제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

SEED와 Triple-DES 전용 암호칩의 설계 및 구현

김 영 미† , 이 정 엽† , 전 은 아† , 정 석 원‡

† 고려대학교 정보보호대학원
‡ 목포대학교 정보공학부

요 약

본 논문에서는 SEED와 Triple-DES 알고리즘을 구현하는 통합 대칭키 암호칩을 설계하고 구현하였다. 시스템 설계 기술 언어인 VHDL(VHSIC Hardware Description Language)로 설계하였으며, 다양한 분야에 응용할 수 있도록 4가지 동작 모드를 지원한다. 자일링스(Xilinx)사의 Virtex-E XCV2000E BG560을 대상으로 설계하였으며 Xilinx Foundation Series 3.1i을 이용하여 기능 시뮬레이션과 타이밍 시뮬레이션을 통해 FPGA 구현 시 데이터의 암호화 복호화 결과를 확인하였다.

Design and Implementation of Crypto Chip for SEED and Triple-DES

Kim Yung Mi† , Lee Jung Youp† , Jun Eun A† , Jung Seok Won‡

† Center for Information Security Technology, Korea University
‡ Major in Information Security, Mokpo National University

ABSTRACT

In this paper a design and an implementation of a crypto chip which implements SEED and Triple-DES algorithms are described. We designed it by VHDL(VHSIC Hardware Description Language) which is a designed system-description language. To apply the chip to various application, four operating Modes such as ECB, CBC, CFB, and OFB are supported. The chip was designed by the Virtex-E XCV2000E BG560 of Xilinx and we confirmed result of it at the FPGA implementation by functional and timing simulation using the Xilinx Foundation Series 3.1i.

1. 서 론

디지털 정보사회가 고도화되고 전자상거래가 활성화됨에 따라 암호 기술의 활용은 특정분야의 특수기술에서 사회 경제의 기반기술로 크게 변화하고 있으며 정보보호의 중요성에 따라 암호 기술의 필요성이 증가하고 있다.

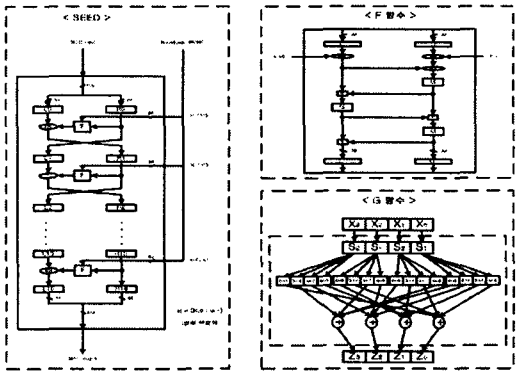
일반적으로 어떤 시스템에 암호화를 적용할 경우 소프트웨어 방식의 구현은 각종 컴퓨터 시스템이나 통신 시스템 속도를 지연시킨다. 계산의 복잡성과 동작 환경의 제약에 의하여 통신 속도를 따라가지 못하며, 불법적인 정보 유출 등의 보안에 있어서도 취약하게 된다. 따라서 실시간 통신이나 고속통신시스템의 안전한 관리를 위하여 고속의 암호화가 이루어져야 하며 각종 보안 서비스를 위하여 암호 알고리즘을 하드웨어로 구현한 암호 프로세서는 필수적이다.

본 논문에서는 전 세계적으로 널리 사용되는 Triple-DES와 국내 표준에서 국제 표준으로 채택된 SEED 블록 알고리즘을 동시에 구현한 암호칩을 설계하고 구현하였다. 2장에서 알고리즘의 구조를 설명하고 3장에서는 암호칩의 설계를 다루었다. 4장에서는 시뮬레이션의 결과와 성능 분석 결과를 기술하였으며 5장에서는 결론 및 향후 연구 방향을 제시하였다.

2. 알고리즘 구조

2.1 SEED 알고리즘

SEED 알고리즘 전체는 Feistel 구조로 이루어져 있으며, 128비트의 평문 블록에 64비트의 라운드 키를 적용하여 128비트의 암호문을 생성한다. Feistel 구조란 각각 t비트인 L_0, R_0 블록으로 이루어진 2t비트 평문 블록(L_0,R_0)이 r라운드($r \geq 1$)를 거쳐 암호문 (L_r,R_r)으로 변환되는 반복 구조를 말한다[2]. 그림 1과 같이 128비트의 입력 평문 블록을 2개의 64비트 블록 ($L_0(64)$, $R_0(64)$)으로 나누어, 라운드 키 k_i를 적용시킨 F함수를 거쳐 블록 ($L_1(64)$, $R_1(64)$)을 생성한다. 이 과정을 16라운드 수행하면 최종 128비트 암호문 블록 ($L_{16}(64)$, $R_{16}(64)$)이 출력된다.



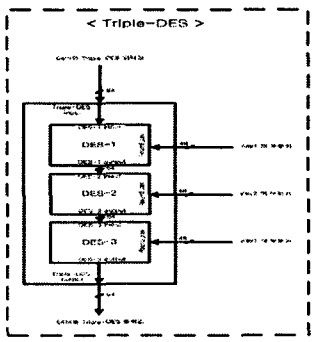
(그림 1) SEED 알고리즘

2.2 Triple-DES 알고리즘

네트워크와 하드웨어 기술 수준이 높아짐에 따라 안전성에 위협을 받게 된 DES의 대안으로서 안전성이 향상된 Triple-DES(3중 DES)가 나오게 되었다.

Triple-DES는 DES 알고리즘 자체에는 변화가 없으며, 2개의 서로 다른 키 k_1과 k_2를 이용하여 DES를 3번 수행한다. Triple-DES의 암호화, 복호화 알고리즘은 다음과 같다.

암호화	$c = E_{k1}(D_{k2}(E_{k1}(m)))$
복호화	$m = D_{k1}(E_{k2}(D_{k1}(c)))$

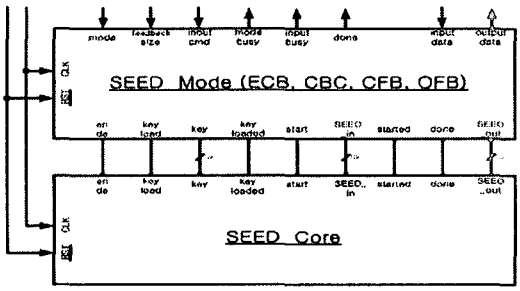


(그림 2) Triple-DES 알고리즘

3. 암호칩 설계

3.1 SEED의 설계

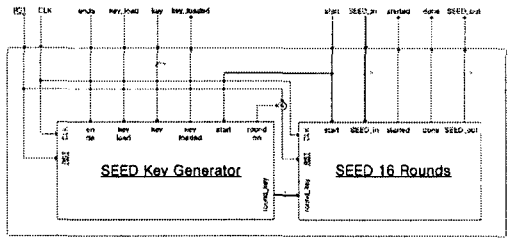
SEED는 Mode와 Core로 구분하였다. Mode는 각 운용 모드(ECB, CBC, CFB, OFB)를 처리하기 위해 XOR과 Shift 연산을 부가적으로 수행하는 모듈이다.



(그림 3) 운영 모드 통합된 SEED

Core는 SEED 알고리즘을 이용해 128비트 메시지를 암호화, 복호화 한다. 라운드 키를 생성하는데 사용하는 키 상수들은 16개 모두를 저장하지 않고, 1라운드의 라운드 키 생성에 필요한 키상수와 16라운드의 라운드 키 생성에 필요한 키상수만을 저장한다. 두 개의 키 상수에서 각각 1비트씩 left-shift, right-shift하면 다음 라운드에 필요한 키상수를 얻을 수 있기 때문이다.

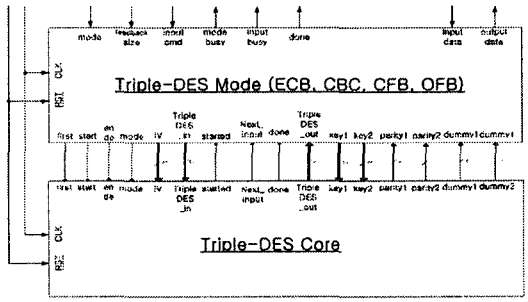
또한 별도의 레지스터를 장착하여 동일한 키로 암복화,복호화할 경우에는 새롭게 라운드 키 생성 과정을 수행할 필요가 없도록 설계하였다.



(그림 4) SEED Core

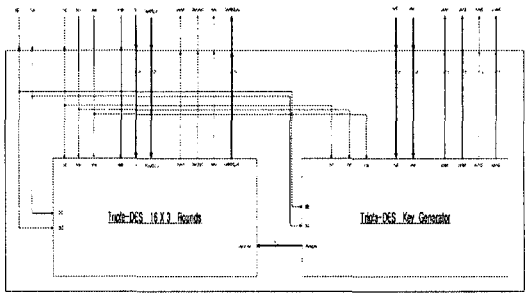
3.2 Triple-DES의 설계

Triple-DES는 Mode와 Core로 설계하였으며, Core는 16×3 Rounds와 Key Generator 모듈로 구성되어 있다.



(그림 5) 운영 모드 통합된 Triple-DES

16×3 Rounds는 DES의 1라운드 구조를 기본으로 하여 48회 반복 동작하게 된다. Key Generator 모듈은 라운드 키를 생성하는 모듈 2개로 구성되어 있으며, 이 중 하나의 모듈에는 16개의 레지스터가 연결되어 있다. 따라서 두 개의 키 중에서 복호화에 사용할 키는 레지스터가 있는 모듈에 대입하여 라운드 키를 생성하고 저장한다.



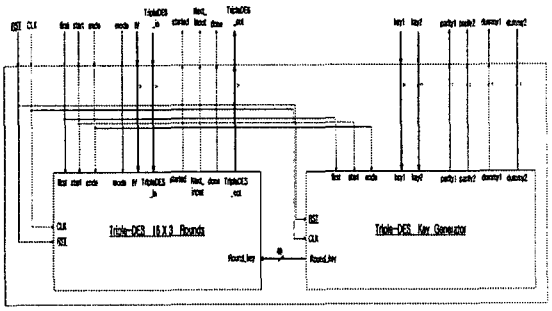
(그림 6) Triple-DES Core

Key Generator 모듈은 정해진 클럭에 입력값이 들어오지 않으면 더 이상의 암호화, 복호화를 진행하지 않는 것으로 간주하고 라운드 키 저장 레지스터를 리셋시킨다. 따라서 저장되어 있던 라운드 키를 삭제함으로써 보안 수준을 높일 수 있

다.

3.3 SEED와 Triple-DES 통합 모듈의 구조

SEED와 Triple-DES 알고리즘은 하나의 I/O를 공유한다. 알고리즘을 선택하는 특정 신호는 I/O에 입력하지 않는다. 그러나 레지스터를 enable 시키는 시그널이 서로 다르기 때문에 선택 알고리즘에 해당하는 내부버스와 레지스터만이 동작하게 된다.



(그림 7) SEED와 Triple-DES 통합 모듈

I/O 모듈은 처리 속도를 향상시키기 위하여 암호화와 복호화가 진행되는 동안에도 읽기와 쓰기를 함께 수행할 수 있도록 파이프라인 동작 구조로 설계하였다.

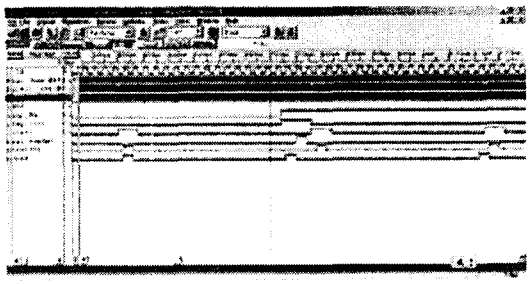
4. 시뮬레이션 결과 및 성능 분석

4.1 SEED 시뮬레이션 결과

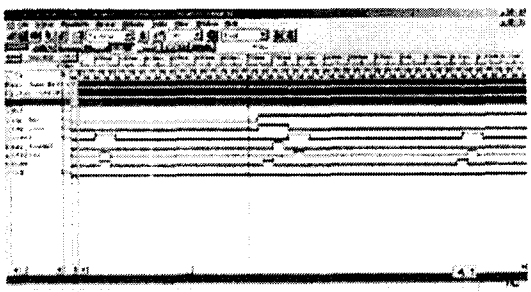
그림 8과 그림 9는 128비트의 평문 블록 2개를 ECB 모드로 암호화 한 후, 암호문 블록 2개를 ECB 모드로 복호화 한 기능 테스트(functional test)와 타이밍 테스트(timing test) 시뮬레이션 결과이다.

평문 "0x00010203040506070809OA0B0C0D0E0F", "0x5EBAC6E0054E166819AFF1CC6D346CDB"을 key "0x00000000000000000000000000000000"에 대하여 ECB 모드로 암호화하여 암호문 "0x5EBAC6E0054E166819AFF1CC6D346CDB", "0x448607CBC8551861E06D808CEC8FFE95"가 출력되는 것을 확인하였다.

암호문 "0x448607CBC8551861E06D808CEC8FFE95", "0x5EBAC6E0054E166819AFF1CC6D346CDB"을 key "0x00000000000000000000000000000000"에 대하여 ECB 모드로 복호화하여 평문 "0x5EBAC6E0054E166819AFF1CC6D346CDB", "0x00010203040506070809OA0B0C0D0E0F"가 출력되는 것을 확인하였다.



(그림 8) SEED 기능 테스트 시뮬레이션 결과

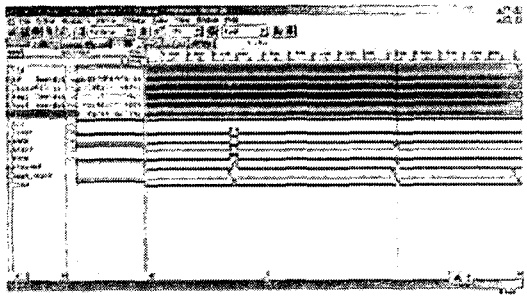


(그림 9) SEED 타이밍 테스트 시뮬레이션 결과

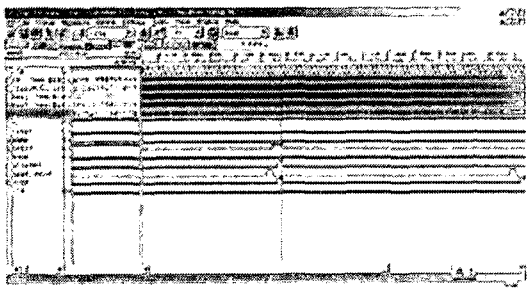
4.2 Triple-DES 시뮬레이션 결과

그림 10과 그림 11은 64비트의 평문 블록 2개를 CBC 모드로 암호화 한 후, 암호문 블록 2개를 CBC 모드로 복호화 한 기능 테스트와 타

이밍 테스트 시뮬레이션 결과이다.



(그림 10) Triple-DES 기능 테스트 시뮬레이션 결과



(그림 11) Triple-DES 타이밍 테스트 시뮬레이션 결과

평문"0x85e813540f0ab405", "0xce2cec156314cc8f", IV"0x85e813540f0ab405"을 key1"0xacbdfe1527384905"와 key2 "0x133457799bbcdff1"에 대하여 CBC 모드로 암호화하여 암호문 "0x62911200442c858a"와 "0xdaa64a47fd73518e"가 출력되는 것을 확인하였다.

암호문 "0xad2b13df47591c20", "0xacbdfe1527384905", IV"0x38bdfe1527384905"을 key1"0x85e813540f0ab405"와 key2 "0x133457799bbcdff1"에 대하여 CBC 모드로 암호화하여 평문 "0xf22fa70373a0739e"와 "0x0ef5ef40dff1531a"가 출력되는 것을 확인하였다.

4.3 성능 분석

본 연구에서 구현한 암호칩은 먼저 각각의 암호 알고리즘을 C언어를 이용하여 모델링한 후 VHDL로 설계하여 SEED와 Triple-DES의 테스트 벡터와 일치하는지 검증하였다. 자일링스(Xilinx)사의 Virtex-E XCV2000E BG560을 타겟 디바이스로 설정하고 FPGA Express Tool을 이용하여 컴파일하였다.

<표 2> 알고리즘의 성능 분석

	SEED	Triple-DES
게이트 수	35,397	26,044
동작 주파수	10.202 MHz	36.597 MHz
최대 성능	82 Mbps	49 Mbps
하드웨어 자원 활용률	11 %	7 %
최대 지연 시간	12.816 ns	12.234 ns
타겟 디바이스	Virtex-E BG560	XCV2000E

5. 결 론

본 논문에서는 SEED와 Triple-DES 블록 암호 알고리즘 전용 암호칩을 설계하고 이를 구현하였다. SEED와 Triple-DES는 ECB, CBC, CFB, OFB 4가지 동작 모드를 지원하며, 1라운드 동작을 1클럭에 수행한다. CFB와 OFB 모드는 최대 128비트/64비트(SEED/Triple-DES)까지 피드백할 수 있다.

SEED와 Triple-DES 코어 모듈은 정해진 시간 안에 암호화 또는 복호화를 진행하지 않으면 라운드 키 보관용 레지스터를 모두 리셋하도록 설계하였다. 암호칩을 사용하지 않을 경우에는 키 정보가 모두 삭제되도록 구현함으로써 보안 수준을 한 층 더 향상시켰다.

향후 연구 과제는 SEED와 Triple-DES와 같은 블록 암호 알고리즘 이외에도 인증에 사용되는 공개키 암호 알고리즘을 통합한 암호칩을 구현하는 것이다.

참고문헌

[1] FIPS PUB 46-3, "DATA ENCRYPTION STANDARD(DES)".
[2] 한국정보통신기술협회. TTA.KO-12.0004, "128-bit Symmetric Block Cipher(SEED).
[3] Stefan Sjoholm, "VHDL for Designers", PRENTICE HALL, 1997.
[4] Steve Trimberger, Raymond Pang, and Amit Singh, "A12Gbps DES Encryptor/Decryptor Core in an PFGA", CHES 2000.
[5] 한국정보보호센터, "128비트 블록 암호 알고리즘(SEED) 개발 및 분석 보고서", 1998.

김 영 미

2002년 경희대학교 수학과 (이학사)
2002년~현재 고려대학교 정보보호대학원 재학

이 정 엽

1998년 경북대학교 전자공학과 (공학사)
2000년 경북대학교 전자공학과 (공학석사)
2001년~현재 고려대학교 정보보호대학원 재학
2002년~현재 (주)스마트게이트팀장

전 은 아

1999년 원광대학교 전자공학과 (공학사)
2001년 원광대학교 전자계산교육 (교육학석사)
2003년~현재 고려대학교 정보보호대학원 재학

정 석 원

1991년 고려대학교 수학과(이학사)
1993년 고려대학교 수학과 (이학석사)
1997년 고려대학교 수학과 (이학박사)
2002~2003년 고려대학교 정보보호대학원 조교수
2004년~현재 목포대학교 정보공학부 교수