AES-128 암호화 칩의 VHDL 설계*

김방현[0] 김태규 김종현
연세대학교 전산학과
legnamai@chol.com[0], windcry@korea.com, jhkim@dragon.yonsei.ac.kr

VHDL Design of AES-128 Crypto-Chip

Bang-Hyun Kim[0] Tae-Kyu Kim Jong-Hyun Kim
Dept. of Computer Science, Yonsei University

요 약

정보 보안을 위한 암호화 처리는 각종 컴퓨터 시스템이나 통신시스템에서 부가적으로 수행되기 때문에 암호화 속도가 느린 경우에는 시스템의 속도 지연을 유발시키게 된다. 따라서 고속의 컴퓨터 연산이나 고속통신에 있어서 이에 맞는 고속의 암호화는 필수적으로 해결되어야 할 과제인데, 이것은 암호화 및 복호화를 하드웨어로 처리함으로서 가능하다.

본 연구에서는 차세대 표준 암호화 알고리즘인 AES-128의 암호화와 복호화를 단일 ASIC칩에 구현하고, 인터페이스 핀의 수와 내부 모듈간의 버스 폭에 따른 칩의 효율성을 평가하였다. 이 연구에서 VHDL 설계 및 시뮬레이션은 Altera 사의 MaxPlus2 9.64를 이용하였으며, ASIC 칩은 Altera 사의 FLEX10KE 계열 칩을 사용하였다.

1. 서 론

정보화 시대에서 무형의 정보의 가치는 유형의 가치에 비해 상대적으로 높기 때문에 정보 보호에 대한 많은 연구가 진행되고 있다. 그 중에서 암호화 기술은 정보의 의미를 당사자 이외에는 알지 못하게 정보를 변환시켜 정보를 보호하는 방법을 말한다. 이러한 암호화 기술은 최근에 인터넷을 통하여 방대한 정보 교환이 이루어짐에 따라 그 중요성이 더욱 커지고 있다.

1998년을 기점으로 표준 기한이 만료된 DES를 대체할 블록 암호의 필요성에 따라, NIST에서는 향후 정부와 산업체에서 사용할 수 있는 블록 암호화 알고리즘 표준으로 AES(Advanced Encryption Standard)의 개발을 추진하였다. NIST는 DES보다 더 효율적이고 안전한 알고리즘을 공모하여 2000년 10월 2일에 Rijndael을 최종 AES 알고리즘으로 선정하여 발표하였다[1]. Rijndael 알고리즘은 기존에 알려진 암호 공격법에 대하여 안전하며 다양한 시스템 환경에서 암호화 속도와 복호화 속도, 그리고 소스코드의 크기가 합리적이라는 점에서 특징이 있다. 발표 이후 NIST는 Rijndael을 공개적으로 검토하고 수정작업을 거쳐 연방정보처리표준(FIPS: Federal Information Processing Standard)으로 선정하였으며, 표준화 작업은 2001년 여름에 완료되었다[2].

일반적으로 어떤 시스템에 암호화를 적용할 경우 암호화 처리는 각종 컴퓨터 시스템이나 통신시스템에서 부가적인 처리로 적용되어지기 때문에 느린 암호화 처리가 시스템의 속도 지연을 발생시키게 된다[3]. 따라서 고속의 컴퓨터 연산이나 고속통신에 있어서 이에 맞는 고속의 암호화는 필수적으로 해결되어야 할 과제이다. 이에 처리 속도의 향상을 위한 연구가 다각도로 이루어지고 있으나, 국내에서는 아직도 정보 보호를 위한 시스템들의 대부분이 소프트웨어로 구현되고 있는 실정이다. 그러나 실시간 통신이나 고속통신시스템 등과 같은 응용분야에 암호화를 적용하기 위해서는 하드웨어로 구현하여 속도를 높여야 한다[4].

암호 알고리즘을 하드웨어로 구현할 경우에는 일반적으로 ASIC(Application Specific Integrated Circuit)칩으로 구현되는데, 하드웨어 특성에 의한 제약과 비용 때문에 여러 가지 방법이 사용되고 있다. 본 연구에서는 Rijndael을 위한 ASIC칩을 설계하였으며, 인터페이스 핀의 수와 내부 모듈간의 데이터 버스 폭에 따른 칩 구현의 효율성을 평가하였다. 실험은 데이터의 길이와 키의 길이가 128비트인 경우에 외부 인터페이스 핀의 수와 내부 모듈간의 데이터 버스 폭이 8, 16, 32, 64, 128 비트인 경우에 대하여 ASIC칩을 각각 VHDL로 설계하여 결과를 비교하였다. VHDL 구현 및 시뮬레이션은 Altera 사의 MaxPlus2 9.64를 이용하였으며, ASIC 칩은 Altera 사의 FLEX10KE 계열 칩을 사용하였다.

2. AES 블록 암호화 알고리즘

Rijndael 알고리즘은 암호화와 복호화에 필요한 키를 동일하게 가지는 대칭 블록 암호 알고리즘으로서 128,

* 이 연구는 2001년도 정보통신부 대학기초연구지원사업의 지원에 의해 이루어졌음

192, 256 비트의 블록 크기와 키 길이를 지원한다. 또한 암호화 키 길이와 암호화의 기본 단위인 블록의 크기를 128, 192, 256 비트 등으로 선택할 수 있다. 따라서 이 알고리즘에서는 키와 블록의 크기를 조합한 9가지의 다양한 선택이 가능하지만, 표준에서는 데이터 블록의 크기는 128비트로 고정하고 키의 크기는 128, 192, 256비트 중에서 선택할 수 있도록 제한하였다[5]. 이 알고리즘은 암호의 불법적 해독을 막기 위하여 핵심기술인 S-박스(s-box)의 설계에 유한체(finite field)라는 고급 수학을 적용하였다[6].

FIPS에서는 Rijndael 알고리즘 중에서 128, 192, 256 비트의 길이를 가진 암호 키를 이용하여 128비트의 데이터 블록을 처리하는 경우만 표준으로 채택하였고 나머지 경우에 대해서는 채택하지 않았으며 이 표준에서 상술된 알고리즘을 "AES 알고리즘"이라 명명하였다. AES 알고리즘에서는 길이가 128, 192, 256 비트인 키가 사용될 수 있는데, 이러한 키들에 대해 각각 "AES-128", "AES-192" 및 "AES-256"라 명명하였다[5]. 본 연구에서는 AES-128을 위한 ASIC 칩을 VHDL로 설계하여 시뮬레이션 했으며, 암호화 및 복호화 처리 시간과 하드웨어 복잡도를 분석하였다.

3. AES-128 칩의 VHDL 설계

ASIC 칩에서 외부 인터페이스 핀의 수와 내부 모듈간의 데이터 버스 폭은 적절한 선택이 필요하다. 응용마다 차이는 있지만 대부분 응용에서 인터페이스 핀의 수가 늘어나면 평문 입력을 입출력하는데 걸리는 시간이 단축되어 처리 속도는 빨라지지만 하드웨어 복잡도가 증가한다. 하드웨어 복잡도의 증가는 ASIC 칩에서는 비용을 의미하며, 주변 인터페이스 회로도 복잡해지는 단점이 있다.

따라서 본 연구에서 설계한 AES-128 암호화 칩은 단일 칩에 암호화 회로와 복호화 회로를 모두 포함하도록 설계하였으며, 'Type' 신호를 이용하여 암호화와 복호화가 동작을 선택할 수 있도록 하였다. 또한 키 입력과 평문 데이터 입력이 하나의 인터페이스를 공유하며, 'Select' 신호를 이용하여 선택할 수 있도록 하였다. 내부 알고리즘 처리는 반복 라운드 형태(Feedback-modes)로 처리되며, 내부 모듈간의 데이터 버스 폭을 외부 인터페이스 핀의 수와 동일하도록 설계하였다. 그리고 S-박스는 Altera FLEX 10KE 계열에 내장된 배열 블록(EAB: Embedded Array Block)을 이용하여 구현하였다. 본 연구에서 설계한 AES-128 암호화 칩의 전체적인 외부 인터페이스는 그림 1과 같다.

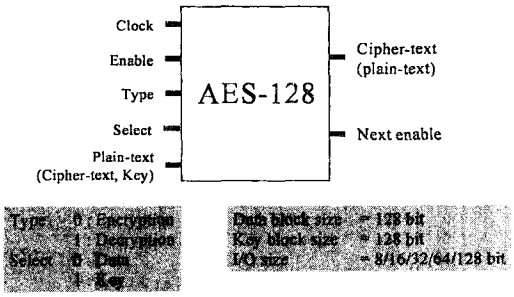

그림 1. AES-128 칩의 인터페이스

내부 모듈은 AES 제어기(AES controller), 키 생성기(key generator), 버퍼, S-Box, AES Core로 구성된다. 그리고 암호처리기는 Sub-Byte, Shift Row, Mix Column, Add Round Key로 구성되는데, 'Type' 신호에 따라서 AES 제어기의 제어 신호를 받아 암호화 또는 복호화의 부분 기능으로 동작된다. 버퍼는 'Select' 신호에 따라서 입력된 키의 버퍼로 사용되거나 데이터 버퍼로 사용된다. 그림 2는 인터페이스의 핀의 수와 내부 모듈간의 버스 폭이 32비트인 경우에 본 연구에서 설계한 AES-128 암호화 칩의 내부 구조를 보여준다.

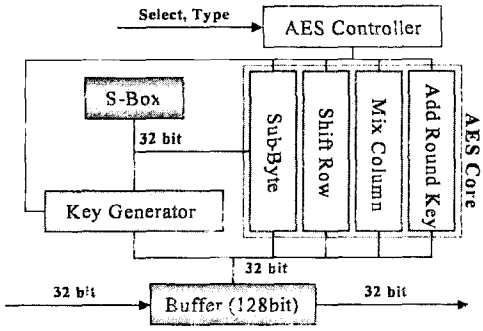

그림 2. AES-128 암호화 칩의 내부 구조

4. 실험 결과

실험은 외부 인터페이스 핀의 수와 내부 모듈간의 데이터 버스 폭이 8, 16, 32, 64, 128 비트인 경우에 대하여 수행하였다. 시뮬레이션 결과, 처리 속도는 인터페이스의 폭이 증가할수록 빨라졌는데, 이것은 전체적인 데이터 입출력과 내부 모듈간의 데이터 입출력에서 소요되는 시간이 단축되기 때문이다. 예를 들어, 8비트인 경우

에는 데이터 입출력을 위하여 최소 16클럭이 소요되기 때문이다. 그림 3은 인터페이스 폭과 암호화 시간의 상관관계를 보여주고 있다.

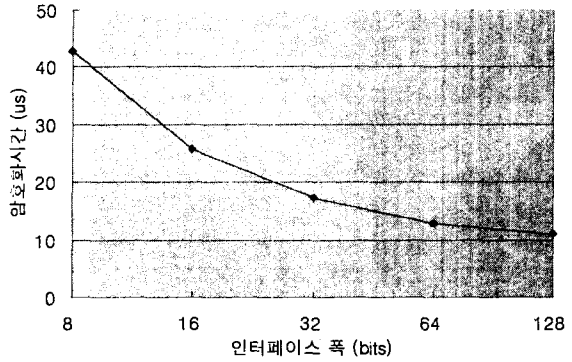

그림 3. 인터페이스 폭에 따른 암호화 시간

그러나 하드웨어 복잡도는 인터페이스의 폭이 증가할수록 감소하다가 32비트일 때 최소가 되고, 그 이후에는 다시 증가하는 결과를 보였다. 이것은 128비트를 나누어 처리할 때 카운트와 쉬프트를 처리하는 부가 회로에 필요한 논리 셀(logic cells)의 수와 인터페이스에 필요한 논리 셀(synthesized logic cells)의 수의 상대적인 비율에 따라서 나타나는 현상이다. 즉, 인터페이스의 폭이 증가하면 부가 회로에 필요한 논리 셀의 수는 감소하지만 인터페이스에 필요한 셀의 수는 증가하기 때문이다. 그림 4는 인터페이스 폭과 하드웨어 복잡도간의 상관관계를 보여준다.

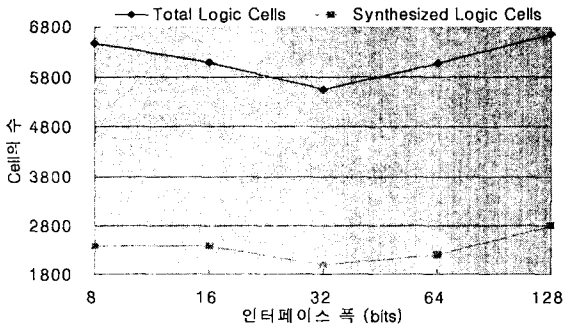

그림 4. 인터페이스 폭에 따른 하드웨어 복잡도

실험결과에 따르면, 인터페이스의 폭이 증가할수록 속도는 증가하지만, ASIC 칩의 하드웨어 복잡도를 고려할 때 가장 효율적인 인터페이스 폭은 32비트인 것으로 볼 수 있다.

5. 결론 및 향후 연구과제

본 연구에서는 최근 새로이 국제 암호화 표준 알고리즘으로 채택된 AES-128 암호화 알고리즘의 암호화와 복호화를 단일 ASIC칩으로 구현하고, 외부 인터페이스 핀의 수와 내부 모듈간의 데이터 버스 폭에 따른 칩의 효율성을 평가하였다. 실험 결과에 따르면, 외부 인터페이스 핀의 수와 내부 모듈간의 데이터 버스 폭이 32비트일 때에 효율성이 가장 좋은 것을 알 수 있었다.

AES 알고리즘은 병렬성이 많이 존재하기 때문에 루프 언롤링(loop unrolling), 내부 라운드 파이프라이닝(inner-round pipelining), 외부 라운드 파이프라이닝(outer-round pipelining), 자원 공유(resource sharing)와 같은 다양한 방법으로 성능을 향상시킬 수 있다[7]. 향후에는 이러한 다양한 방법을 본 연구에 적용하여 AES 칩이 최적의 성능과 효율성을 가질 수 있도록 하는 연구를 계속 진행할 예정이다.

참 고 문 헌

[1] Advanced Encryption Standard Home Page : http://csrc.nist.gov/encryption/aes.

[2] U.S. Department of Commerce, National Institute of Standards and Technology, "Draft Federal Information Processing Standards(FIPS) for the Advanced Encryption Standard," February 2001.

[3] Charles P. Pfleeger. Security in Computing, Prentice Hall. 1989.

[4] Kazumaro Aoki, Helger Lipmaa, "Fast Implementations of AES Cadidates," The Third Advanced Encryption Standard (AES3) Candidate Conference, April 13, 2000.

[5] E. Roback and M. Dworkin, "First Advanced Encryption Standard(AES) Candidate Conference," Journal of Research of the National Institute of Standards and Technology, vol. 104, no. 1, pp. 97-105, 1999.

[6] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," Document version 2, March 9, 1999, http://www.esat.kuleuven.ac.be/~rijmen/rijndael.

[7] Kris Gaj and Pawel Chodowiec, "Comparison of the hardware performance of the AES candidates using reconfigurable hardware," The Third Advanced Encryption Standard (AES3) Candidate Conference, April 13, 2000.