32 비트 데이터 버스를 이용한 3-DES Coprocessor의 설계 및 구현

최홍묵*, 김용범*, 조화현*, 최명렬*
*한양대학교 전자전기제어계측공학과
e-mail : chmook@asic.hanyang.ac.kr

Design and Implementation of Triple-DES Coprocessor for 32-bits Data Bus

Hong-Mook Choi*, Yong-Bum Kim*,
Hwa-Hyun Cho*, Myung-Ryul Choi*
*Department of EECI, Hanyang University

요 약

정보 통신 기술의 발전이 우리 생활을 편리하게 만들고 있지만, 한편으로는 해킹, 도청 등의 부작용이 발생하고 있다. 이러한 부작용을 최소화시키는 결정적인 역할을 하는 분야가 암호학이다. 현재의 정보 보호 시스템 대부분이 소프트웨어 방식으로 구현되어 있어 암호화 속도 문제 및 해킹에 의한 불법 정보 유출의 위험성이 높은 현실이다. 이러한 점을 해결하기 위해 암호 알고리즘의 하드웨어 구현은 필수적이다. 따라서 본 논문에서는 암호 알고리즘의 속도 및 안전성 문제를 향상시키기 위해 기존에 많이 이용되고 있는 3-DES를 32 비트 데이터 버스를 이용한 하드웨어로 설계 및 구현하여 검증하고 성능 분석을 하였다.

1. 서론

21세기 현대 사회는 정보화시대이다. 컴퓨터와 통신기술의 발전은 금융업무, 전자상거래, 사이버 강의는 물론 화상회의 시스템에 이르기까지 다양한 분야에 응용되어 우리 사회를 편리하게 만들고 있다. 그러나 이러한 장점 못지 않게 해킹, 도청, 신분위조, 신분노출 등을 통한 여러 가지 부작용이 발생하는 것 또한 사실이다. 이와 같은 부작용을 최소화시켜 주는 결정적인 역할을 하는 분야가 암호학이다.

암호학 즉, 정보보호 기술은 위성 통신, CATV 등을 비롯하여, 각종 통신 이용 산업 및 전자 상거래 (EC, Electronic Commerce), 스마트 카드 등의 거의 모든 정보 통신 관련 산업 분야에서 요구되고 있다. 특히 전자 상거래 및 인터넷을 통한 정보 서비스를 사용자들이 신뢰하며 사용하기 위해서는 정보 시스템의 보안과 처리 속도가 우선적으로 보장되어야 한다. 대부분의 정보 보호를 위한 시스템이 소프트웨어 방식으로 구현되고 있어서, 암호화 속도 문제와 해킹에 의한 불법적인 정보 유출의 위험성이 높다. 그러므로 고속 통신 시스템에 암호화를 적용하거나, 키의 안전한 관리를 위해서는 암호 알고리즘의 하드웨어 구현이 필요하다. 현재 보편적으로 널리 사용되고 있는 DES 암호 알고리즘은 고성능 프로세서의 개발로 알고리즘 자체의 안정성이 위협받고 있는 상황이다. 이에 대한 대안으로 제안된 방법 중 한가지인 3-DES 암호 알고리즘은 현재 안전한 것으로 평가되고 있다[1].

따라서 본 논문에서는 암호화 과정의 처리 속도를 향상시킬 수 있도록 하기 위해 32 비트 데이터 버스를 이용하여 3-DES를 하드웨어로 설계하였다. 설계한 3-DES Coprocessor는 시뮬레이션, 합성 및 FPGA 구현으로 성능을 분석하고 검증하였다.

2. DES와 3-DES 암호 알고리즘의 개요 및 구조

DES 암호 알고리즘은 IBM의 Lucifier 암호 알고리즘을 기반으로 개발되었으며, Feistel 구조를 갖는 64 비트의 데이터와 키를 갖는 암호 알고리즘이다. 그림 1은 DES 암호 알고리즘의 구조를 나타낸다.

암호화 및 복호화가 동일한 동작의 반복으로 이루어지는 DES를 구현하는 중요한 기법은 치환(P-box), 대입(S-box) 및 키의 운영계획 등에 있으며, 이 과정을 자세하게 설명하면 다음과 같다[2].

1) 64 비트의 평문비트 블록 M을 표1에 주어진 초기치환(IP, Initial Permutation)에 의하여 치환하여 64 비트 블록 IP(M)을 얻는다.
2) 16회전의 Feistel 연산 F를 수행하여 64 비트 블록 F(IP(M))을 얻는다.
3) 64 비트 블록 F(IP(M))으로부터 표1에 주어진 초기치환의 역치환을 이용하여 64 비트 암호문 블록 IP-1(F(IP(M)))을 얻어 암호문 C를 생성한다.

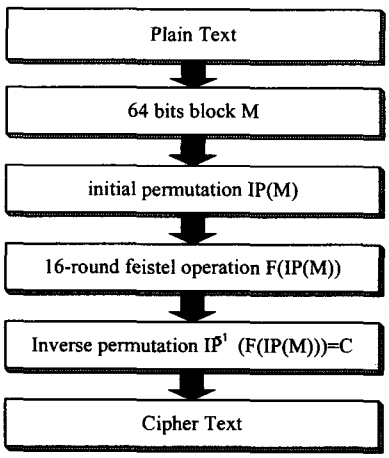

그림 1. DES 암호 알고리즘의 구조

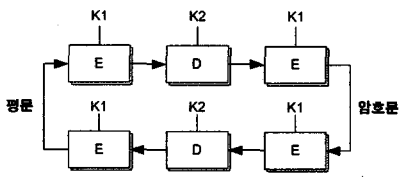

그림 2. 3-DES 암호 알고리즘의 원리

현재 1977년에 발표된 DES 암호 알고리즘의 취약성을 개선하기 위한 방안으로 다중 DES 암호 방식이 있다. 기존 DES 알고리즘을 반복적으로 적용하여 보안을 강화한 구조이다. 그 중 2개 키를 사용하는 3DES 방식이 안정성 측면과 기존 DES와 호환이 쉽게 유지되는 장점이 있어서, 키 관리 표준인 ANS X9.17과 ISO 8732에 표준으로 채택되고 있다. 그림 2는 2개의 키를 갖는 3-DES 암호 알고리즘에 대한 원리를 나타낸다[3].

3. 3-DES Coprocessor의 설계

3-DES coprocessor는 32 비트 데이터 버스를 이용하여 설계하였으며 그림 3과 같이 6개의 블록으로 구성되어 있다. 컨트롤러 블록은 3-DES 블록의 암/복호화 과정을 수행하기 위해 필요한 제어 신호를 생성하여 컨트롤 레지스터, 데이터 레지스터, 키 레지스터, 클럭 생성기, 3-DES 코어 블록에 제공한다. 컨트롤 레지스터는 3-DES의 시작 신호, 암/복호화 결정 신호, 클럭 분주 제어 신호를 생성한다. 컨트롤러로부터 입력된 32 비트씩의 데이터 및 키를 이용하여 64 비트의 평문과 128비트의 키를 생성하는 데이터 레지스터와 키 레지스터는 3-DES 코어 블록에 제공한다. 클럭 생성기는 컨트롤 레지스터에서 생성된 클럭 분주 제어 신호를 이용하여 클럭을 2분주, 4분주, 정지하는 기능을 수행하는 블록이다. 3-DES 코어 블록은 라운드 키를 생성하고 이 라운드 키를 이용하여 실질적인 암/복호화를 수행하는 블록이다. 3-DES 코어 블록의 구성은 그림 4와 같다. 1라운드 구조의 하드웨어를 16라운드 동안 반복적으로 사용하는 구조로 설계하였으며, DES의 기본 하드웨어 구조를 3번 반복하도록 설계하였다.

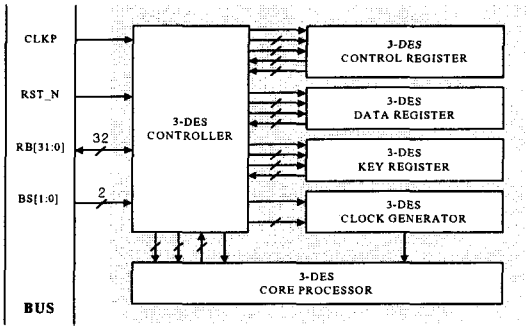

그림 3. 3-DES Coprocessor의 블록 다이어그램

그림 3에서의 CLKP, RST_N, RB[31:0]와 BS[1:0] 신호의 내용은 표 1과 같다.

표 1. 3-DES의 신호

구분	I/O	내용
CLKP	I	클럭
RST_N	I	RST_N='0' → 리셋
RB[31:0]	I/O	R/W 신호, 어드레스/데이터 버스
BS[1:0]	I	00 : 데이터 입력 01 : R/W 및 어드레스 입력 10 : 사용안함 11 : Bus idle

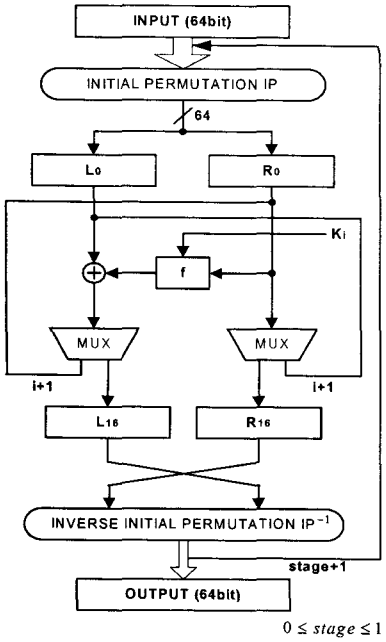

그림 4. 3-DES 코어 블록의 구조

라운드 키 생성과정은 그림 5와 같다. 라운드 키 생성도 반복구조로 설계하여 하드웨어의 면적 효율성을 높였다.

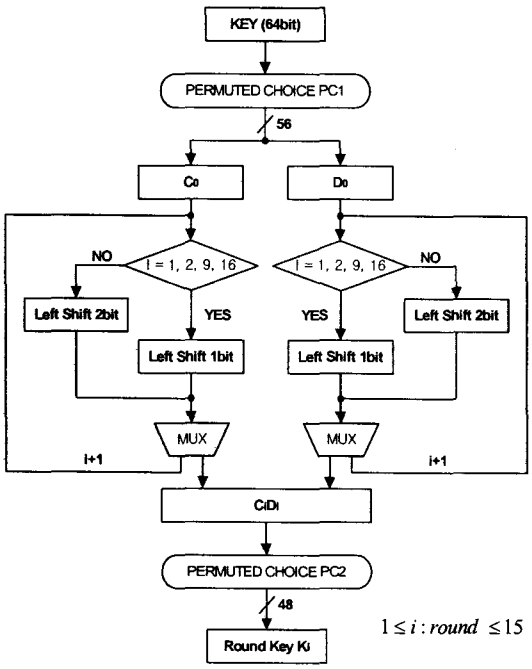

그림 5. 라운드 키 생성 과정

4. 시뮬레이션 및 합성 결과

4.1 시뮬레이션

표 2에 나타나 있는 NIST의 테스트 벡터[4]를 이용하여 시뮬레이션 하였다. K1 = K2일 경우 기존의 DES와 동일한 암/복호화 동작을 한다. 따라서 K1 =K2일 경우를 이용 그림 5-8과 같이 시뮬레이션하여 3-DES coprocessor를 검증하였다.

표 2. NIST의 DES 테스트 벡터

입 력 키 K1	10316E028C8F3B4A
입 력 키 K2	10316E028C8F3B4A
평 문	0000000000000000
암 호 문	82DCBAFBDEAB6602

그림 6은 표 2의 평문을 데이터 레지스터 영역에 쓰는 과정을 나타내고 있다.

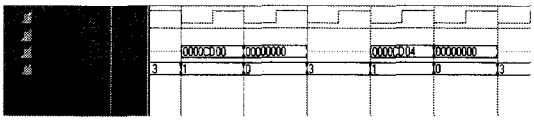

그림 6. 64비트의 평문 쓰기

그림 7은 표 2의 입력키 K1을 키 레지스터 영역에 쓰는 과정을 나타내고 있다.

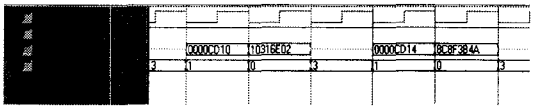

그림 7. 64비트 키 값 K1 쓰기

그림 8은 표 2의 입력키 K2를 키 레지스터 영역에 쓰는 과정을 나타내고 있다.

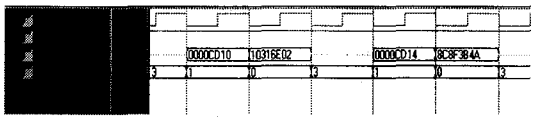

그림 8. 64비트 키 값 K2 쓰기

그림 9는 암호화된 암호문을 읽어오는 과정을 나타내고 있다.

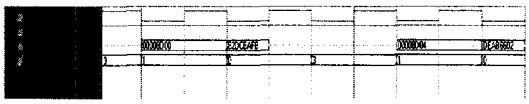

그림 9. 암호화된 데이터 읽기

NIST 테스트 벡터를 이용한 위의 시뮬레이션 결과로 본 논문에서 설계한 3-DES coprocessor를 검증할 수 있었다.

4.2 합성

합성은 Fujitsu의 CS66_uc_core 라이브러리를 이용하였으며, Synopsys사의 Design Compiler를 사용하였다. 그림 10은 3-DES의 합성 결과를 나타내고 있다. 합성 결과 3-DES coprocessor는 약 7,400개의 게이트로 구성되었다.

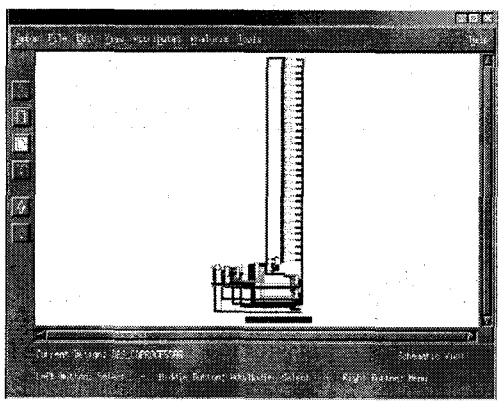

그림 10. 합성 결과

5. FPGA 구현 및 성능 분석

본 연구에서 설계한 3-DES coprocessor는 Xilinx의 FPGA 칩인 Virtex XCV300에 프로그램한 후, RS-232 통신을 이용하여 올바른 동작이 이루어짐을 확인하였다. 그림 11은 3-DES coprocessor의 검증에 사용된 FPGA를 이용한 보드이다.

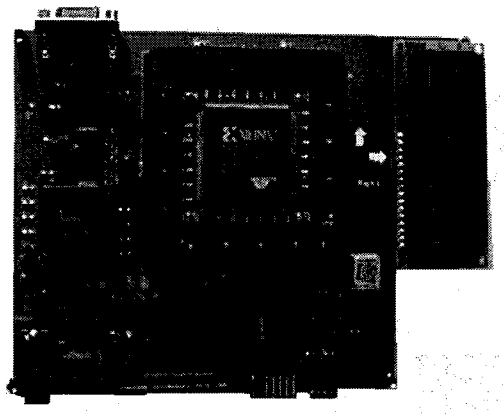

그림 11. 3-DES의 FPGA 구현

표 3은 3-DES coprocessor의 성능 분석을 나타낸다.

표 3. 3-DES의 성능 분석

게이트 수	약 7,400
최대 동작 주파수	70MHz
최대 성능	61.4Mbps
FPGA 칩	Virtex XCV300

6. 결론 및 향후 연구 방향

본 논문에서는 암호 알고리즘의 속도 및 안전성 문제를 향상시키기 위해 기존의 DES 알고리즘을 확장한 3-DES 알고리즘을 32 비트 데이터 버스를 이용한 하드웨어로 설계 및 구현하여 검증하고 성능 분석을 하였다. 그 결과 3-DES coprocessor는 약 7,400개의 게이트로 구성되며 61.4Mbps의 성능을 갖고 있음을 알 수 있었다.

향후 DES와 같은 블록 암호 알고리즘인 SEED와 비밀키 방식인 RSA, ECC 등도 설계하여 검증할 예정이다.

참고문헌

[1] 정진욱, 최병윤, "3중 DES와 DES 암호 알고리즘용 암호 프로세서의 VLSI 설계", 한국멀티미디어학회 춘계학술발표논문집, 2000.

[2] 이민섭, "현대암호학", 교우사

[3] 박창섭, "암호이론과 보안", 대영사

[4] FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), NIST