SEED Coprocessor의 설계 및 구현

김용범° 최홍묵 최명렬
한양대학교 전자전기제어계측공학과
{falcon20°, chmook, choimy}@asic.hanyang.ac.kr

Design and Implementation of SEED Coprocessor

YongBum Kim° HongMook Choi and MyungRyul Choi
Department of EECI, Hanyang University

요 약

본 논문에서는 한국 정보보호진흥원에서 개발한 128 비트 블록 암호 알고리즘인 SEED를 VHDL로 설계하였으며, FPGA의 구현으로 성능 분석을 하였다. 암호화 과정에서의 라운드 키 생성과정을 복호화 과정에서도 동일하게 적용할 수 있게 설계하여 처리속도를 향상시켰고 라운드키 생성과정과 F 함수에서 사용되는 5개의 G 함수를 하나의 G함수로 공유하여 게이트 수를 감소시켰다. Xilinx사의 Virtex XCV300 FPGA에 구현하였으며 합성결과 게이트 수는 10,610 개이고 최대 40MHz에서 동작하여 35.7Mbps로 암호화를 수행 할 수 있다.

1. 서 론

정보화 시대의 발전으로 위성 통신, CATV 등을 비롯하여, 전자 상거래 및 스마트 카드 등의 정보 통신 관련 산업이 발달하였다. 전자 상거래 및 인터넷을 통한 정보 서비스를 사용자들이 신뢰하며 사용하기 위해서는 정보 시스템의 보안과 처리 속도가 우선적으로 보장되어야 한다[1]. 그러므로 고속 통신 시스템에 암호화를 적용하거나 키를 안전하게 관리하기 위해서는 암호 알고리즘의 하드웨어 구현이 필요하다. 현재 널리 사용되고 있는 DES 암호 알고리즘은 고속 프로세서의 개발로 알고리즘 자체의 안전성에 위협이 되고 있는 상황이다[2]. 미국에서는 DES를 대신할 새로운 대칭형 암호 표준 AES가 사용될 예정이다[3]. 이러한 추세에 맞추어 한국에서도 독자적인 128비트 SEED 암호 알고리즘을 개발하여 표준으로 정하였다[4]. SEED 암호 알고리즘은 설계시 안전성을 고려하여 128비트 구조를 취하고 있으며 DES에 비해 복잡한 Feistel 구조를 갖고 있다. 그러나 SEED 알고리즘은 DES에 비해 안전성은 증가하였지만, 내부 구조의 복잡성으로 하드웨어 구조가 복잡하고 속도가 크게 떨어지는 단점이 있다. 따라서 칩 사이즈와 속도 측면에서 우수한 성능을 갖는 SEED 암호 프로세서 개발이 필요하다.

따라서 본 논문에서는 암호화 과정의 처리 속도를 향상시키고 칩 사이즈를 최소화하기 위한 하드웨어 구현방안을 제시하였다. 본 논문의 구성은 본론에 SEED 알고리즘의 구조를 알아보고 제안한 SEED Coprocessor에 대해 알아보겠다. 마지막으로 합성 후 결론에서 성능분석을 하였다.

2. 본 론

1. SEED 암호 알고리즘

1.1 전체구조

SEED는 대칭키 암호 알고리즘으로, 블록단위로 메시지를 처리하는 블록 암호알고리즘이다. 전체 구조는 그림 1과 같이 Feistel 구조로 이루어져 있으며 128비트의 평문 입력과 암호문 출력을 가진다. 128비트 평문 블록을 2개의 64비트 블록으로 나누고 우측의 64비트 블록은 64비트의 라운드 키와 함께 라운드 함수인 F 함수의 입력이 된다. 16개의 64비트 라운드 키를 이용하여 16라운드를 수행한 후, 최종 128비트 암호문 블록을 출력한다.

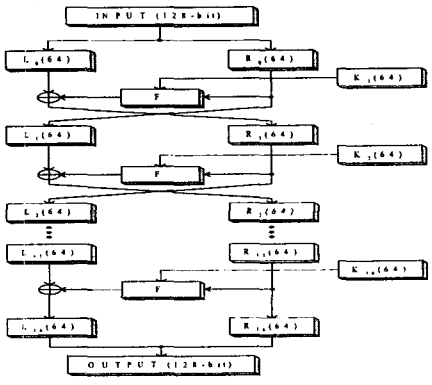


그림 1. SEED의 전체구조

1.2 라운드 함수 F

F 함수는 그림 2 와 같이 수정된 64 비트 Feistel 구조이고 입력은 각 32 비트 입력 2 개(C, D)와 64 비트 라운드 키 K_i ($K_{i,0}$;$K_{i,1}$)를 받아 32 비트 모듈로 연산과 G 함수를 적용하여 32 비트 출력 2 개(C', D')를 만든다.

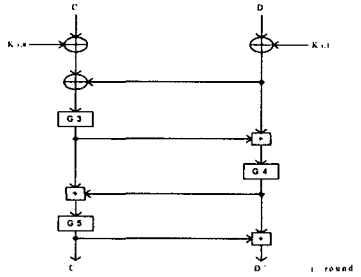


그림 2. F함수의 구조

1.3 G 함수

G 함수는 그림 3 과 같이 SEED 암호 알고리즘의 안전성을 구현하는 핵심 부분으로 2 쌍의 S1, S2 박스에 대한 테이블 룩업 동작, 마스킹 동작과 XOR 연산을 통해, 32 비트 출력을 생성한다. 실행과정은 입력 32 비트를 4 개의 블록으로 분할(a,b,c,d)한후 2 개의 S-Box(S1, S2)에 매핑하고 AND 연산과 XOR 연산을 취한다.

$a' = (S_1(a)\&m_0) \oplus (S_2(b)\&m_1) \oplus (S_1(c)\&m_2) \oplus (S_2(d)\&m_3)$
$b' = (S_1(a)\&m_1) \oplus (S_2(b)\&m_2) \oplus (S_1(c)\&m_3) \oplus (S_2(d)\&m_0)$
$c' = (S_1(a)\&m_2) \oplus (S_2(b)\&m_3) \oplus (S_1(c)\&m_0) \oplus (S_2(d)\&m_1)$
$d' = (S_1(a)\&m_3) \oplus (S_2(b)\&m_0) \oplus (S_1(c)\&m_1) \oplus (S_2(d)\&m_2)$
(m_0 = oxfc, m_1 = oxf3, m_2 = oxcf and m_3 = ox3f)

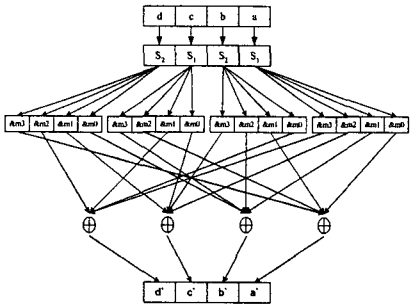


그림 3. G함수의 구조

1.4 라운드 키 생성과정

128비트의 마스터 키 또는 중간 라운드의 조정된 마스터키 값을 64비트씩 좌우로 나누어 블록을 8비트씩 좌우로 회전 이동시켜 재조정된 마스터 키를 생성함과 동시에 중간 라운드의 4개의 입력값(D,C,B,A)에 대해 32비트 모듈로 덧셈, 뺄셈 및 G 함수를 적용하여 그림 4와 같이 라운드 키(K_i)를 생성한다.

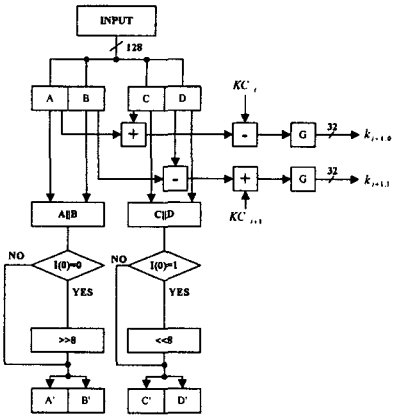


그림 4. 키 생성 블록의 구조

2. 제안한 SEED Coprocessor

제안한 SEED Coprocessor 는 16 비트 데이터 버스를 사용하고 그림 5 와 같이 콘트롤러, 콘트롤 레지스터, 데이터 레지스터, 키 레지스터와 클럭 생성기 블록으로 구성된다. 콘트롤러 블록은 SEED 의 암/복호화를 실행하기 위해 다른 블록에 콘트롤 신호를 제공한다. 콘트롤 레지스터는 시작 신호, 암/복호화 모드 선택 신호 그리고 SEED 코어 블록의 클럭 생성 제어 신호를 생성한다. 데이터 레지스터는 SEED 코어 블록에 128 비트 입력 데이터를 제공하고 키 레지스터는 SEED 코어 블록에 128 비트 입력 키값을 제공한다. 클럭 생성기 블록은 입력 클럭을 2 분주 4 분주하여 SEED 코어 블록에 제공한다.
SEED 코어 블록은 라운드 키를 생성하고 이 라운드 키와 입력받은 데이터 값으로 암/복호화를 실행한다.

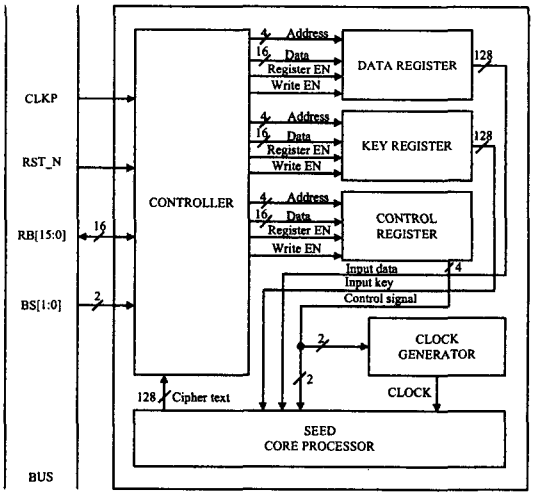
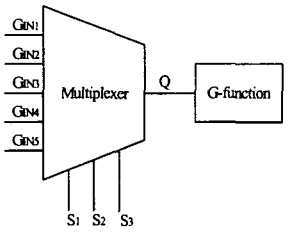


그림 5. 제안한 SEED Coprocessor 블록 구성도

표 1. 입출력 신호

Name	I/O	Function
CLKP	I	Clock
RST_N	I	Low active reset
RB[15:0]	I/O	R/W signal, Address/Data bus
BS[1:0]	I	Status of bus 00 : Data information 01 : Address and R/W information 10 : Not support 11 : Bus idle



Select signal	Q
S3S2S1	
000	GIN1
001	GIN2
010	GIN3
011	GIN4
100	GIN5
others	X

그림 6. G함수 공유

제안한 SEED Coprocessor는 그림 6과 같이 라운드 키 생성과정과 F함수에서 사용되는 다섯개의 G함수를 하나의 G함수로 공유해서 하드웨어 리소스를 감소시켰다. 또한 키 레지스터를 사용하지 않고 각 라운드마다 동시에 라운드키를 생성하여 하드웨어 리소스를 감소시켰다. 또한 암호화 과정에서의 라운드키 생성과정을 복호화시에도 동일하게 적용할 수 있게 설계하여 처리속도를 향상시켰다.

3. 시뮬레이션 및 합성 결과

본 논문에서 제안한 SEED Coprocessor는 Synopsys 툴을 사용하여 설계하였고 한국 정보보호진흥원에서 제공하는 테스트 벡터로 검증하였다. 제안한 SEED Coprocessor는 Fujitsu의 cs66_uc_core 라이브러리를 사용하여 합성한 결과 10,610 게이트로 구성되었다.

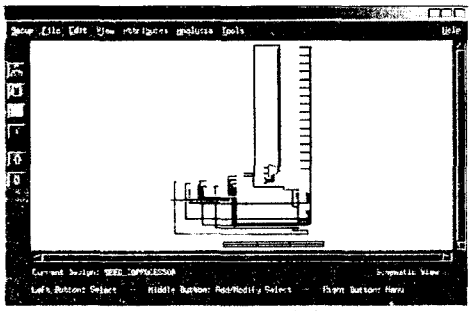


그림 7. 합성 결과

3. 성능 분석 및 결론

본 논문에서 제안한 SEED Coprocessor 는 Xilinx 의 FPGA 칩 Virtex XCV300 에 프로그램한 후, RS-232 통신을 이용하여 올바른 동작이 이루어짐을 확인하였다.

본 논문에서는 칩 사이즈를 최소화하기 위해 기존의 설계방식[7]에서 사용한 키 레지스터를 사용하지 않았으며 5개의 G함수를 1개의 G함수로 공유하였다. 또한 속도 향상을 위해 암호화의 라운드키 생성 방식을 복호화에도 동일하게 적용하였다. 이를 16비트 데이터 버스를 사용해서 하드웨어로 설계 및 구현하여 성능 분석을 하였다. 그 결과 제안한 SEED Coprocessor는 약 10,610 게이트로 구성되었으며 35.7Mbps의 성능을 갖고 있음을 알 수 있었다.

표 2. SEED Coprocessor의 성능분석

게이트 수	약 10,610
최대 동작 주파수	40MHz
최대 성능	35.7Mbps
FPGA 칩	Virtex XCV300

제안한 SEED Coprocessor는 위에 설명한 기존의 설계방식에 비해 칩 사이즈는 약 37% 줄었고, 속도는 14배 향상됐다.

4. 참고문헌

[1] William Stalling, Cryptography and Network Security, Prentice Hall, 1999.
[2] Jenes-Peter Kaps, High Speed FPGA Architecture for the Data Encryption Standard, Master Thesis, May, 1988.
[3] Kris Gaj, Pawel Chodowiec, " Comparison of the hardware performance of AES candidates using reconfigurable hardware" , Third AES candidate Conference, April, 2000.
[4] 한국 정보 보호 센터, 128 비트 블록 암호 알고리즘 (SEED) 개발 및 분석 보고서, 1998. 12.
[5] 이민섭, " 현대암호학" , 교우사
[6] 박창섭, " 암호이론과 보안" , 대영사
[7] Y. H. Seo, J. H. Kim, and D. W. Kim, " Hardware Implemen- tation of 128-bit Symmetric Cipher SEED" , AP-SIC 2000. Proceedings of the Second IEEE Asia Pacific Conference on, pp.183-186, 2000