AES 암호 프로세서의 VLSI 설계

*정 진 욱, *최 병 윤, **서 정 욱
*동의대학교 컴퓨터공학과, **(주)한국 전자 지불 연구원

VLSI Design of AES Cryptographic Processor

Jin-Wook Jeong, Byeong-Yoon Choi, and Chung-Wook Suh
Dept. of Computer Engineering, Dongeui University
E-mail : bychoi@hyomin.dongeui.ac.kr

Abstract

In this paper a design of cryptographic coprocessor which implements AES Rijndael algorithm is described. To achieve average throughput of 1 round per 5 clocks, subround pipelined scheme is applied. To apply the coprocessor to various applications, three key sizes such as 128, 192, 256 bits are supported. The cryptographic coprocessor is designed using 0.25 μ m CMOS technology and consists of about 36,000 gates. Its peak performance is about 512 Mbps encryption or decryption rate under 200 Mhz clock frequency and 128-bit key ECB mode(AES-128 ECB).

I. 서론

전자 상거래 및 인터넷을 통한 정보 서비스를 사용자들이 신뢰를 갖고 사용하기 위해서는 정보 시스템의 보안과 처리 속도가 우선적으로 보장되어야 한다[1]. 현재 보편적으로 널리 사용되고 있는 DES(Data Encryption Standard) 암호 알고리즘은 고속 프로세서의 개발로 알고리즘 자체의 안전성에 위협이 되고 있는 상황이다. 따라서 미국 상무부 기술 표준국(NIST)에서는 1997년부터 DES를 대신할 새로운 대칭형 암호 표준 AES(Advanced Encryption Standard)[2]를 전세계에 공모하여 3단계의 평가 절차를 거쳐서 2000년 10월에 벨기에 Proton World International(PWI)사의 연구원인 John Daemen과 K.U.Leuven 대학의 Vincent Rijmen이 제안한 Rijndael 알고리즘을 선정하였다. Rijndael 알고리즘 자체는 가변 블록 길이와 가변 키 크기를 지원하지만, 최종 AES 알고리즘은 128-비트의 고정된 블록 크기에 대해 암호 키 길이로 128, 192, 256 비트를 지원하며, 보안성, 효율성, 융통성을 갖추고 있다. AES는 키 길이에 따라 AES-128, AES-192, AES-256으로 구분되며, 3가지 키는 응용 분야에 따라 선택적으로 구현할 수 있으며, 취약 키가 존재하지 않는다는 특징을 갖고 있다. AES 알고리즘으로 채택된 Rijndael은 소프트웨어 구현, FPGA 구현, 스마트 카드 구현, 대규모 집적회로 구현 평가를 통해, 가장 적합한 대칭키 암호 알고리즘으로 평가를 받았다. 그러나 AES 알고리즘은 모든 라운드 동작을 단일 클록으로 구현하는 경우 하드웨어 양이 DES에 비해 너무 많이 필요하다는 결점이 있다. 따라서 AES를 스마트 카드를 비롯한 다양한 응용 분야에 적용하기 위해서는, 응용 분야의 사양을 만족하며 면적 과 속도 측면에서 우수한 성능을 갖는 AES 암호 보조 프로세서 구조에 연구가 필요하다. 본 논문에서는 AES 암호 알고리즘의 여러 가지 구현 방안을 비교하고, 면적과 속도 측면에서 효율적인 구조를 제안하고, 이를 하드웨어로 설계한 후 성능을 분석하였다.

II. AES 알고리즘

DES를 비롯한 대부분의 대칭키 암호 시스템들은 Feistel 구조의 라운드 변환을 기반으로 하는데 비해, AES 암호 알고리즘은 non-Feistel 구조를 바탕으로 하고 있으며, 3개의 독립된 역변환 가능한 라운드 변환으로 구성된다. AES는 키 길이에 따라 AES-128, AES-192, AES-256으로 불리며, 라운드 수는 각각 10, 12, 14이다. AES 대칭키 암호 알고리즘의 연산 처리 과정은 그림 1 과 같이 초기 라운드 키 가산(AddRoundKey)후에 (Nr-1)번의 반복 라운드 및 최종 라운드의 순서로 처리된다. 최종 라운드를 제외한 각 라운드는 ByteSub, ShiftRow, MixColumn 및 AddRoundKey 등의 라운드 변환동작으로 구성된다. 이러한 라운드 변환 동작은 외부에서 주어진 1차원 형태의 128 비트 블록을 2차원의 4행 × Nb열(단, Nb는 4)로 구성되는 State로 변환한 후, State내 byte 배열에 대해 연산을 수행한다.

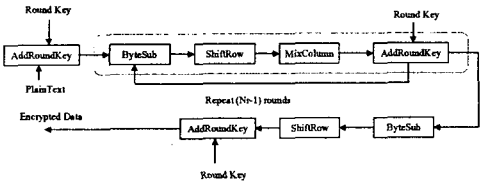

그림 1. AES 암호 알고리즘의 연산 처리 과정

ByteSub 블록은 State를 구성하는 각 바이트에 대해 개별적인 비선형 바이트 치환 동작을 수행하며, 이러한 치환 동작은 $2^8 \times 8$ 비트 룩업 테이블(lookup table) 형태의 S 박스(S-box)로 구현된다. 그림 2는 ShiftRow 라운드 변환을 나타내며, 첫째 행을 제외한 나머지 행들은 각각 1, 2, 3 바이트씩 왼쪽으로 순환이동 동작을 수행한다. 여기서 $a_{i,j}$ 와 $b_{i,j}$는 바이트 형태의 값을 나타낸다.

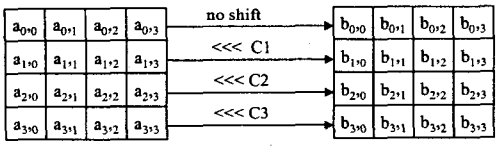

그림 2. ShiftRow 라운드 변환(C_1=1, C_2=2, C_3=3)

MixColumn 라운드 변환은 State의 Column들을 $GF((2^8)^4)$의 다항식으로 생각하고, b(x) = c(x) ⊗ a(x) 형태의 다항식 곱셈으로 처리한다. 여기서 c(x)는 $c(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x^3 + \{02\}$ 형태의 고정된 계수 값을 갖는다. 한편 AddRoundKey 변환은 State값과 라운드 키간의 XOR 연산으로 처리된다.

III. AES 알고리즘의 여러 가지 구현 방식 비교 분석

아래에 주어진 6가지 AES 동작 모델에 대해 상대적인 면적(A), 상대적인 연산 시간(T), AT, AT^2의 성능을 분석하였다. 6가지 모델에서 라운드 당 클록 수는 하나의 라운드를 수행하는데 필요한 클록 수를 의미하며, 파이프라인(P)은 부분 라운드간에 파이프라인 기법이 적용되었음을 의미한다. 그리고 PR은 라운드 키가 현재 라운드보다 앞선 이전 라운드에 미리 계산되었음을 나타낸다.

① 1-RP-4NP(1 round per 2 clocks with no pipeline)
② 1-RP-4P(1 round per 4 clocks with pipeline)
③ 1-RP-1NP-PR(1 round per 1 clocks with no pipeline and round key precomputation)
④ 1-RP-1NP(1 round per 1 clock with no pipeline)
⑤ 1-RP-8NP(1 round per 8 clocks with no pipeline)
⑥ 1-RP-8P(1 round per 8 clocks with pipeline)

6가지 모델에 대한 면적 분석 시 Synopsys 합성 소프트웨어를 사용하여, S-Box, ShiftRow_4, $GF((2^8)^4)$ 곱셈기[3], 32 비트 XOR회로, 32 비트 레지스터를 합성해서 게이트 수를 추출한 후, 각 모델에 필요한 모듈 개수만큼 곱해서 각 모델에 대한 근사적인 게이트 수를 계산하였다. 단, 암호와 복호 동작이 하나의 칩에 구현되어야 하므로 복호 동작에 기인한 하드웨어를 포함시켰다. 그리고 라운드 키 생성회로가 라운드 하드웨어보다 작은 지연 시간을 갖는 것으로 가정하였다. 그리고 연산 시간은 클록 주기와 사이클 수의 곱으로 평가하였는데, 라운드 동작을 부분 라운드로 분할하여 처리할 경우, 부분 라운드의 지연 시간이 동일한 값을 갖는 것으로 설정하였다. 반면 1-RP-1NP-PR의 경우 라운드 키의 사전 계산에 의해, 연산 완료에 소요되는 클록 사이클 수가 1만큼 증가하여 11로 평가하였다. 그림 3은 본 연구에서 채택한 1-RP-8P 방식을 면적과 연산 시간의 기준 값 1.0으로 설정한 후 나머지 5가지 모델에 대한 상대적인 면적(A), 상대적인 연산 시간(T), AT 성능, AT^2의 성능을 평가한 값을 나타내며, 값이 높을수록 우수한 특성을 의미한다.

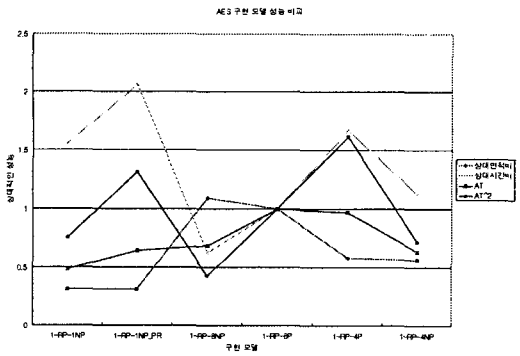

그림 3. 6가지 AES 구현 모델에 대한 상대 면적(A), 상대 연산 시간(T), AT, AT^2에 대한 성능 비교

그림에 보는 바와 같이 AT 성능은 1-RP-8P방식과 1-RP-4P 방식이 우수하며, AT^2 성능 척도를 사용할 경우 1-RP-4P 방식이 가장 바람직하며, 연산 시간(T)만을 고려할 경우 1-RP-1NP-PR 방식이 가장 우수한 결과를 보여준다. 본 연구에서는 AT 성능을 고려하여 1-RP-8P 구조를 채택하여 하드웨어를 설계하였다.

IV. AES 프로세서의 VLSI 설계

본 연구에서는 하드웨어 구현시 AES ShiftRow 연산은 행 단위로 수행되고, MixColumn 연산은 열 단위로 수행되는 연산 특성을 고려하여, 각 라운드를 2개의 부분 라운드로 나누고, 각 부분 라운드는 4 클록에 수행되며, 부분 라운드간에 파이프라인을 적용하는 그림 4의 AES 연산 기법(1-RP-8NP)을 프로세서 설계에 사용하였다.

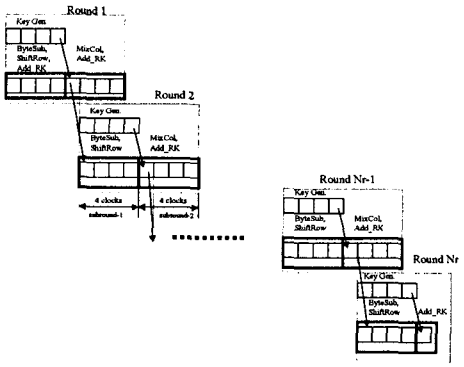

그림 4. 부분 라운드간 파이프라인과 온라인 라운드 키 계산을 사용한 AES 연산 기법

설계된 암호 프로세서의 블록도는 그림 5와 같다. 외부의 데이터 버스를 통해 암호 키와 CBC, CFB, OFB 모드에서 사용되는 초기값(IV) 데이터를 입력한다. 암호 동작과 외부 입출력 동작을 동시에 수행할 수 있도록 하여 입출력 시간에 따른 성능 저하를 방지하기 위해, 입·출력 버퍼 레지스터(I/O buffer Reg)과 내부 암호 코어의 입출력 레지스터(DIN/DOUT Reg.)를 분리시켰다. 즉, 암호 동작 중에 입·출력 버퍼 레지스터를 통해 입출력 동작을 수행할 수 있도록 하였으며, 새로운 암호 동작에 대한 시작 신호 발생시 DIN/DOUT 레지스터에 담긴 암·복호 결과와 I/O 버퍼 레지스터에 저장된 외부 입력 데이터를 서로 교환하는 동작을 수행한다. SR(status register) 레지스터는 동작 모드, 외부 인터페이스 방안, CFB와 OFB 모드 시 암· 복호 블록 단위를 지시하는 필드와 암호 키 길이 등의 제어 정보를 갖고 있다.

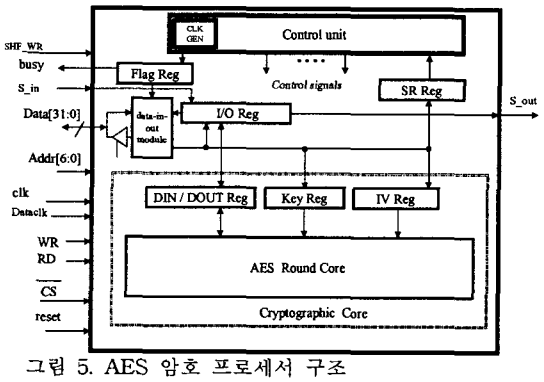

그림 5. AES 암호 프로세서 구조

그림 6은 암·복호 동작 수행시 라운드 동작과 온라인 라운드 키 생성 동작을 수행하는 AES 라운드 코어를 나타낸다. AES 라운드 데이터 패스는 암호 동작과 함께 복호 동작이 필요하므로, 기존 암호 기능을 위한 모듈에 기능을 복호 동작을 위한 기능을 추가해서 구현한다. 단, InvByteSub를 구현하는 Si-Box는 S-Box의 수정으로 변경이 불가능하므로, 별도로 병렬로 배치하며, 나머지 라운드 변환용 모듈은 기존 암호 동작에 복호 동작을 위한 기능을 추가하는 형태로 설계되었다. 복호 동작시에는 마지막 라운드에 사용하는 라운드 키부터 역순으로 라운드 키가 적용되어야 하는데, DES와 같은 블록 암호와 달리 마지막 라운드 키가 외부에서 제공되는 암호 키에서 직접 생성이 불가능하므로, 복호 동작 시에는 먼저 라운드 키 생성부를 라운드 회수만큼 수행해서 미리 마지막 라운드 키를 만들어 IC_Start_Key 레지스터에 저장해 두고, 복호

동작시 IC_Start_Key 레지스터에 담긴 마지막 라운드 키 값을 불러와 역순으로 라운드 키를 온라인 방식으로 생성하도록 하였다. 이러한 마지막 라운드용 라운드 키 생성 동작은 동일한 키를 사용하는 복호 동작시 한번만 필요하다. 이러한 마지막 라운드를 생성하고, IC_Start_Key 레지스터에 저장하는 동작은 외부 호스트 프로세서가 지시한다. 단, 라운드 키 계산 동작이 최악 경로가 되는 것을 방지하기 위해 라운드 키 계산에 4 클록을 할당하였다.

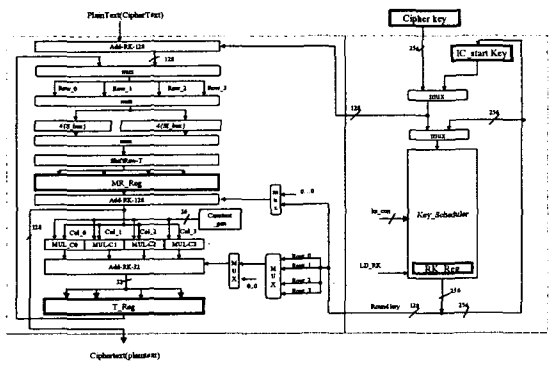

그림 5. AES 라운드 코어

V. 성능 분석

AES 암호 보조 프로세서 검증 과정에 AES 표준 공고안[4]에 명시한 테스트 벡터를 올바로 만족함을 확인하였다. 설계한 회로를 0.25 μm CMOS 라이브러리를 사용하여 Synopsys[5] 소프트웨어를 사용하여 합성하였다. 합성 결과 암호 보조 프로세서의 최악 동작 경로는 약 4.6ns로서 최대 동작 주파수는 200 Mhz이었으며, 총 게이트 수는 약 36,000이었다. 본 연구의 AES 암호 프로세서의 ECB와 CBC 모드에 대한 암·복호율은 다음식과 같다.

$$ECB와\ CBC\ 모드에\ 대한\ 암\cdot 복호율 = (\frac{128}{Nr*5})\times f$$

여기서 Nr은 라운드 수, f 는클록주파수

따라서 ECB 모드의 경우 암·복호율은 키가 128, 192, 256 비트인 경우 라운드 수가 10, 12, 14이므로, 각각 200Mhz 클록 조건에서 약 512 Mbps, 427 Mbps, 365 Mbps의 성능을 나타낸다.

본 연구의 AES 암호 보조 프로세서는 AT 성능이 뛰어나므로, 면적과 속도 측면이 모두 중시되는 보안 분야에 암호 모듈로 효율적으로 장착될 수 있을 것으로 판단된다. 그리고 본 연구의 라운드 데이타패스 구조는 S 박스와 $GF((2^8)^4)$곱셈기 등의 하드웨어 추가를 통해, 1-RP-4P 또는 1-RP-1NP-PR 구조로 쉽게 변경이 가능하다.

VI. 결론

본 논문에서는 면적 측면과 속도 측면에서 효율적인 AES 암호 보조 프로세서를 설계하였다. 설계한 AES 암호 보조 프로세서는 1 라운드 동작을 2개의 부분 라운드로 분할하며, 각 부분 라운드를 4 클록으로 처리하며, 부분 라운드간 파이프라인 기법을 사용하여 평균 5 클록에 1개의 라운드를 처리하는 구조를 갖는다. 면적과 속도 특성을 곱한 AT 성능 평가 기준으로 판단할 때 가장 효율적인 구조를 갖고 있음을 알 수 있었다. 또한 라운드 키를 온라인 방식으로 생성함에 의해서, 키 설정 지연 시간을 없애며 라운드 키를 저장하기 위한 별도의 메모리 공간을 제거할 수 있다. 현재 설계한 AES 칩은 약 36,000개의 게이트로 구성되며, 0.25 μm CMOS 공정에서 약 200 Mhz의 동작 주파수를 가지며, AES-128 ECB 모드에서 약 512 Mbps의 암·복호율를 얻을 수 있었다. 그리고 본 연구에서 설계한 암호 프로세서는 4가지 동작 모드와 3가지 키 길이(128, 192, 256 비트)를 모두 지원하는 구조를 갖고 있으므로, AES 암호 알고리즘이 적용되는 네트웍, 전자 상거래 시스템 등의 보안 모듈로 사용될 수 있을 것으로 판단된다.

감사의 글

본 논문은 "System IC 2010 선행 핵심 IP 연구개발" 사업의 지원으로 이루어졌으며, 회로 구현시 IDEC 지원 장비를 사용하였습니다.

참고 문헌

[1] William Stalling, *Cryptography and Network Security*, Prentice Hall, 1999.

[2] Miles E. Smid, "From DES to AES", 2000, http://www.nist.gov/aes.

[3] Christof *Parr, Efficient VLSI Architectures for Bit-Parallel Computations in Galois Fields,* Ph.D thesis, Institute for Experimental Mathematics, University of Essen, Essen, Germany, June, 1994.

[4] NIST, "Announcing the Advanced Encryption Standard(AES)", FIPS PUB ZZZ, 2001, http://www.nist.gov/aes.

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