SEED 와 TDES 암호 알고리즘을 구현하는 암호 프로세서의 VLSI 설계

°정 진 욱, 최 병 윤
동의대학교 컴퓨터 공학과

VLSI Design OF Cryptographic Processor for SEED and Triple DES Encryption Algorithm

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

Abstract

This paper describes design of cryptographic processor which can execute SEED, DES, and triple DES encryption algorithm. To satisfy flexible architecture and area-efficient structure, the processor has 1 unrolled loop structure with hardware sharing and can support four standard mode, such as ECB, CBC, CFB, and OFB modes. To reduce overhead of key computation, the precomputation technique is used. Also to eliminate increase of processing time due to data input and output time, background I/O technique is used which data input and output operation execute in parallel with encryption operation of cryptographic processor. The cryptographic processor is designed using 2.5V 0.25 μm CMOS technology and consists of about 34.8K gates. Its peak performances is about 250 Mbps under 100 Mhz ECB SEED mode and 125 Mbps under 100 Mhz triple DES mode.

1. 서 론

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 보다 안전한 관리를 위해서는 암호 알고리즘의 하드웨어 구현이 필요하다. 현재 보편적으로 널리 사용되고 있는 DES(Data Encryption Standard) 암호 알고리즘은 고속 프로세서의 개발로 알고리즘 자체의 안전성에 위협이 되고 있는 상황이다. 이에 대한 대안으로 제안된 방법 중 한가지인 3중(Triple) DES(TDES) 암호 알고리즘은 거의 안전한 것으로 평가되고 있다[1]. 그리고 세계 각국은 인터넷을 이용한 전자 상거래를 21세기 국가 경쟁력을 결정하는 중요한 요소로 간주하여, 국가 전략적으로 전자 상거래의 활성화를 위해 많은 노력을 경주하고 있다. 이러한 추세에 맞추어 한국에서도 독자적인 128 비트 SEED 암호 알고리즘을 개발하여 표준으로 정하였다[2].

따라서 본 연구에서는 다양한 응용 분야와 안전성, 기존 시스템과의 호환 등을 고려하여, SEED, DES 암호 알고리즘과 3중 DES 암호 알고리즘을 모두 구현하는 암호 프로세서를 설계하였으며, 프로세서의 성능을 구조적인 측면에서 성능을 비교·분석하였다.

2.SEED, DES와 TDES 암호알고리즘

3가지 암호 알고리즘 중 상대적으로 소개가 되어 있지 않은 SEED 암호 알고리즘을 중심으로 암호 알고리즘을 간단히 살펴본다. SEED 암호 알고리즘 전체 구조는 Feistel 구조로 이루어져 있으며, 128 비트의 평문과 128 비트 키를 입력으로 받아서, 128 비트 키에서 생성된 64비트 라운드 키(16개)를 입력으로 받아, 총 16 라운드를 거쳐 128 비트 암호문을 생성한다. 그림 1은 SEED 암호 알고리즘의 전체 구조를 나타낸다. 128 비트 블록은 2개의 64비트 블록(Lo(64), Ro(64))으로 나누어, 16 라운드 동작을 수행한 후, 최종 128 비트 출력($L_{16}(64)$, $R_{16}(64)$)을 생성한다. SEED 암호 알고리즘의 F 함수는 안전성을 향상시키기 위해 DES 암호 알고리즘에 비해 훨씬 복잡한 구조를 갖고 있다. 따라서 이러한 F 함수가 갖는 복잡성으로 SEED는 DES에 비해 속도가 크게 떨어지며, 면적인 많이 필요한 구조적인 문제를 갖고 있다. F 함수 내부에 있는 G 함수는 4개의 $2^8 \times 8$ lookup table과 XOR 회로로 구성된다. 반면 SEED의 키 생성 알고리즘은 128 비트의 암호키를 64비트씩 좌우로 나누어 모듈로 덧셈과 뺄셈, G 연산을 통해 64 비트 라운드 키를 생성한다.

반면 DES 암호 알고리즘은 다양한 Permutation과 Substitution을 통해, Shannon이 제안한 이상적인 암호 시스템의 Diffusion과 Confusion의 근사적인 특성을 구현한다. DES 암호 알고리즘은 SEED와 유사한 Feistel 구조를 갖지만, 입출력 부분에 데이터 정렬(permutation) 부분이 추가로 존재하며, 64-비트 데이터와 64비트 키(패리티 비트 8비트 포함)를 갖는 암호 알고리즘이다. 다중 DES 암호 방식은 기존 DES 알고리즘을 반복적으로 적용하여 보안을 강화한 구조이다. 그리고 대칭형 암호 알고리즘의 경우 안전도와 Stream Cipher 응용을 고려하여, 4가지 동작 모드의 구현을 필요로 한다[3,4].

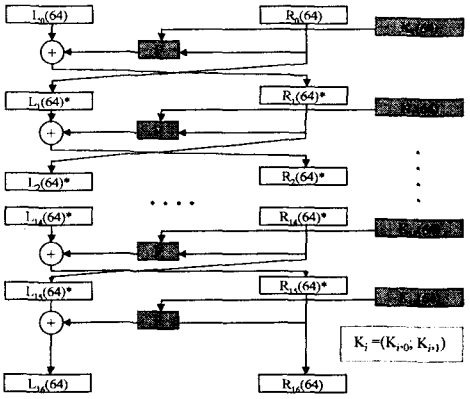

그림 1 SEED 암호 알고리즘의 구조

3. 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) 과 내부 암호 모듈의 입출력 레지스터(DIN/OUT Reg)을 분리시켜, start신호 발생 시, 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 가능할 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. (SEED+DES) Core는 데이터 Round Core와 Key Round Core로 구성된다. 여기서 SR 레지스터와 Flag F/F을 제외한 모든 레지스터는 128 비트를 갖는다. DES, TDES와 SEED가 하드웨어를 공유하

면서 4가지 동작 모드를 구현하기 위해서, DES와 3중 DES의 경우 입력값 64비트가 IOR에서 DIN_OUT 레지스터로 swap될 때 상위 64비트에도 동일 값으로 복사된다.

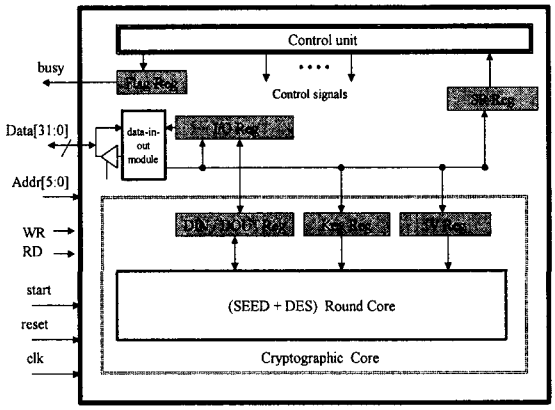

그림 2 암호 프로세서 구조

4가지 모드를 구현하기 위해, 1 round 구조의 하드웨어를 배치하고 16 라운드 동안 반복적으로 사용하는 구조(1 unrolled loop structure)를 사용하였다. 그러나 SEED 암호 알고리즘의 경우 F 함수가 복잡하고, 키 생성과정에 많은 시간이 소요되므로, DES와 TDES와 같이 1 클럭으로 1 round를 구현하는 방식은 많은 하드웨어가 소요되며, 클럭 주파수를 감소시켜 DES와 TDES의 성능도 동시에 낮추게 되는 문제를 야기시킨다. 따라서 본 연구에서는 SEED 라운드 동작을 3개의 클럭으로 구현하고, 키 계산은 이전 round에 사전계산(precomputation)하는 방식[5]을 사용하였다. 그림 3은 3개의 클럭으로 SEED의 1 round를 구현하는 방식을 나타낸다. 이러한 기법은 하드웨어 공유를 극대화시켜 각 클럭에 1개의 G 함수만 필요하게 되어 하드웨어 면적을 1 round/1 clock 방식에 비해 2/3 정도 감소시킬 수 있었다. 그리고 라운드 키 계산 동작은 online 계산 방식으로 내부적인 파이프라인 처리를 통해 3개의 클럭과 1개의 G와 1개의 3-operand adder로 구현하였다. 그림 4는 (SEED+DES) Round 코어를 나타낸다.

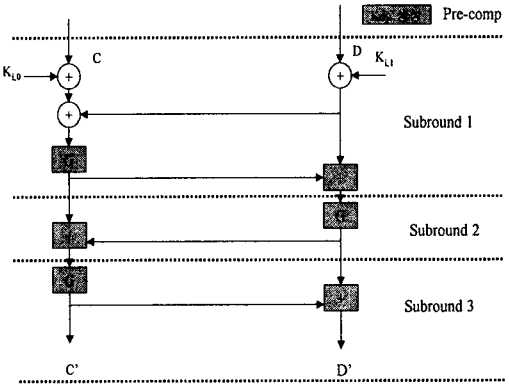

그림 3 SEED 1 round를 3개의 클럭으로 구현하는 방법

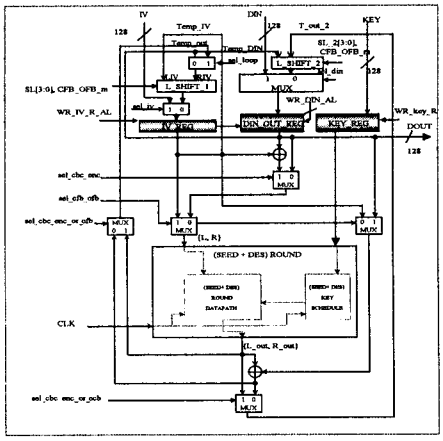

그림 4. SEED_DES Round Core 구조

제어 회로는 SEED, DES 와 3중 DES 암호 알고리즘에 따라, 동작 흐름을 ASM(Algorithmic State Machine) Chart로 표현한 후, 이를 F/F당 하나의 상태를 할당하는 방식(one-hot assignment) 방식으로 FSM(finite state machine)를 구현하여 제어 회로를 구현하였다.

4. 검증 및 성능 분석

본 연구에서 설계한 암호 프로세서는 먼저 암호 알고리즘을 C 언어로 모델링 한 후, 이를 Verilog HDL 언어로 변환하여, 2가지 동작이 일치하는 지

확인하였다. 그리고 설계한 회로는 0.25um CMOS 공정으로 Synopsys tool로 합성한 후 동작을 합성한 회로가 올바로 동작 함을 확인하였다. 최악 경로는 약 9.38ns 이었다. 표 1은 SEED 암호 알고리즘의 여러 가지 구현 방식을 비교하였다. 표 1에 따르면 본 연구의 SEED 구현 방식은 고속으로 동작함과 동시에 면적 측면에서 효율적인 구조임을 알 수 있다. 표 2는 설계한 암호 프로세서의 특성과 성능을 나타낸다. 표 1과 2을 보면 본 연구의 암호 프로세서는 면적과 동작 측면에서 기존 방식에 비해 우수한 구조를 갖고 있음을 알 수 있다.

표 1. SEED 암호 알고리즘의 구현 방식 비교

방식	G 함수 수	S box 수	성능 (클럭수) @ECB	주요 특징
1 round/ 1 clock	5	20	16	-low freq.
1 round/ 4 clocks	3	12	64	-많은 수의 clock 필요
1 round/ 3 clocks (본 연구)	2	8	48 + 3	-high freq. -key 사전 계산

표 2. 암호 프로세서의 특징

지원 알고리즘	SEED, DES, TDES
동작 모드	ECB, CBC, CFB, OFB
게이트 수	약 34,800
round key 계산	online precomputation
I/O 동작	background Input/Output
외부 인터페이스	8/16/32-bit
암·복호화 단위(J) @CFB, OFB	8/16/32/64/128 @SEED 8/16/32/64 @DES, TDES
암·복호화 율	250 Mbps @ECB, SEED 125 Mbps @ECB, TDES 400Mbps @ECB, DES
동작주파수	100 Mhz
사용 공정	0.25 μm CMOS
전 원	2.5 Volt

5. 결 론

본 연구에서는 DES, 3중 DES, SEED 암호 알고리즘을 단일 칩에 구현한 암호 프로세서를 설계하였다. 설계한 암호 프로세서는 4가지 동작 모드(ECB, CBC, CFB, OFB) 모드를 모두 지원함과 함께 다양한 외부 호스트 컴퓨터에 인터페이스할 수 있는 구조를 갖고 있다. 3가지 암호 알고리즘에 모두 키의 사전 계산 기법을 사용함으로서, 라운드 키 계산 동작이 라운드 datapath의 동작 주파수를 감소시키는 문제를 제거하였다. 또한 입출력 동작을 암호 동작에 대해 background로 수행하도록 하여, 입출력의 overhead를 제거하였다. 특히 SEED 암호 알고리즘의 경우 3개의 클럭을 사용하여, 1개의 round를 구현함에 의해서, 하드웨어 공유를 극대화시킴과 동시에 높은 동작 주파수의 특성을 유지할 수 있었다. 그리고 내부 round 코어를 제외한 부분은 SEED, DES, TDES가 모두 하드웨어를 공유할 수 있도록 하여, 최소의 게이트수로 3가지 암호 알고리즘을 구현할 수 있었다. 설계한 암호 프로세서는 현재 전자상거래 등 대칭키 암호 알고리즘이 필요한 다양한 암호 응용 분야에 적용 할 수 있을 것으로 판단된다.

참고 문헌

[1] 최 병 윤, "암호프로세서용 제어기 설계", ETRI 과제 최종 보고서, 1999.11

[2] 한국 정보 보호 센터, 128 비트 블록 암호 알고리즘(SEED) 개발및 분석보고서, 1999

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

[4] National Bureau of Standards, DES Modes of Operation, Federal Information Processing Standards Publication FIPS PUB 81, December 1980

[5] 정진욱, 최병윤, "3중 DES와 DES 암호 알고리즘용 암호 프로세서의 VLSI 설계", 2000년도 한국 멀티미디어 학회, 춘계 학술 발표대회 논문집, pp.117-120, 2000.5