SEED 블록 암호 알고리즘의 파이프라인 칩 설계에 관한 연구

이규원[0], 엄성용
이랜드시스템스 3G연구소, 서울여자대학교 컴퓨터학과
(leekw@elandsystems.com, osy@swu.ac.kr)

A Study on Pipeline Chip of SEED Block Cipher Algorithm

Kyu-Won Lee[0], Seong-Yong Ohm
3G Labs, Elandsystems, Dept. of Computer Science, Seoul Women's University

요 약

본 논문에서는 한국정보보호 진흥원에서 표준으로 개발한 128비트 블록암호 알고리즘의 표준인 SEED를 하드웨어 칩으로 설계 연구하였다. 설계 연구 방법은 기존 암호 연산부의 속도 개선의 한 방법으로 암호 블록의 16 라운드 각각을 하나의 프로세서로 보고, 이를 파이프라인 방식으로 설계하여 암호 연산의 속도를 증진시키는 방법으로 설계하였다. Cadence의 NCVHDL로 Functional Simulation하고, Synopsys의 Compiler II 로 Optimize 된 Schematic을 검증하였다.

1. 서론

일반적으로 블록 암호 알고리즘은 기밀성 서비스 제공의 중요 수단으로 전자 상거래에서의 안전성 확보에 필수 불가결한 요소 기술이다. 우리나라에서는 국내 표준 암호 알고리즘으로 128비트 블록암호 알고리즘 SEED를 1998년에 개발 발표하였다. 현재 국내 보안 업체 및 하드웨어 설계 업체에서는 SEED 암호 알고리즘을 지원하는 암호 프로세서를 기반으로 보안 솔루션 등이 개발 중에 있으며, 스마트 카드등에 응용하고 있다. [1]

본 논문의 목적은 기본적으로 소프트웨어 기반의 단점인 보안에 소요되는 시간을 최소화하고, 보안 강도는 유지하면서 암호화에 소요되는 시간을 최소화하는 블록 암호 알고리즘 SEED를 설계하는 것을 목표로 하여 SEED의 암호부를 파이프라인 구조로 설계한다.

이는 두 가지 의미를 지니는데 첫째로, 하드웨어 프로그래밍에 의한 칩(chip) 구현에서 얻을 수 있는 장점인 모듈화를 통해 범용적인 재사용이 용이하다는 것과, 성능측면에서 보다 만족스러운 결과를 얻을 수 있다는 것, 그리고 제품의 소형·경량화에 유리하다는 점등이다. 둘째로, 기존에 SEED를 구현한 연구의 대부분은 칩의 면적을 최소화를 목표로 한 것과 one chip을 목표로 한 것이 대부분이었다. 그러나 본 논문에서는 속도개선에 주안점을 두어 파이프라인 구조로 설계한다는 점이다

2. 관련 연구 및 연구방향

2.1 블록 암호 알고리즘

대부분의 블록 암호알고리즘은 Feistel 구조로 설계되고 있다(DES, FEAL, LOKI, MISTY, Blowfish, CAST, Twofish 등). Feistel 구조란 각 t비트인 L0, R0 블록으로 이루어진 2t비트 평문 블록(*L0, R0*)을 r라운드($r \geq 1$)를 거쳐 암호문 (Lr, Rr)을 내는 반복구조를 말한다. 반복구조란 평문 블록이 몇 번의 라운드를 거쳐 암호화를 수행하는 것을 말하고, 라운드($1 \leq i \leq t$)란 암호키 K로부터 유도된 각 서브키 Ki(또는, 라운드 키라 불림)를 중요 입력으로 하는 $Li = Ri\text{-}1$, $Ri = Li\text{-}1 \oplus f(Ri\text{-}1, Ki)$를 통해($Li\text{-}1$, $Ri\text{-}1$) $\Rightarrow$ Ki $\Rightarrow$ (Li ,Ri)로 바꾸어 주는 함수를 말한다. 또한, 전체 알고리즘의 라운드 수는 요구되는 보안 강도와 수행 효율성의 상호 절충적 관계에서 결정된다. 보통 Feistel 구조는 3라운드 이상이며, 짝수 라운드로 구성된다. 이러한 Feistel 구조는 라운드 함수에 관계없이 역 변환이 가능하며(즉, 암·복호화 과정이 같음), 두 번의 수행으로 블록간의 완전한 diffusion이 이루어지며, 알고리즘의 수행속도가 빠르고, H/W 및 S/W 구현이 용이하고 아직 구조상의 문제점이 발견되고 있지 않다는 장점을 지니고 있다. (단, ⊕은 XOR 연산을 의미한다.)

2.2 SEED의 특징 및 알고리즘 전체 구성

SEED 암호 알고리즘의 데이터 처리단위는 8, 16, 32비트 모두 가능하다.[2] 암·복호화 방식은 블록암호방식으로 이뤄졌다. 입·출력문의 크기는 128비트이며, 입력키의 크기 역시 128비트를 기준으로 설계되었다. SEED의 전체 내부구조는 Feistel구조로 16라운드로 구 성되었으며, 내부함수는 SPN 구조이며. 비 선형 함수를 Look-up 테이블로 변형하여 사용하였다. 128비트 블록을 2개의 64비트 블록(L0(64), R0(64))으로 나누어, 16개의 라운드 키(64비트)와 함께 16라운드를 수행한 후, 최종 128 비트 출력(L16(64), R16(64))을 낸다.

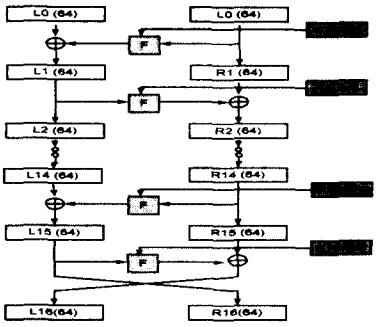

그림 1. SEED 알고리즘 전체구조도

2.3 키 생성 알고리즘

SEED의 키 생성 알고리즘은 128비트의 암호키를 64비트씩 좌우로 나누어 이들을 교대로 8비트씩 좌/우로 회전 이동 후, 결과의 4워드들에 대한 간단한 산술 연산과 G 함수를 적용하여 라운드 키를 생성한다. 키 생성 알고리즘은 기본적으로 하드웨어나 (모든 라운드 키를 저장할 수 없는) 제한된 자원을 갖는 스마트 카드와 같은 응용에서의 효율성을 위하여, 암호화나 복호화시 암호키로부터 필요한 라운드 키를 간단히 계산할 수 있도록 설계하였다. [2]

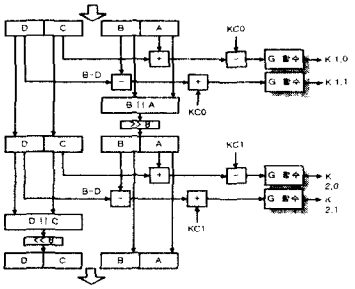

그림 2. 키 생성 알고리즘 구조도

2.4 기존논문 연구

기존에 SEED를 구현한 연구의 대부분은 라운드 공유/비공유 방식에 따른 소요 게이트 수와 데이터 처리량에 대한 비교등 칩의 면적을 최소화를 목표로 한 것과 one chip을 목표로 한 것이 대부분이었다.[3],[5] 또한 블록암호에서 쓰이는 Feistel 구조자체를 병렬화시킨 DES의 구조에 관한 연구가 있다. [4]

3. SEED 암호화 칩 설계

3.1 VHDL 설계 과정

VHDL 설계는 크게 상위 수준과 하위 수준 설계로 나뉜다. 상위 수준 설계에 해당하는 과정은 본 논문에서는 Cadence의 NCVHDL을 이용하여 VHDL을 Compile하고 Elaboration의 과정을 거친 후 Functional 시뮬레이션을 수행하고, Siganl Wave를 통해 기능을 검증하였다.

기능 검증 과정 이후에 합성(Synthesis)의 단계를 거친다. 합성이란 HDL을 이용한 설계에서 가장 중요한 과정으로 변환(translation)과 최적화(optimization)의 단계인 변환의 과정은 동작적 또는 RTL기술(HDL 설계)을 구조적 기술(게이트 레벨 표현)로 바꾸는 것이다. 최적화의 단계는 면적의 최소화와 동작의 고속화를 해 주는 작업을 한다. 본 논문에서는 Synopsys의 CompilerⅡ를 이용하여 Optimize된 Schematic을 확인하였다. 또한 Synplify 5.1.4로 Xillinx Vertex를 Target Device로 하여 Synthesis를 테스트하였다.

3.2 전체 모듈 (SEED TOP 블록) 설계

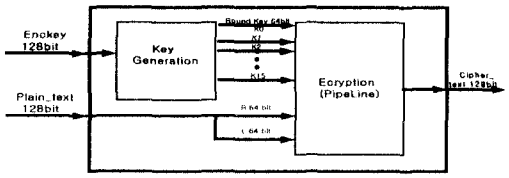

그림 3. 전체 모듈 SEED TOP 블록

먼저 128 비트 암호키(EncKey)를 입력으로 하는 키 생성부 블록(Key Generation)을 수행한 키 생성 결과인 16개의 라운드 키(Round Key)가 암호부의 각 라운드의 입력 값이 된다. 입력된 라운드 키 값(Round Key 64 bit)과 평문 데이터(Plain_text 128 bit)의 입력으로 암호부의 연산 후 암호문(Cipher_text 128 bit)이 출력된다.

3.3 Encryption 함수부(파이프라인블록) 설계

본 논문에서 설계한 암호부는 파이프라인 블록이라 명시한다. 파이프라인 블록의 특징은 게이트 수에 상관없이 각 라운드부를 파이프라인으로 연결하여 그 속도를 최소화하는 방법을 사용한다. 암호부를 파이프라인 방식으로 설계하기위하여 고려되는 사항은 키 생성 블록(Key_Gen)에서의 16개의 라운드키가 항상 병렬로 공급되어야 한다는 점이다.

암호부 블록에는 16개의 라운드 블록(Round0 … Round15)이 있고, 각각의 라운드 블록 안에는 F 함수부(F0_Fun … F15_Fun)를 수행하도록 설계하였다. 각각의 라운드 블록의 수행 후 다음 라운드 블록으로 진행하기 전에 잠시 데이터를 저장하는 역할을 하는 레지스터(Register0 … Register15)를 둔다. 파이프라인부의 입력은 128비트의 데이터와 각 라운드별 입력에 해당하는 16개의 64비트 라운드키이다. 각 서브 프로세서간의 데이터의 흐름은 함수 블록이라 할 수 있다. 서브프로세서간의 데이터의 흐름은 상위 64비트와 하위 64비트로 나뉘어서 데이터를 동작하며, 마지막 라운드(라운드15)의 수행 후에는 상위 64비트와 하위 64비트의 데이터가 교환되어 출력된다.

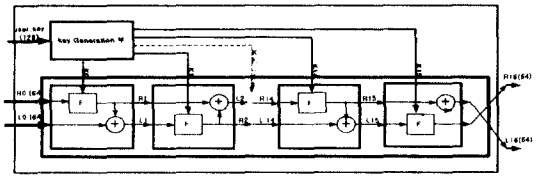

그림 4. Encryption 함수부(파이프라인 블록)

3.4 키 생성 블록 설계

128비트 암호키를 입력하여 키생성 블록을 거쳐 연산을 한 후 16개의 64비트 라운드키를 생성한다. 생성된 라운드키는 파이프라인 블록안의 각 라운드의 F함수부의 라운드키로 입력된다. 16개의 라운드 키 값은 파이프라인 블록의 각 라운드에 병렬적으로 항시 입력되도록 설계한다. 키 생성 블록은 클럭이 없는 컴비네이션 로직으로 구성한다. 복호화시에는 키 순서만 역으로 적용한다.

3.5 시뮬레이션 검증 및 합성 결과

한 아래 그림은 SEED 표준안 부록의 참조 구현 값1에 대한 test vector 값을 넣어 128비트 평문을 입력하여 키 생성 블록을 거쳐 연산한 SEED TOP 블럭을 시뮬레이션 한 결과이다.

암호문 "00000000000000000000000000000000"와
데이터 "000102030405060708090A0B0C0D0E0F"를
입력으로 한 SEED의 결과는
"C11F20140505084483597E4370F43"임을 검증한다.

키 생성은 0ns부터 되고, 340ns에 데이터 결과 값을 확인할 수 있다.

그림 5. SEED TOP 블록 시뮬레이션 결과

그림 6. 파이프라인 블록 합성 결과

다음의 표1은 Synplify를 이용한 테스트결과이다.

표1. 파이프라인구조로 설계한 SEED의 테스트결과

Mapping to Part	v1000vg560-4	
Real Time	5.748 seconds	
CPU Time	5.788 seconds	
Cell usage	MUXCY_	3443 uses
	XORCY	3555 uses
	MUXF5	22307 uses
	MUXF6	9905 uses
	VCC	1 use
	GND	1 use
	FDE	2048 uses
	BUF	5118 uses
I/O Primitives	IBUF	257 uses
	OBUF	128 uses
	BUFGP	1 use
I/O Register bits	0	
Register bits not including I/Os	2048	
Total LUTs	54803	

4. 결론 및 향후 연구 방향

본 논문은 한국 표준 암호 알고리즘인 SEED를 하드웨어로 설계하였다. 특히 암호부를 파이프라인으로 설계하는 배경은, SEED의 Feistel 구조의 각 16개의 라운드를 프로세서로 보고 설계 한 것이다. 설계 방법은 16개의 라운드 프로세서를 동시에 동작시키기 위하여 라운드 부에는 각각의 레지스터를 두어 데이터를 임시 저장시키는 방법을 이용하였다. 암호부를 파이프라인 구조로 동작시키기 위하여 키 생성 블록을 컴비네이션 로직으로 구성하고, 병렬적으로 16개의 라운드 키를 파이프라인 블록으로 출력시키는 방법을 사용하였다. 3장에서 기술한 것과 같이 속도를 최소화 시키기 위하여 파이프라인으로 설계한 SEED 알고리즘은 Vertex칩 1개로 설계 및 검증 가능함을 확인하였다.

본 논문에서는 SEED 암호 프로세서 칩의 암호 코어 부분만을 설계하였으나, 앞으로 실제 인터페이스 부분을 설계해야 할 것이다.

참고 문헌

[1] 국내 민간분야 암호 사용 정책 , 한국정보보호센터 기술 정책 연구 98-3, pp. 107-111, 1998. 12

[2] 128비트 블록 암호알고리즘(SEED) 개발 및 분석 보고서, 한국정보보호센터, pp. 1-21, 1998. 12

[3 염동복, 블록 암호화 프로세서 및 인터페이스 설계 및 구현, 석사학위논문, 한국 항공대학교, 2000. 2

[4] 이선근, DES의 데이터 처리속도 향상을 위한 변형된 Feisel 구조에 관한 연구, 전자공학회논문지, 2000. 12, pp. 91-97

[5] 송문빈, 고명관, 정연모, SEED 암호화 알고리즘의 하드웨어 구현, 한국정보처리학회, 2000년도 추계학술발표논문집 제7권 제2호, 경희대학교, pp. 1453-1456

[6] Bruce Schneuer , "Applied Cryptography",Wiley, 1996.[7]

[7] 128비트 블록 암호 표준 SEED, 한국정보보호센터, pp.14-

[8] 반도체 교육센터, 암호화 칩 설계, pp.97-136, 2000. 2

[9] 박현철, VHDL 회로설계와 응용 , 한성 출판사, 1995. 11

[10] http://www.kisa.or.kr 한국정보보호진흥원