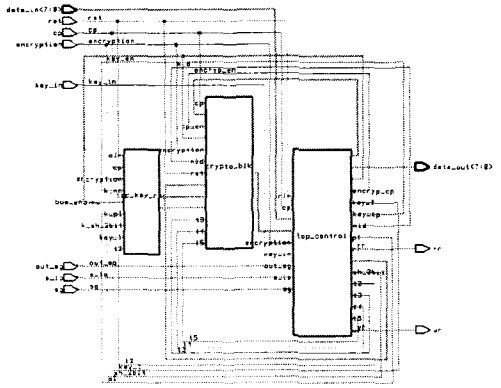
1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

3.2.4 제어부

이 블록은 데이터 입·출력과 암·복호화 처리에 관한 제어신호를 생성하여 암·복호처리부와 키 생성부에 제공하는 역할을 수행한다. 데이터 입력은 입력 레지스터(input_reg) 블록에서 외부장치로부터 입력신호를 받아 8 비트씩 데이터를 저장하며, 실제 암·복호화 수행시 필요한 96비트의 데이터와 키 데이터를 암·복호처리부와 키 생성부로 보내준다. 출력은 출력 레지스터(output_reg) 블록에서 암·복호처리부로부터 처리된 데이터를 받아 외부장치 제어신호에 의해 8 비트씩 출력한다. 또한 암·복호처리부와 키 생성부의 동작을 위한 제어신호를 생성하는 곳으로 데이터와 키의 입·출력에 관한 제어신호를 발생하는 data_process와 암·복호 수행에 관한 제어신호를 발생하는 encryp_process, 머신 사이클을 발생하는 st_gen 블록으로 구성된다.

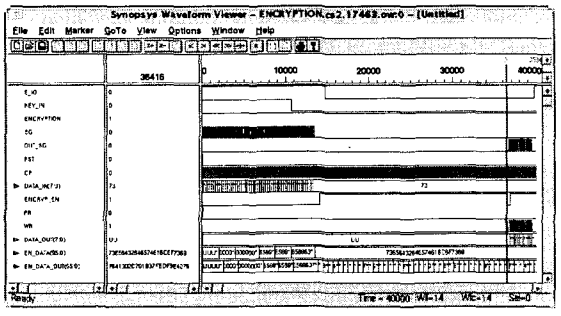
4. 구현 및 시뮬레이션 결과

본 논문에서는 개선된 Isolated 2중 DES의 알고리듬을 구현하기 위해 필요한 각 모듈은 하드웨어 기술언어인 VHDL을 이용하여 설계하였다. 설계한 회로는 Synopsys^{TM}의 Design Analyzer상에서 Altera^{TM}의 FLEX10K 셀 라이브러리를 이용하여 논리합성 수행시 총 3915 cell area의 합성 결과를 보였다. <그림 4>는 설계한 회로의 top level 블록도를 나타낸다.

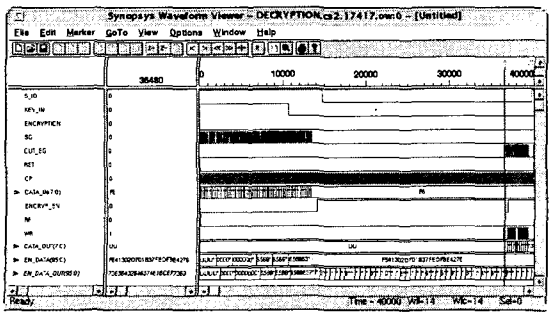


<그림 4> 개선된 Isolated 2중 DES의 top level 블록도

<그림 5>와 <그림 6>은 각각 Synopsys^{TM}에서 암호화와 복호화에 대한 VHDL 시뮬레이션 결과를 나타낸다.



<그림 5> 암호화를 위한 시뮬레이션 결과



<그림 6> 복호화를 위한 시뮬레이션 결과

적용 키(ASCII)	anyanguniversitycomputers cienceinfdepartment
적용 데이터(ASCII)	isolated2des

5. 결 론

본 논문에서는 VHDL을 이용하여 개선된 Isolated 2중 DES알고리듬의 설계 및 구현에 관하여 기술하였다. 제안한 알고리듬은 단일 DES의 짧은 키 길이와 2중 DES의 중간 결과에 의한 공격에 대한 취약점 등 기존 방법에서의 문제점 해결할 수 있다. 또한, 하드웨어적으로 구현함으로써 실시간 처리가 가능하며, 단일 DES와 2중 DES보다 높은 비도로 암·복호화가 가능하다.

본 시스템의 설계는 Synopsys^{TM}사의 Design Analyzer를 이용하여 논리합성을 수행하였고, 시뮬레이션 결과를 통하여 암·복호화가 정확히 수행됨을 확인하였다.

구현된 시스템은 전자 상거래에 이용되는 신용카드 번호 및 현금자동인출기 암호화 등에 적용할 수 있다.

참 고 문 헌

[1] NBS, "*Data Encryption Standard*," FIPS Pub. 46, U.S, National Bureau of Standard, Washington DC, Jan. 1977.

[2] "Data Encryption Algorithm," American National Standard X3, 92. ANSI, NY. 1981.

[3] M. Matsui, "Linear Crytanalysis of DES Cipher(I)", Symposium on Cryptography and Information Security'93, 1993.

[4] Diffie. W., and Hellman, M. "Exhaustive Cry ptanalysis of the NBS Data Encryption Stand ard," Computers, June 1977.

[5] 최용락, 소우영, 이재광, 이임영, "*통신망 정보 보호*", 그린 출판사, 1996.

[6] Biham, E., and Shamir, A., "Differential Cry ptanalysis of the Data Encryption Standard," New York: Springer-Verag, 1993.

[7] "2x Isolated Double-DES: Another Weak Two-Level DES Structure", http://www.l0 pht.com/pub/blackcrwl/encrypt/2XISOLAT.TXT.

[8] "Encryption Policy and Market Trends", http://guru.cose.georgetown.edus/~denning/crypt o/trends.html.

[9] 오행수, 한승조, "VHDL을 이용한 확장된 DES (HDES) 설계", 한국통신학회 논문지 Vol. 20 No 9, 1995.