SEED 알고리즘용 암호 보조 프로세서의 설계

정회원 최 병 윤*, 서 정 욱**

Design of Cryptographic Coprocessor for SEED Algorithm

Choi Byeong-Yoon*, Suh Chung Wook** *Regular Members*

요 약

본 논문에서는 SEED 알고리즘을 구현하는 암호 보조 프로세서를 설계하였다. 속도 와 면적 사이의 상반 관계를 고려하여, 암호 보조 프로세서는 1 라운드 동작을 3개의 부분 라운드로 나누고, 클럭마다 하나의 부분 라운드를 수행하는 구조를 갖는다. 동작속도를 향상시키기 위해서 암호 및 복호 동작의 라운드 키를 온라인 사전 계산 기법을 사용하여 계산하였으며, 다양한 분야에 응용할 수 있도록 4가지 동작 모드를 지원한다. 그리고 데이터의 외부 입출력 동작에 따른 성능 저하 문제를 제거하기 위해, 암호 보조 프로세서의 암·복호 동작과 데이터의 입출력 동작을 병렬로 수행하는 방식을 사용하였다. 설계한 암호 보조 프로세서는 0.25 μm CMOS 공정으로 설계되었으며, 설계된 회로는 약 29,300개의 게이트로 구성되며, 100 Mhz 동작 주파수와 ECB 동작 모드 조건에서 약 237 Mbps의 암·복호율의 성능을 얻을 수 있었다.

ABSTRACT

In this paper a design of cryptographic coprocessor which implements SEED algorithm is described. To satisfy trade-off between area and speed, the coprocessor has structure in which 1 round operation is divided into three subrounds and then subround is executed for one clock. To improve clock frequency, online precomputation scheme for round key is used. To apply the coprocessor to various applications, four operating modes such as ECB, CBC, CFB, and OFB are supported. Also to eliminate performance degradation due to data input and data output time between host computer and coprocessor, background input/output method is used. The cryptographic coprocessor is designed using 0.25 μm CMOS technology and consists of about 29,300 gates. Its peak performance is about 237 Mbps encryption or decryption rate under 100 Mhz clock frequency and ECB mode.

I. 서 론

정보 보호 기술은 위성 통신, 인터넷 전자 문서 교환, 전자 상거래 및 스마트 카드 등의 거의 모든 정보 통신 관련 산업 분야에서 요구되고 있다. 특히 전자 상거래 및 인터넷을 통한 정보 서비스를 사용자들이 신뢰하며 사용하기 위해서는 정보 시스템의 보안과 처리 속도가 우선적으로 보장되어야 한다[1]. 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[2]. 그리고 세계 각국은 인터넷을 이용한 전자 상거래를 21세기 국가 경쟁력을 결정하는 중요한 요소로 간주하여, 국가 전략적으로 전자 상거래의 활성화를

* 동의대학교 컴퓨터공학과(bychoi@hyomin.dongdui.ac.kr), ** 한국전자지불연구원
논문번호 : 00271-0714 접수일자 : 2000년 7월 14일
※ 이 논문은 1999년도 동의대학교 교내 연구비에 의해 수행되었음

위해 많은 노력을 경주하고 있다. 그리고 미국에서는 조만간 DES를 대신할 새로운 대칭형 암호 표준 AES(Advanced Encryption Standard)[3]가 선정되어 사용될 예정이다. 이러한 추세에 맞추어 한국에서도 독자적인 128 비트 SEED 암호 알고리즘을 개발하여 표준으로 정하였다[4]. SEED 암호 알고리즘은 설계시 안전성을 고려하여, 128 비트 구조를 취하고 있으며, 1개의 라운드 동작이 DES에 비해 복잡한 Feistel 구조를 갖고 있다. 그러나 SEED 알고리즘은 DES에 비해 안전성은 크게 증가하였지만, 내부 구조의 복잡성으로 하드웨어가 복잡하고 속도가 크게 떨어지는 결점이 있다. 즉 네트워을 비롯한 통신에 사용되었을 때, SEED 암호 블록이 병목 현상을 야기 시킬 수 있다. 따라서 SEED를 전자 상거래 등 다양한 응용 분야에 적용하기 위해서는 면적 과 속도 측면에서 우수한 성능을 갖는 SEED 암호 프로세서 개발이 필요하다.

본 논문에서는 SEED 암호 알고리즘의 여러 가지 구현 방안을 비교하고, 면적 과 속도 측면에서 효율적인 구조를 제안하고, 이를 하드웨어로 설계한 후 성능을 분석하였다. 본 논문의 구성은 2장에서는 SEED 암호 알고리즘을 구성과 특징을 간단히 기술하고, 3장에서는 SEED 암호 보조 프로세서의 설계를 다루며, 4장에서는 암호 보조 프로세서의 검증 및 성능 분석을 기술하였으며, 5장에서는 결론 및 향후 연구 방향을 제시하였다.

Ⅱ. SEED 암호 알고리즘

SEED 암호 알고리즘은 기존 3중 DES 보다 암·복호율이 효율적인 구조를 목표로 설계되었으며, 그림 1과 같이 128 비트 평문은 2개의 64 비트 블록($L_0(64)$, $R_0(64)$)으로 나눈 후, 16쌍의 라운드 키 $K_i(K_{i,1}, K_{i,0})$와 함께 Feistel 구조의 16 라운드 동작을 수행한 후, 최종 128 비트 출력($L_{16}(64)$, $R_{16}(64)$)을 출력하는 구조를 갖고 있다. SEED의 동작 특성을 결정하는 그림 2의 F 함수는 Ri(64)값과 라운드 키 K_i ($K_{i,1}$, $K_{i,0}$)를 입력으로 받아, 64 비트 블록(D', C')을 생성한다. SEED 복호 동작은 암호 동작과 유사하지만 라운드 키 적용 순서가 암호 과정과 반대이다. 즉 암호 동작의 첫 번째 라운드에 사용하는 라운드 키가 복호 동작의 경우 마지막 라운드에 사용된다.

G 함수는 SEED 암호 알고리즘의 안전성을 구현하는 핵심 부분으로 2쌍의 S1, S2 박스에 대한 테

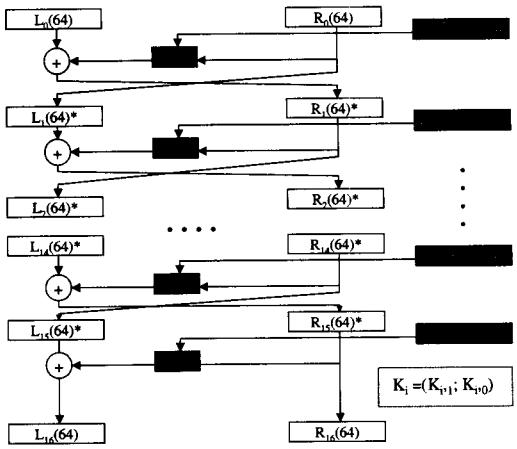

그림 1. SEED 암호 알고리즘의 구조

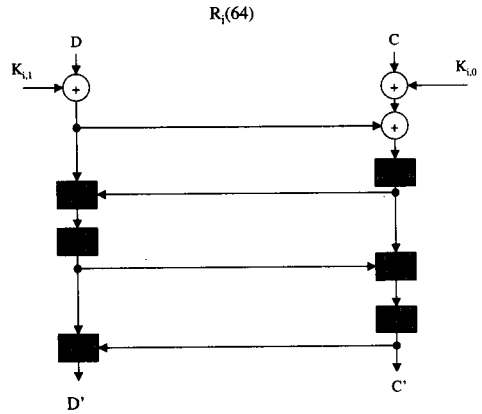

그림 2. F 함수의 구조

이블 룩업 동작, 마스킹 동작과 XOR 연산을 통해, 32 비트 출력을 생성하는 회로이다. 암호 동작에 사용되는 라운드 키 생성 알고리즘은 128 비트의 마스터 키 또는 중간 라운드의 조정된 마스터키 값을 받아 64 비트씩 좌우로 나눈 후, 이들을 8 비트씩 좌 또는 우로 회전 이동시켜 새로이 조정된 마스터 키를 생성함과 동시에 중간 라운드의 4개의 입력 값(D, C, B, A)에 대해 32 비트 모듈로 덧셈, 뺄셈 및 G 함수를 적용하여 라운드 키(K_i)를 생성한다. 그림 3은 암호 동작에 대한 라운드 키 생성 알고리즘을 나타낸다. 그림에서 ||, <<, 와 >> 표현은 각각 연결 접속, 좌 또는 우측 순환 이동 동작을 나타낸다. 실제 하드웨어 구현 시 순환 이동 부분은 별도의 배럴 시프터를 사용하지 않고 고정 배선으로 구현된다. 키 생성부에 사용되는 라운드 상수 KCi는 식(1)과 같이 결정된다. 여기서 i 값은 암호 동작에 대한 라운드를 나타낸다. 즉 각 라운드에 사용되는

라운드 상수는 이전 라운드 값을 좌측으로 1 비트 만큼 회전시켜 생성 가능하다.

$$KC_1 = 0x9e3779b9$$
$$KC_i = KC_{i-1} \ll 1 \text{ for } 2 \le i \le 16 \quad (1)$$

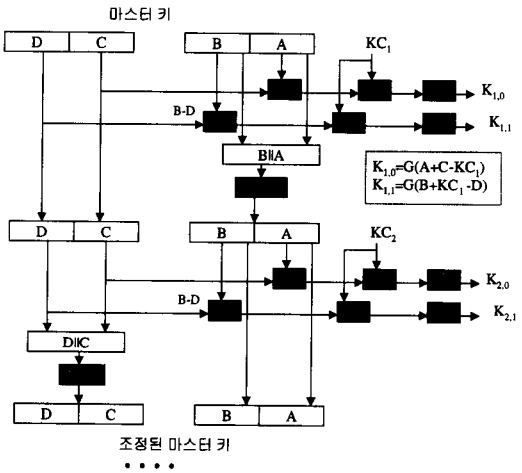

그림 3. 암호 동작에 대한 라운드 키 생성 알고리즘

Ⅲ. SEED 암호 보조 프로세서의 VLSI 설계

본 장에서는 2장에서 기술한 SEED 암호 알고리즘을 구현하기 위한 암호 보조 프로세서의 설계 사양, 구조 결정 시 고려 사항 및 프로세서 내부 구조 설계를 기술한다.

1. 암호 보조 프로세서의 외부 인터페이스와 설계 사양

본 논문의 암호 프로세서는 외부 호스트 프로세서에 대한 보조 프로세서 형태로 설계되어, 다양한 호스트 환경에 접속이 가능하도록 개발되었다. 또한 SEED 암호 프로세서를 다양한 응용 분야에 암·복호 모듈로 사용될 수 있도록, 4가지 운영 방식, 즉 ECB(Electronic CodeBook), CBC(Cipher Block Chaining), CFB(Cipher FeedBack) 및 OFB(Output FeedBack) 방식을 모두 지원하도록 하였다[5]. 그림 4는 암호 보조 프로세서의 전체 구조를 나타낸다. 외부의 데이터 버스를 통해 마스터 키와 CBC, CFB, OFB 모드에서 사용되는 초기값(IV) 데이터를 입력한다. 단, 암호 동작과 외부 입출력 동작을 동시에 수행하여 입출력 시간에 따른 성능 저하를 방지하기 위해, 입·출력 버퍼 레지스터(I/O buffer Reg) 과 내부 암호 코어의 입출력 레지스터(DIN/DOUT Reg)을 분리시켜 암호 동작 중에 입·출력 버퍼 레지스터를 통해 입출력 동작을 수행할 수 있도록 하였으며, 시작 신호 발생 시 DIN/DOUT 레지스터에 담긴 암·복호 결과와 I/O 버퍼 레지스터에 저장된 새로운 입력 데이터를 서로 교환하는 동작을 수행한다. 그리고 암호 연산 수행 동안 Busy 플래그가 "1" 상태로 되어, 암호 동작이 진행 중임을 나타낸다. Busy 신호가 "1" 인 동안 호스트 프로세서는 암·복호화 할 새로운 데이터를 I/O 버퍼 레지스터에 두고, Busy 신호가 "0"이 될 때까지 대기한다. 그리고 외부 호스트 프로세서가 8 비트, 16 비트, 32 비트 등의 데이터 버스를 가질 수 있으므로, 이를 해결하기 위해 data_in_out 모듈은 외부 호스트 시스템의 특성에 맞게 암호 보조 프로세서의 Data[n-1:0] 핀으로 데이터가 전달될 수 있도록 하는 기능을 담당한다. 여기서 n은 호스트 프로세서의 데이터 크기를 나타낸다. SR 레지스터는 동작 모드, 외부 인터페이스 방안, CFB와 OFB 모드 시 암·복호 단위를 지시하는 필드를 갖고 있다. 주소 값 Addr[5:0]는 호스트 프로세서가 데이터 버스를 통해 내부 레지스터에 데이터를 전달할 때, 특정 레지스터의 특정 바이트 주소 값을 구별하는데 사용된다. 단, 내부 모듈의 보안 측면을 고려하여, 암호 보조 프로세서의 Key와 IV, SR값은 외부에서 읽는 동작이 허용되지 않도록 설계되었다.

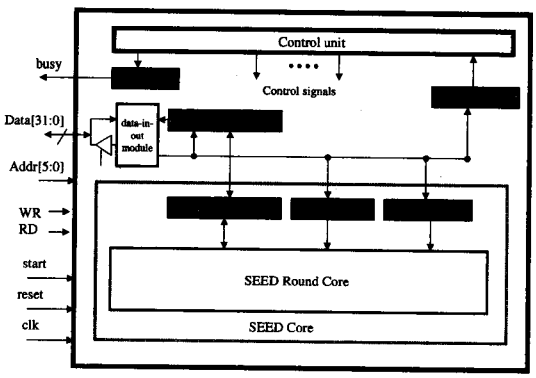

그림 4. SEED 암호 보조 프로세서의 블록 구성도

2. SEED 코어 설계

SEED 코어는 그림 5에 보이는 바와 같이 입출력 데이터, 키, 초기값의 정보를 담고 있는 레지스터, 배럴 시프터 L_shift_1, L_shift_2 와 SEED

round core로 구성된다. DIN_OUT 레지스터는 암·복호 동작을 수행할 128 비트 입력 데이터를 담는 기능과 암·복호 동작의 결과 값을 저장하는 역할을 함께 수행한다. L_shift_1과 L_shift_2 회로는 동작 방식에 따라 128 비트 좌측 이동 또는 j 비트 좌측 이동 동작을 통해 4가지 동작 모드(ECB, CBC, CFB, OFB)에 대한 초기 값과 중간 결과의 좌측 이동 동작 또는 갱신 동작을 지원한다. 여기서 j 비트는 CFB 또는 OFB 모드에서 암·복호 단위를 나타내는 값으로 SR 레지스터에 그 값이 정의된다. SEED 라운드 코어(round core)는 16 라운드 동작을 구현하는 라운드 데이타패스와 라운드 키를 생성하는 키 생성부 부로 나뉘어 진다. SEED 라운드 코어 설계 시 귀환 출력이 사용되는 CBC, CFB 및 OFB 모드의 지원에 따라 파이프라인 구조는 불가능하므로, 1 라운드 동작에 필요한 하드웨어를 갖추고, 이를 16 라운드 반복 사용하여 암·복화 동작을 구현하는 구조를 채택하였다. 그런데 SEED 알고리즘의 1 라운드를 1 클록으로 구현할 경우 그림 2의 F함수의 특성에 의해 3개의 G 함수가 필요하다. 그리고 G 함수는 내부에 2쌍의 S_1과 S_2 박스가 필요하다. 그리고 그림 1을 보면 각 라운드 동작 전에 라운드 키의 계산 동작이 필요한데, 이러한 라운드 키의 계산에는 2개의 G 함수가 추가적으로 필요하다. 따라서 SEED 암호 알고리즘을 클록 당 1 라운드(1 round/clock) 방식으로 구현할 경우 하드웨어 공유가 불가능하므로, 전체적으로 5개의 G함수, 즉 20개의 S 박스가 필요하다. 이러한 S 박스는 $2^8 \times 8$ 크기의 ROM 테이블, 마스크 로직 및 XOR 게이트로 구성되므로, 1 라운드 구현에 필요한 하드웨어 양이 기존 DES 알고리즘에 비해 훨씬 크게 되며, 내부 라운드 동작의 직렬 연산에 따른 긴 최악 경로로 낮은 동작 주파수를 갖게 된다.

본 연구에서는 다음과 같은 방식으로 이러한 문제를 해결하였다.

첫째, SEED의 1 라운드 동작을 그림 6과 같이 3개의 부분 라운드로 분할한 후, 각 부분 라운드를 단일 클록으로 구현하는 방식(1 round/3 clocks)을 사용하였다. 이 방식의 경우 각 부분 라운드 내에는 한 쌍의 G함수와 32 비트 모듈라 덧셈기가 존재하므로 하드웨어 공유가 극대화될 수 있다. 그리고 각 부분 라운드 구현 시 연결 관계를 단순화시키기 위해서, 각 부분 라운드의 출력을 엇갈리게(cross)하는 형태를 채택하였다. 단, 부분 라운드 1의 경우 4가지 모드 지원하기 위한 일부 멀티프렉서와 XOR 기능이 추가로 포함된다.

둘째, 라운드 키 계산은 라운드 동작 진행과 병행하여 계산하는 온라인(on-line) 계산 방식을 사용한다. 16개의 라운드 키를 암호 또는 복호 동작 전에 모두 계산하는 오프라인(off-line) 방식은 라운드 키 저장에 필요한 다수개의 레지스터와 라운드 키 계산에 따른 연산 시간 증가 문제로 본 연구에서는 배제하였다.

셋째, 복호 동작의 경우 암호 동작과 반대 순서로 라운드 키 생성이 필요한 데, 독립적인 별도의 하드웨어를 사용하지 않고, 암호 동작용 라운드 키 생성 회로에 마스터키의 초기 정렬과 반대 방향의 좌·우측 회전 이동 회로의 추가를 통해 복호 동작에 대한 라운드 키 생성이 가능하도록 하였다. 단, 이러한 동작을 위해 각 라운드에 대한 키 상수(KC_i)도 암호 및 복호 동작에 맞게 온라인 방식으로 생성하였다.

넷째, 라운드 키의 계산은 이전 라운드에 파이프라인 방식으로 미리 계산하는 방식(precomputation)을 사용한다. 그림 6의 라운드 동작을 3개의 클록 내에 수행하므로, 라운드 키의 계산에 활용할 수 있는 시간이 3개의 클록 길이라는 동작 특성을 활용하여, 라운드 키 계산을 병렬 계산 방식이 아닌 파이프라인 기법을 통해 그림 7과 같이 수행하였다. 파이프라인 계산 방식의 경우 $K_{i,1}$과 $K_{i,0}$를 동시에 계산하는 병렬 계산 방식에 비해 32 비트 파이프라인 레지스터와 캐리 보존 가산기(carry save adder)가 추가되었지만, 병렬 방식에 비해 G함수 1개와 모듈로 가산기가 3개 감소되어 하드웨어 감소 측면에서 약 2배 효과가 있다. 그리고 각 파이프라인 단계가 G 함수 또는 32 비트 모듈로 가산기로 구성되므로 그림 5의 부분 라운드 보다 작은 지연 시간을 가지므로, 동작 주파수를 감소시키는 최악 경로를 생성하지 않는다. 단, 모듈로 가산기는 고속 동작을 위해 32 비트 CLA(carry lookahead adder) 가산기를 사용하였다.

이러한 4가지 주요 기법을 통해 필요한 G 함수의 개수를 5개에서 2개로 축소할 수 있었다. 즉 S 박스 수로 비교하면 20개에서 8개로 크게 축소된다. 그리고 모듈로 덧셈기의 감소 등을 고려할 때, 기존 클록당 1 라운드 수행 방식에 비해, 본 논문에서 사용한 방식은 약 3배 정도의 하드웨어 감소 효과가 있다. 그림 8은 그림 6에서 제안한 기법을 하드웨어로 구현한 라운드 데이터패스를 나타낸다. 그림에서 Sub_r_23 신호는 두 번째와 세 번째 부분 라운드

동작의 경우, 중간 부분 라운드 결과를 저장하고 있는 T 레지스터 값을 입력으로 선택하는 동작을 수행한다.

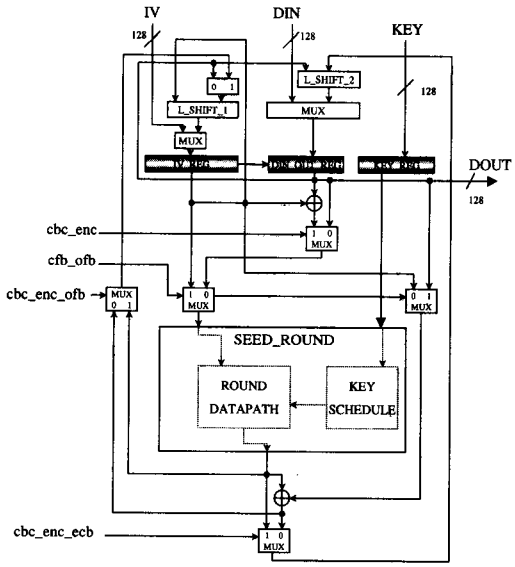

그림 5. SEED 코어의 블록도

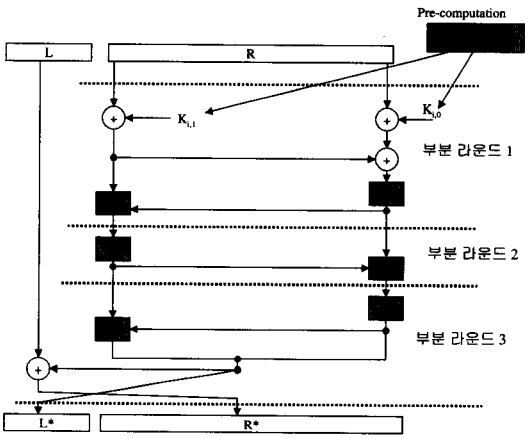

그림 6. 1 라운드를 3개의 부분 라운드로 분할하는 기법

3. 제어 회로 설계

제어 회로는 외부 호스트 프로세서가 제공하는 입출력 커맨드를 해독하여, 필요한 입출력 동작을 수행하는 입출력 제어부(I/O control)와 호스트 프로세서가 제공하는 시작신호를 받아서 SEED 암호 알고리즘을 구현하는 코어 제어부(core control)로 나뉜다. SEED 암호 보조 프로세서가 외부 호스트와 별도의 클록으로 동작하므로, 호스트가 제공하는 명

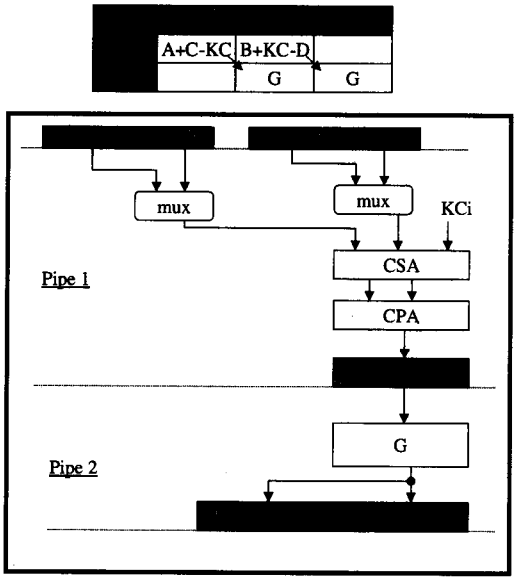

그림 7. 파이프라인 계산을 사용한 라운드 키의 사전 계산 방법

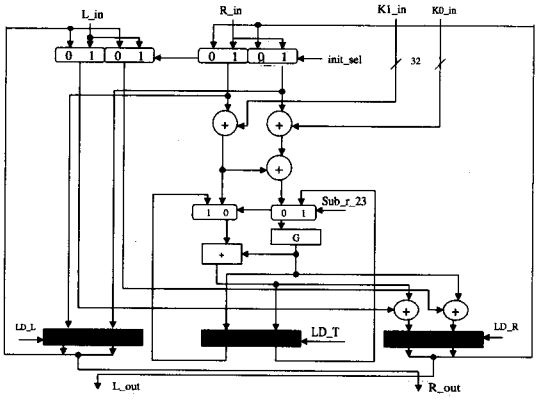

그림 8. 라운드 데이터패스

령 중 시작신호는 SEED 암호 프로세서의 동기 클록과 동기화가 필요하다. 따라서 외부에서 제공되는 시작 신호는 보조 프로세서 내부에 포함된 동기화 회로를 거쳐 코어 제어부에 제공되도록 함에 의해서, 외부 명령이 비실행 또는 다중 실행되는 것을 방지하도록 하였다. 그림 9의 코어 제어부는 FSM(finite state machine)부, 카운터부, 제어신호 생성부(Main_Local_Con)로 구성된다. 코어 제어 회로 설계는 데이터패스의 동작 흐름을 ASM (Algorithmic State Machine) 차트로 표현한 후, 이를 제어 회로로 변환하는 방법을 사용하였다. 코어 제어 회로의 카운터 부는 4가지 동작 모드를 구현하기 위해 3개의 카운터, 즉 RND_CNT, KEY_

CNT 및 IT_CNT로 구성된다. IT_CNT는 CFB와 OFB 모드 시, 암·복호화 단위(j)에 의해 결정되는 반복 회수로 128/j만큼의 반복 동작이 필요한데, 이를 제어하기 위한 카운터이다. 본 연구의 암호 프로세서에서 지원하는 j값은 8, 16, 32, 64 및 128이다. 본 연구의 SEED 암호 보조 프로세서는 라운드 키의 사전 계산 방식을 채택함에 따라 그림 5의 라운드 데이타패스와 키생성부 동작에 필요한 라운드 값이 다르므로 2개의 16진 카운터를 사용하여 각각의 동작을 제어하는 방식을 사용하였다.

Ⅳ. 검증 및 성능 분석

본 연구에서 설계한 암호 프로세서는 먼저 SEED 암호 알고리즘을 C 언어로 모델링한 후, 이를 Verilog HDL[6] 언어로 변환하여 2가지 동작이 일치하는지 확인하는 과정을 사용하였다. 검증 과정에 ECB 모드의 경우 정보 보호 센터 보고서[4]에서 명시한 테스트 벡터를 올바로 만족함을 확인하였다. 그리고 나서 설계한 회로를 0.25 μm CMOS 라이브러리를 사용하여 Synopsys Tool[7]을 사용하여 합성하였다. 합성 결과 암호 보조 프로세서의 최악 동작 경로는 약 9.38ns로서 최대 동작 주파수는 100Mhz이었으며, 총 게이트 수는 약 29,300이었다. 그림 10은 설계한 암호 프로세서의 ECB 모드에 대한 동작 타이밍을 나타낸다. round 1 이전에 라운드 키의 사전 계산을 위한 3개의 클럭을 포함해 총 51개의 클록으로 구성된다. 단, 16 라운드의 동작 수행 후에 SEED 라운드 최종 결과가 그림 8의 {L,R} 레지스터에 위치가 반대로 담기게 되므로, 외부 호스트로 전달을 하기 위해서는 {L,R} 레지스터 값을 엇갈리게 DIN_DOUT 레지스터로 이동시키는 추가의 사이클이 필요하다. 따라서 실제 ECB 동작 구현에 소요된 사이클 수는 (48+1)+3=52이다. 반면 CBC, CFB, OFB 모드의 경우, 이러한 추가의 동작 사이클 과정에 XOR 게이트와 L_shift 회로를 활용하여, IV 레지스터와 DIN_DOUT 레지스터 값을 적절히 갱신한다. 따라서 ECB 모드의 경우 암·복호율은 식(2)에 따라 100Mhz 클록 조건에서 약 237 Mbps 이다. 반면 CFB와 OFB 모드의 경우 암·복호율은 식 (3)과 같이 정의된다.

$$ECB\text{와 }CBC\text{모드에 대한 암·복호율} = (128 \div 52) \times f$$

여기서 f 주파수

(2)

$$CFB\text{와 }OFB\text{모드에 대한 암·복호율} = \frac{128}{49 \times \frac{128}{j} + 3} \times f$$

여기서 j는 암·복호 단위

(3)

그림 11은 Synopsys Tool을 사용하여 암호 보조 프로세서를 합성한 회로도를 나타낸다. 표 1은 암호 프로세서의 전기적 특성을 나타낸다. S 박스에 대한 구현 방안으로 식의 논리 최소화를 이용하는 방식은, 테이블 룩업 방식에 비해 회로 개선 효과가 크

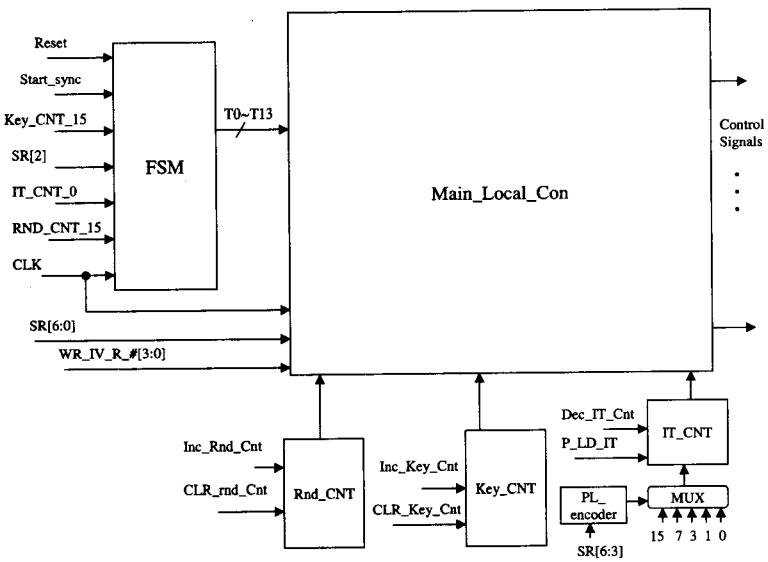

그림 9. 코어 제어부 블록도

지 않고 배선을 복잡하게 하는 문제가 있어서, 본 연구에서는 이진 룩업 테이블(binary lookup table) 형태로 구현하는 방식을 사용하였다. 표 2는 본 SEED 암호 프로세서와 여러 가지 SEED 암호 프로세서의 구현 방안을 아키텍쳐 측면에서 비교한 결과이다. 단, 최종 {L, R} 레지스터 값의 DIN_DOUT 레지스터로의 이동 동작은 구현 측면의 동작 특징이므로 표 2의 계산에는 포함시키지 않았다. 여기서 1 round/4 clocks 방식은 라운드 키를 사전에 계산하지 않고, 라운드 키 계산을 첫 번째 부분 라운드로 할당한 방식을 나타낸다. 그리고 만일 ECB 모드만 지원하는 보안 시스템을 개발하는 경우, 본 연구에서 제안한 방식을 3개의 클럭 사이클 또는 매 클록마다 1개의 128 비트 출력을 생성하는 파이프라인 구조로 변형하여 구현이 가능하다. 표 2에 따르면 본 암호 프로세서는 면적과 속도 측면에서 효율적임을 알 수 있다. 즉 1 round/clock 방식에 비해 소요되는 클록 수가 많지만, 라운드 키의 사전 계산 특성에 의해 동작 주파수가 4배 정도 빠르므로, 실제 전체 연산은 1.25배 빠르게 수행된다.

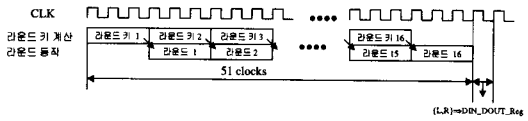

그림 10. ECB 모드에 대한 암호 프로세서의 타이밍 분석

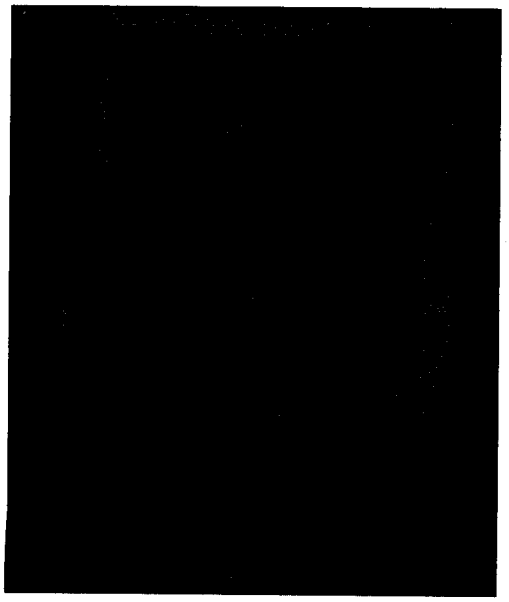

그림 11. 암호 보조 프로세서의 합성도

표 1. 전기적 특성

지원 암호 알고리즘	SEED@ECB, CBC, CFB, OFB
라운드당 클럭수	3
S 박스 구조	2진 lookup table(28 × 8)
게이트 수	약 29,300
동작 주파수	100 Mhz
라운드 키 계산 방식	online pipelined precomputation
암·복호율	237 Mbps @ ECB, CBC mode 237 Mbps @ CFB, OFB mode (J=128) 16 Mbps @ CFB, OFB mode (J=8)
입출력 방식	background input/output
외부 인터페이스	8-bit/16-bit/32-bit
암·복호화 단위(J) (@CFB, OFB)	8, 16, 32, 64, 128 비트

표 2. SEED 암호 프로세서 구현 방식 비교

방 식	G 함수 수	S 박스 수	모듈라 가산기수	성능 (클럭수) @ECB	클럭 주기	연산 시간
1 round/ 1 clock	5	20	7	16	T	16T
1 round/ 4 clocks	3	12	4	4×16 =64	T/4	16T
본 연구 (1 round/ 3 clocks)	2	8	2	3×16+3 =51	T/4	12.75T

표 3. 기존 대칭키 암호 프로세서와 특성 비교

프로세서명	지원 알고리즘	지원 모드	성 능	동작 주파수
PCC101[8]	DES, TDES	ECB, CBC, CFB, OFB	132 Mbits/sec	33 Mhz
RICO[9]	RSA, DES, MD5	ECB, CBC, CFB, OFB	19.9 Mbyte/sec	45 Mhz
GaAs DES[10]	DES	ECB, CBC	1 Gbits/sec	350 Mhz
본 연구	SEED	ECB, CBC, CFB, OFB	237 Mbits/sec	100 Mhz

그리고 면적 측면에서 비교할 때 약 3배 정도 면적 개선 효과가 있다. 표 3은 기존 DES를 구현한 암호 프로세서와 본 연구의 암호 프로세서와의 특징을 비교한 결과이다. GaAs DES의 경우 동작 속도는 고속이지만 실리콘 공정이 아니고 GaAs 공정을 사용하였으며, 동작 모드가 2가지로 제안되는 문

제점이 있다. 이러한 특성을 고려할 때 본 연구의 SEED 암호 프로세서는 SEED 암호 알고리즘을 보안 모듈로 사용하는 시스템에 효율적으로 장착될 수 있을 것으로 판단된다.

V. 결 론

본 논문에서는 면적 측면과 속도 측면에서 효율적인 SEED 암호 보조 프로세서를 설계하였다. 설계한 SEED 암호 보조 프로세서는 4가지 동작 모드를 모두 지원하며, 1 라운드 동작을 3개의 부분 라운드로 분할 처리, 라운드 키의 온라인 파이프라인 계산 기법을 통해 하드웨어 공유를 극대화시켜, 기존 1 round/1 clock 방식에 비해 약 1/3의 하드웨어 크기를 갖는다. 그리고 라운드 키의 사전 계산 기법을 통해 동작 주파수와 연산 사이클 수를 개선 시켜, 1 round/1 clock 방식에 비해 전체 연산 시간을 1.25배 개선할 수 있었다. 또한 외부 호스트 컴퓨터와 암호 프로세서사이의 입출력 동작과 암호 프로세서 동작을 병렬로 수행함으로서, 입출력 시간에 따른 성능 저하 문제를 제거하였다. 또한 외부 호스트 컴퓨터와의 인터페이스를 8비트, 16비트, 32 비트로 다양하게 프로그래밍 할 수 있는 기능을 갖추고 있다. 그리고 본 연구에서 설계한 암호 프로세서에서 4가지 동작 모드를 구현하는 구조는 융통성이 크므로, 암호 알고리즘의 변경에 따라 내부 라운드 코어의 변경을 통해 다양한 암호 알고리즘에 적용할 수 있다. 현재 설계한 SEED 칩은 약 29,300개의 게이트로 구성되며, 0.25 μm CMOS 공정에서 약 100 Mhz의 동작 주파수를 가지며, ECB 모드에서 약 237 Mbps의 암·복호율를 얻을 수 있었다. 이러한 구조적인 특성으로 본 연구에서 설계한 암호 보조 프로세서는 SEED 암호 알고리즘이 적용되는 네트워, 전자 상거래 시스템 등의 보안 모듈로 사용될 수 있을 것으로 판단된다. 그리고 AES 표준안이 확정되면 단일 칩에 SEED와 AES암호 알고리즘을 구현하는 프로세서 연구가 필요하다.

참 고 문 헌

[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, 1998.

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

[6] IDEC 반도체 설계 교육센터, *Cadence Tool 교육 강좌 자료*, 1999.5.

[7] IDEC 반도체 설계 교육센터, *Synopsys Tool 교육 강좌 자료*, 1999.4.

[8] PIJNENBURG, *PCC101 DES/3DES Data Encryption Device*, http://www.pijnenburg.nl/pcc101.htm

[9] IBM Japan, "High Performance RSA Hardware Accelerator Design", http:// www.trl.co.jp/projects/embtec/rico2e.htm

[10] Hans Eberle, "A High-speed DES Implementation for Network Applications", CRYPTO '92, pp.521-539, 1993, Springer-Verlag.

최 병 윤(Byeong-Yoon Choi)

1981년~1985년 : 연세대학교 전자공학과(공학사)
1985년~1987년 : 연세대학교 전자공학과(공학석사)
1987년~1992년 : 연세대학교 전자공학과(공학박사)
1997년~1998년 : 일리노이 주립대 Vsiting Professor
1993년~현재 : 동의대학교 교수
<주관심 분야> 마이크로프로세서 설계, 통신 및 암호 회로의 VLSI 설계

서 정 욱(Chung-Wook Suh)

1984년~1999년 :
한국전자통신연구원 재직
TDX교환기 개발 참여
CDMA 개발
세부과제 책임자 역임
초고속통신망 개발
세부과제 책임자 역임
정보보호기술 개발 책임자 역임
해킹방지용 암호프로세서기술 개발 책임자 역임
1999년~현재 : 차세대 IC카드 프로젝트 그룹 의장
재직 국제 Global Platform Consortium의
이사 재직
2000년~현재 : 한국전자지불연구원 원장 재직
1992년 : 과학기술부공인 전자응용기술사 자격 취득
1999년 : 정보통신부장관 표창
<주관심 분야> 전자 화폐, 스마트 카드, 암호 프로세
서 설계