SEED 암호 알고리즘을 이용한 암호 프로세서의 VLSI 설계

°정 진 욱, 최 병 윤
동의대학교 컴퓨터 공학과

VLSI Design OF Cryptographic Processor for SEED Encryption Algorithm

Jin-Wook Jung and Byeong-Yoon Choi
Department of Computer Eng., Dongeui University

Abstract

본 논문에서는 현재 우리나라 전자상거래 표준인 SEED 암호화 알고리즘을 하드웨어로 구현하였다. 이 암호화 프로세서는 유연성과 하드웨어 면적을 줄이기 위해 파이프라인이 없는 1 unrolled loop 구조를 사용하였다. 그리고 ECB, CBC, CFB, OFB의 4가지 모드를 모두 지원할 수 있도록 하였다. key computation은 오버헤드를 감소시키도록 precomputation 기법을 사용하였다. 또한, 데이타 입·출력 시 증가되는 처리시간을 제거하기 위하여 외부 입·출력 레지스터와 data 입·출력 레지스터를 분리하여 데이타 입·출력 연산이 암호 프로세서의 암호화 연산과 병행하여 처리되도록 하였다. 암호 프로세서는 0.25㎛ CMOS 기술을 사용하여 검증하였고 gate수는 대략 29.3K gate 정도가 소요되었으며, 100 Mhz ECB 모드에서 최고 237 Mbps의 성능을 보였다.

I. 서 론

현재 보안이란 문제가 거론되지 않는 분야가 없을 정도로 암호화 분야는 널리 이용되고 있다.

정보 보호 기술은 위성 통신, CATV 등을 비롯하여, 각종 통신 이용 산업 및 인터넷 전자 문서교환(EDI, Electronic Data Exchange)을 포함하는 전자상거래(EC, Electronic Commerce), 스마트 카드 등의 거의 모든 정보 통신 관련 산업 분야에서 요구되고 있다. 특히 전자 상거래 및 인터넷을 통한 정보 서비스의 사용자정보에 대한 불법적인 유출을 막기 위해서는 정보 시스템의 보안과 처리 속도가 우선적으로 보장되어야 한다. 현재 사용되고 있는 암호화 알고리즘의 문제점들이라면 속도와 해킹에 대한 방어대책 등을 지적할 수 있을 것이다. 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 보다 안전한 관리를 위해서는 암호 알고리즘의 하드웨어 구현이 필요하다고 생각한다.

세계 각국은 인터넷을 이용한 전자상거래를 21세기 국가 경쟁력을 결정하는 중요한 요소로 간주하여, 국가 전략적으로 전자 상거래의 활성화를 위해 많은 노력을 경주하고 있다. 현재 한국에서도 독자적인 128비트 블록 암호 알고리즘인 SEED 암호 알고리즘을 개발하여 표준으로 정하였다.

본 논문에서는 현재 한국 전자상거래 표준인 SEED 암호 알고리즘을 이용한 암호 프로세서를 설계하였으며, 프로세서의 성능을 구조적인 측면에서 성능을 비교·분석하였다.[1]

II. SEED 암호 알고리즘

SEED 암호 알고리즘은 Feistel 구조로 이루어져 있으며, 128비트의 평문과 128비트의 키를

입력 받고, 입력된 128비트의 키는 64비트의 라운드 키(16개)를 생성하고, 16라운드를 거치면서 128비트의 암호문을 생성한다. 그림 1은 SEED 암호 알고리즘의 전체 구조를 나타낸다.

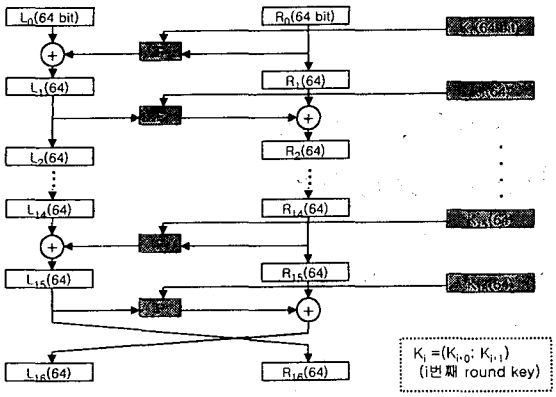

그림 1 SEED 암호 알고리즘의 구조

128비트 블록은 2개의 64비트 블록(L_0(64), R_0(64))으로 나누어, 16라운드 동작을 수행한 후, 최종 128비트 출력(L_{16}(64), R_{16}(64))을 생성한다. SEED 암호 알고리즘의 F 함수는 안전성을 향상시키기 위해 같은 블록 암호화 알고리즘인 DES에 비해 훨씬 복잡한 구조를 갖고 있다. 따라서 이러한 F 함수가 갖는 복잡성으로 인해 SEED는 DES와 비교하자면 속도가 크게 떨어지며, 하드웨어 면적도 상당히 요구된다. F함수 내부에 있는 G 함수는 4개의 $2^8 \times 8$ Lookup table과 XOR 회로로 구성된다. 반면 SEED의 키 생성 알고리즘은 128비트의 암호키를 64비트씩 좌우로 나누어 모듈로 덧셈과 뺄셈, G 연산을 통해 64비트 라운드 키를 생성한다.

III. 암호 프로세서의 VLSI 설계

본 연구의 암호 프로세서는 외부 호스트 프로세서에 대한 암호 보조 프로세서 형태로 설계되어, 다양한 컴퓨터 시스템 환경에 접속이 가능하도록 개발되었다. 그림 2는 암호 보조 프로세서의 전체 구조를 나타낸다. 외부의 데이터 버스를 통해 키와 초기값(IV : Initial Value), 입력 데이터를 입력한다. 단, 입출력 시간에 따른 성능 저하를 방지하기 위해, 데이터 입 · 출력 레지스터(I/O Reg)와 내부 암호 모듈의 입출력 레지스터(DIN/OUT Reg)을 분리시켜, start신호 발생시, 이전 데이터의 암호화 결과와 새로운 입력 데이터가 서로 swap되는 동작을 수행한다. 그리고 암호 연산 수행 동안 Busy Flag가 High상태로 되어, 암호 동작이 진행 중임을 나타낸다. Busy가 High인 동안 Host Processor는 암 · 복호화 할 새로운 데이터를 IOR에 두고, Busy가 0이 될 때까지 대기한다. 그리고 외부 Host 프로세서가 8 비트, 16비트, 32 비트 등의 다양한 시스템이 가능 할 수 있도록 data_in_out 모듈은 외부 Host 시스템의 특성에 맞게 databus[n-1:0]으로 데이터가 전달될 수 있도록 하는 기능을 담당한다. 여기서 n은 지원하는 Host 프로세서의 데이터 버스 크기를 나타낸다.

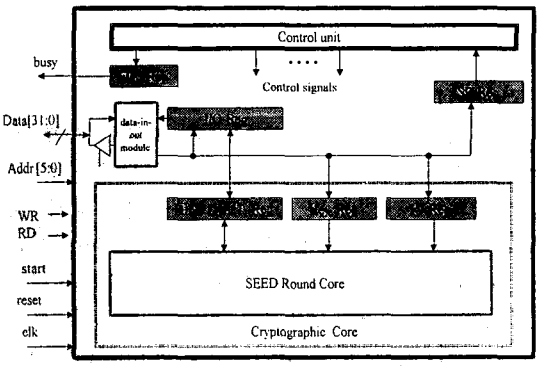

그림 2 암호 프로세서 구조

SEED Core는 데이터 Round Core와 Key Round Core로 구성된다. 여기서 SR 레지스터와 Flag F/F을 제외한 모든 레지스터는 128비트를 가진다.

본 연구에 사용되는 암호 프로세서는 ECB, CBC, CFB, OFB의 4가지 모드를 구현하기 위해, 1라운드 구조의 하드웨어를 배치하고 16라운드 동안 반복적으로 사용하는 구조(1 unrolled loop structure)를 사용하였다. 그러나 SEED 암호 알고리즘은 F 함수가 복잡하고, 키 생성과정에 많은 시간이 소요되어, 1 clock로 1 round를 구현하는 방식은 많은 하드웨어 면적을 요구하고, 클럭 주파수를 감소시켜 성능을 저하시킨다.
따라서, 본 연구에서는 SEED 라운드 동작을 3개의 클럭으로 구현하였고, Key computation 방식r은 이전 round에서 사전계산(precomputation)하는 방식[4]을 사용하였다.

그림 3은 3개의 클럭으로 SEED의 1라운드를 구현하는 방식을 나타낸다. 이러한 기법은 하드웨어 공유를 극대화시켜 각 클럭당 1개의 G 함

수만 필요하게되어 하드웨어면적을 1 round/ 1 clock 방식에 비해 2/3 정도 감소시킬수 있었다. 그리고 round Key 계산 동작은 online 계산 방식으로 내부적인 파이프라인 처리를 통해 3개의 클럭과 1개의 G와 1개의 3-operand adder로 구현하였다.

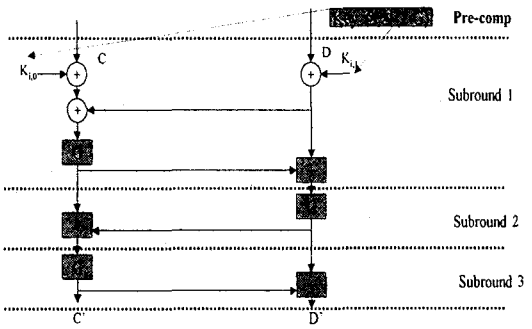

그림 3 SEED 1 round당 3 clock으로 구현하는 방법

그림 4는 SEED Round Core를 나타내었다.

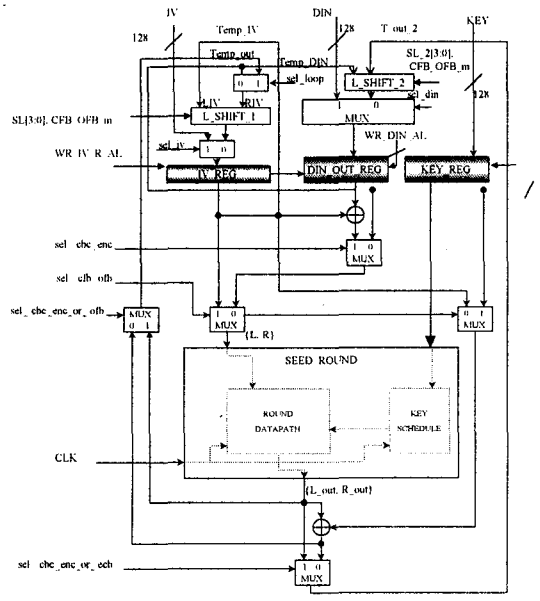

그림 4 SEED Round Core 구조

제어 회로는 암호 알고리즘에 따라, 동작 흐름을 ASM(Algorithmic State Machine) Char로 표현한 후, 이를 F/F당 하나의 상태를 할당하는 방식(one-hot assignment) 방식으로 FSM(finite state machine)을 구현하여 제어회로를 구현하였다.

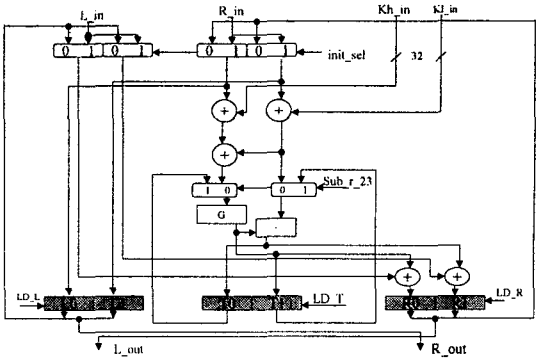

그림 5 SEED 알고리즘의 Round Datapath

그림 5는 SEED Round datapath를 나타내었다. 라운드당 클럭수를 3으로 하여 G함수와 adder를 하나만 사용하도록 하는 구조를 가졌다. 라운드당 3번의 G함수와 3번의 adder 연산이 사용되는 것을 하드웨어적으로는 clock당 하나의 G함수와 adder를 사용하고 그것을 3번 반복하는 구조로 하드웨어 면적을 축소 시켰다.

Ⅳ. 검증, 성능 분석 및 결론

본 연구에서 설계한 암호 프로세서는 먼저 SEED 암호 알고리즘을 C 언어로 모델링 한 후, 이를 Verilog HDL 언어로 변환하여, 2가지 동작이 일치하는 지 확인하는 과정을 사용하였다. 이러한 검증 동작 후에 설계된 회로는 0.25 ㎛ CMOS 라이브러리를 사용하고, Synopsys Tool을 사용하여 합성하였다. 합성결과 동작을 합성한 회로가 올바로 동작함을 확인하였고 최악 동작 경로는 9.38ns 이었다. 표 1은 Round당 Clock수에 따른 성능비교이다. 표 1에 따르면 본 연구의 SEED 구현 방식은 고속으로 동작함과 동시에 하드웨어 면적 측면에서도 효율적인 구조임을 알수 있다. 표 2는 설계한 암호 프로세서의 특성과 성능을 나타낸다. 표 1과 2를 종합해보면 본 연구의 암호프로세서는 면적과 동작 측면에서 기존 방식에 비해 우수한 구조를 가지고 있음을 알 수 있다.

표 1 SEED 암호 알고리즘의 구현방식 비교

방식	G함수 수	S box 수	성능 (클럭수, ECB경우)	주요특징
1 round/ 1 clock	5	20	16	-low freq
1 round/ 4 clock	3	12	64	-많은 수의 클럭 요구
1 round/ 3 clock (본 연구)	2	18	48+3	-high freq -key 사전 계산

표 2 SEED 암호알고리즘의 전기적 특성

지원 암호알고리즘	SEED @ECB, CBC CFB, OFB
라운드당 클럭 수	3
S 박스 구조	2진 lookup table ($2^8 \times 8$)
게이트 수	약 29,300
동작 주파수	100 ㎒
라운드 키 계산	online precomputation
I/O 동작 방식	background Input/Output
외부인터페이스	8/16/32 bit
암 · 복호화 단위 (J)(@CFB, OFB)	8/16/32/64/128 bit
암 · 복호화 율	237 Mbps @ ECB, CBC 237 Mbps @ CFB, OFB (J = 128) 16 Mbps @ CFB, OFB (J = 8)

V. 결 론

본 연구에서는 SEED 암호 알고리즘을 VLSI로 구현한 암호 프로세서를 설계하였다. 설계항 암호 프로세서는 4가지 동작모드(ECB, CBC, CFB, OFB) 모드를 모두 지원함과 함께 다양한 외부 호스트 컴퓨터에 인터페이스 할 수 있는 구조를 가지고 있다. 키 계산 방식으로는 키 사전 계산 기법을 이용함으로써, 라운드 키 계산 동작이 라운드 datapath의 동작주파수를 감소시키는 문제를 제거하였다. 또한 3개의 클럭을 사용하여, 1개의 라운드를 구현함에 의해서, 하드웨어 공유를 극대화 시킬 뿐만 아니라, 그와 동시에 높은 주파수 특성을 유지할 수 있었다.

이러한 구조적인 특성으로 본 연구에서 설계한 암호 보조 프로세서는 SEED 암호 알고리즘이 적용되는 Network, 전자상거래 등의 보안모듈로 사용할 수 있을 것이며 대칭키 암호 알고리즘이 필요한 다양한 암호 응용분야에 적용할 수 있을 것으로 판단된다.

앞으로는 인터넷보안에 가장 널리 이용되는 RSA 암호 알고리즘과 곧 확정될 AES 표준안이 나오면 이 두가지 암호 알고리즘을 구현하는 프로세서 연구가 필요할 것이라고 본다.

참고 문헌

[1] 한국 정보 보호 센터, 128비트 블록 암호 알고리즘(SEED) 개발 및 분석보고서, 1999

[2] Feistel, "Cryptography and Computer Privacy", Scientific American, May, 1973.

[3] 정진욱, 최병윤, "3중 DES와 DES 암호 알고리즘용 암호프로세서의 VLSI 설계", 2000년도 한국 멀티미디어 학회, 춘계 학술 발표 대회 논문집, pp.117-120, 2000. 5

[4] 정진욱, 최병윤 "SEED 와 TDES 암호 알고리즘을 구현하는 암호 프로세서의 VLSI 설계", 2000년도 대한전자공학회, 하계 종합 학술대회 논문집 II, pp.169-172, 2000. 6