AES/SEED암호화 모듈 설계와 멀티레벨 보안 시스템 구현

박 덕 용, 최 경 문, 김 현 성, 차 재 원, 김 영 철
전남대학교 전자공학과
전화 : 062-530-0369 / 핸드폰 : 019-608-0273

Design of AES/SEED Encription Module and Implemention of Multi-Level Security System

Duck Ryong Park, Kyung Mun Choi, Hyun Sung Kim, Jae Won Cha, Yong Chol Kim
Dept. of Electronic Engineering, Chonnam National University
E-mail : drpark@neuron.chonnam.ac.kr

Abstract

This paper has been studied about the implemention of the data-encription processor and imformation security system. Also in the paper, the brief contents of the verification of the data-encryption algorithm and the method of using HDL-level sources implemented is described.

And then this paper has been designed for multi-level data secure system to verify and analyze the data-encryption processor implemented as VHDL.

I. 서론

IT산업의 발전과 더불어 영상 컨텐츠를 활용한 인터넷 정보산업이 발전하고 있다. 특히 웹카메라와 같은 멀티미디어를 지원하는 장비의 기술발전과 대중화로 인하여 특정 장소의 보안을 위한 원격 감시나 원격 접속이 보편화 되고 있는 추세이다. 그러나 웹카메라를 이용한 영상 전송 시스템들 중 데이터를 제 3자로부터 보호할 수 있는 장치들을 갖춘 시스템이나 장비는 극소수이다. 정보화 사회의 발전을 위해서는 정보의 보안을 유지하면서 데이터의 고속 처리가 가능한 시스템의 구현이 필수적이다.

본 논문에서는 다양한 응용에 적용 가능한 보안모듈과 외부디바이스와 Local Bus를 제어할 수 있는 제어모듈을 내장한 암복호화 프로세서와 응용시스템을 구현하였다. 데이터 보안 모듈은 AES와 SEED알고리즘을 이용하여 하드웨어로 구현하였다. 대용량 데이터의 고속 처리를 위해 메모리 및 버스 컨트롤러를 구현하였으며, 응용시스템은 32bit 전송이 가능한 PCI를 사용한 윈도우2000기반의 응용시스템을 구축하였다.

※ 본 논문은 일부 "한국과학재단 지정 전남대학교 고품질 전기전자부품 및 시스템 연구센터의 연구비 지원"과 "IDEC의 CAD툴 지원"에 의해 이루어졌음.

II AES/SEED 암호화 모듈 구현

2.1. AES/SEED암호 알고리즘

SEED 암호 알고리즘은 1999년 11월 TTA(Telecommunications Technology Association)에서 발표한 한국 표준 블록 암호화 알고리즘[1]이다.

미국 상무부 기술 표준국(NIST : National Institute of Standards and Technology)에서 시행한 AES (Advanced Encryption Standard) 공모에서 2000년 10월 벨기에의 Rijndael 알고리즘이 선정되었으며[2], 2001년 11월에는 미 연방 표준(FIPS 197 : Federal Information Processing Standards Publication 197)으로도 채택되었다[3].

2.1.1. AES암호화 알고리즘

벨기에의 Joan Daemen과 Vincent Rijmen에 의해 개발되었으며, SPN(Substitution Permutation Network) 구조의 가변 블록 길이를 지원하는 블록암호로, 지원 블록 길이에 따른 Key Length, Block Size, 라운드 수등은 '표 1'에 정리되어 있다.

암호 연산 처리 과정(그림 1)은 초기 라운드에 AddRoundKey 연산을 수행한 후, 최종 라운드를 제외한 각 라운드((Nr-1)회)는 SubByte, ShiftRow, MixColumn, AddRoundKey 4종류의 연산(변환)으로 구성된다. 최초 1차원 형태의 128비트의 입력 데이터(블록)가 들어오면, 2차원 형태(4행×Nb열(Nb=4))로 구성되는 State로 변환한 후, State내 byte 배열에 대해 연산을 수행한다. 즉 State는 내부 연산에 사용되는 블록을 의미한다.

표 1. 키 길이에 따른 라운드 수 변화

	키 길이	블록 크기	라운드 수
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

2.1.2. SEED암호화 알고리즘

SEED 암호 알고리즘은 DES 알고리즘과 같은 Feistal 구조를 갖고 있으며, 입출력 처리 기본 단위(블록크기)가 128 비트인 한국 표준 암호 알고리즘으로 TTA 를 통하여 발표 되었다. 이러한 SEED 암호 알고리즘의 전체 동작은 128비트의 평문 블록 단위 당 128비트의 입력키로 부터 생성된 16개의 64비트 라운드 키를 입력를 사용하고 있으며, 총 16 라운드를 거쳐 128비트 암호문 블록을 출력하는 구조이다.

2.2. AES/SEED암호화 알고리즘의 하드웨어 구현[4]

자원의 효율적인 공유와 높은 암·복호율을 가질 수 있도록 두 알고리즘 모두 라운드 변환을 반복 처리하는 구조를 채택하였으며, 암·복호화율 향상 및 칩 면적 감소를 위해 critical path에 해당하는 연산 블록을 분리한 후, pipeline 기법을 적용하여 component를 반복 사용할 수 있도록 설계하였다.

AES 알고리즘은 SubByte와 Mix-Column 연산블록을 각각 분리하여 하나의 라운드를 2개의 부분 라운드로 나누고, 각 부분 라운드를 4개의 clock으로 구현하여 32비트의 라운드 연산 블록으로 128비트를 처리 할 수 있는 pipeline 방식(그림 1)을 적용하였다[5].

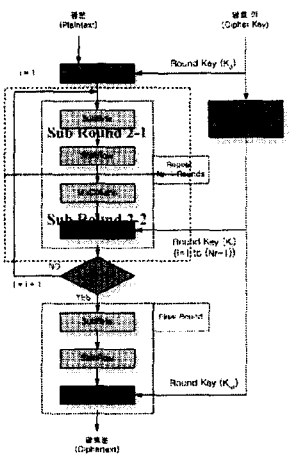

그림 1. AES 암호화를 위한 Pipeline 동작

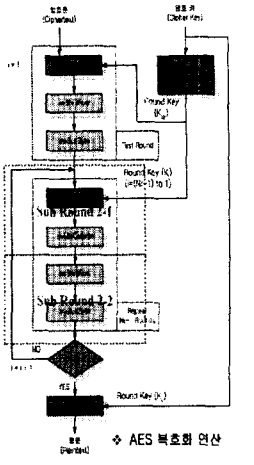

그림 2. AES 복호화를 위한 Pipeline 동작

SubByte 블록은 곱셈기와 역원 생성회로 기능을 등가 구현할 수 있는 치환 테이블 S-Box와 그 역동작을 수행하는 Inverse S-Box로 구현하였으며, MixColumn 연산 블록은 비트 단위의 *modulo-2* 덧셈 연산으로 변경하여 구현하였다[6].

SEED알고리즘의 내부 연산은 크게 F함수, G함수로 구성되어 있다. F함수 및 라운드 키 생성 블록 내부에 pipeline구조를 적용하기 위해 1-round를 3-clock으로 처리할 수 있게 설계하였으며, 이로 인해 각각 하나의 덧셈 및 뺄셈 연산 블록과 G함수 연산블록을 가지고 라운드 연산을 처리 할 수 있게 되었다.

'그림 3'는 AES와 SEED 알고리즘을 통합 구현한 구성도를 보여주고 있다.

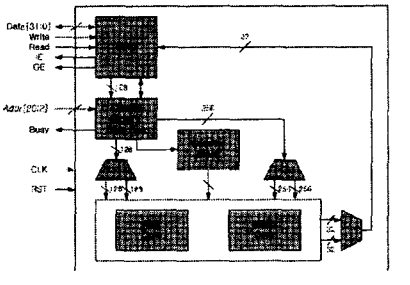

그림 3. AES, SEED 통합 구조

2.3 AES/SEED 암호화 모듈의 검증

설계된 암호 프로세서는 Xilinx Foundation 4.1을 사용하여 합성 및 시뮬레이션을 수행하였으며, 입력 데이터는 표준문서에 명시되어 있는 test vector를 사용하였다. 실제적인 동작 검증을 위해서는 FPGA prototype board(Xilinx XCV-1000E FPGA)에 설계된

암호 프로세서의 비트 스트림 파일을 다운로드 시켜 logic debugger를 통해 검증하였으며, Xilinx timing simulation과 logic debugger 출력 값을 표준문서의 데이터와 비교하여 구현모듈을 검증하였다.

Ⅲ AES/SEED암호화 모듈을 내장한 멀티레벨 보안시스템의 구현

3.1 멀티레벨 보안시스템의 개요

멀티레벨 보안 시스템의 전체적인 구성은 '그림 4'에서와 같이 웹카메라로부터 입력 받은 영상데이터는 응용소프트웨어에 의해 MPEG Codec으로 압축되며, 압축된 영상 데이터는 PCI 보드[7]로 구현된 로컬 시스템을 통해 암호화된다. 암호화된 데이터는 데이터의 복호화를 위해 구현된 응용소프트웨어나 하드웨어에 의해서만이 복호화 및 재생이 가능하다.

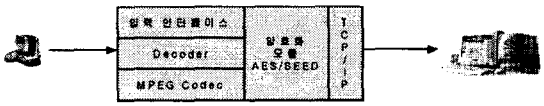

그림 4. 멀티레벨 보안시스템 구성도

3.2 멀티레벨 보안시스템의 구현

멀티레벨 보안 시스템은 하드웨어와 소프트웨어 구성되며, 하드웨어는 입력된 데이터의 암호화 및 복호화를 그리고 소프트웨어는 입력된 영상데이터의 압축과 재생 및 저장 그리고 구현된 하드웨어의 옵션 설정 및 제어를 수행한다.

3.2.1. 응용 하드웨어 구현[8]

하드웨어의 구성은 '그림 5'에서 보는 바와 같이 5개의 주요 블록과 2개의 Configuration 블록으로 이루어져 있다.

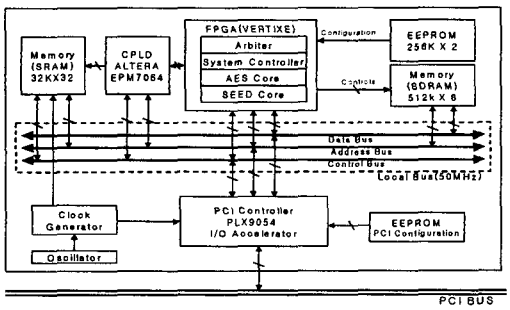

그림 5. 멀티레벨 보안시스템 HW블록

'그림 6'은 실제 구현된 PCI 보드이며, 블록도에 나와 있는바와 같이 PCI Controller(①), FPGA Block(②), FPGA를 Configuration하기 위한 EPROM Block(③), 암호화 Core가 내장되어 있는 프로세서의 데이터 처리속도를 보장하기 위한 메모리 블록(④), PCI Controller의 전송속도를 향상시키기위한 서브메모리 블록(⑤) 그리고 서브메모리와 외부 디바이스 및 로컬 버스의 상태를 Control하기 위한 Controller의 구성이 가능한 CPLD Block(⑥)으로 구성되어 있다.

데이터 버스는 고속 전송을 위하여 PLX사의 PLX9054[9]를 사용하여 32-bit PCI 방식으로 구현하였으며, 내부 데이터 전송 및 처리를 위하여 50MHz의 로컬 버스를 구성하였다.

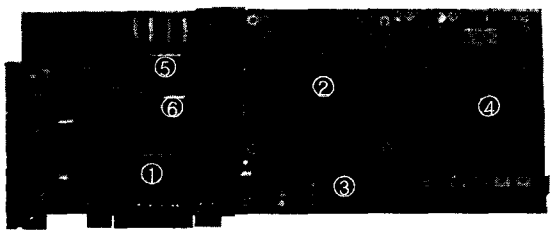

그림 6. 구현된 보안 시스템 PCI 보드

FPGA Block[10]은 100만 Gate Level의 칩을 사용하여 AES/SEED Core와 인터페이스 블록 그리고 별도의 시스템 컨트롤러 블록을 통합하여 구현하였다. 메모리 블록(④)은 512K X 8 SDRAM 4개를 사용하여 32-bit size의 입출력 데이터를 저장할 수 있도록 하였으며, 암복호화 프로세서의 고속 데이터 전송 및 처리를 가능하게 하였다.

3.2.2. 응용 소프트웨어 구현

소프트웨어는 PCI 디바이스 드라이버를 제어하는 기능과 암복호화된 영상을 재생 및 저장하는 기능, 그리고 사용자 인증 기능과 하드웨어로 암호화된 데이터를 소프트웨어로 복호화 하는 기능을 옵션으로 설정하여 테스트가 용이하게 구현하였다.

응용프로그램은 입력 데이터를 암호화 하여 전송하는 서버의 기능을 구현한 서버용 어플리케이션('그림 7-1')과 서버로부터 전송되는 데이터를 받아서 사용자에게 결과를 보여주는 클라이언트용 어플리케이션('그림 7-2')으로 분리하여 구현하였다. 각각 데이터의 암복호와 성능 및 전송 성능 분석을 위한 영상 암복호화시 수행 시간 분석기능('그림 8')과 데이터 전송시 전송 delay를 분석하는 기능들을 내장하고 있다.

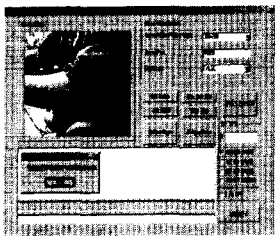

그림 7-1. 서버용 응용 프로그램

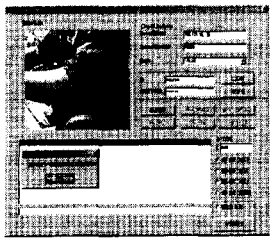

그림 7-2. 클라이언트용 응용 프로그램

'그림 7-1'과 '그림 7-2'는 서버/클라이언트용 응용프로그램으로써 하드웨어 설정 기능 및 암복호화 기능, 전송기능과 하드웨어 테스트기능을 갖추고 있다.

그림 8. 응용프로그램의 영상 및 파일 암복호화

3.3. 멀티레벨 보안시스템의 구현 결과 및 성능 검증

영상데이터의 입력과 압축을 위한 Codec부분의 처리는 MS VC++6.0을 이용하여 구현하였으며, 암복호화 프로세서는 FPGA로 구현하여 PCI보드에 장착하였다.

성능 분석은 데이터의 암호복호화 수행 시간을 소프트웨어로 처리한 결과와 구현한 하드웨어로 처리한 결과를 비교하는 방법에 의해 실행하였으며, 그 결과는 '표 2'에 정리 하였다. '표 2'에서 보면 데이터의 암복호화 수행효율면에서 AES128의 경우 8sec가 향상되었으며, AES256의 경우 11.4sec가 향상되었다. SEED의 경우 7.3sec 향상되었다.

표 2. HW/SW 모듈의 데이터 암호화 시간

처리방식	키 길이	Stream (36Mbyte)	File (36MByte)
SW	AES(128)	14.4sec.	11.316sec.
	AES(256)	19.2sec.	13.148sec.
	SEED(128)	13.5sec.	11.203sec.
HW	AES(128)	6.4sec.	4.8sec.
	AES(256)	7.8sec	5.7sec.
	SEED(128)	6.2sec.	4.6sec.

Ⅳ 결론

본 논문에서는 웹 카메라의 보안을 위해서 국내외 대표적 블록 암호 알고리즘 표준인 SEED와 AES(128, 192, 256-bit key) 알고리즘을 통합 구현하여 다양한 분야에 널리 사용할 수 있는 암호 프로세서와 검증을 위한 응용시스템을 설계하였으며, 시스템 레벨의 검증을 수행하였다. FPGA로 구현된 암복호화 프로세서는 제한된 하드웨어를 요구하는 분야에서 사용될 수 있도록 두 알고리즘 모두 라운드 변환을 반복 처리하는 구조를 채택하였으며, critical path에 해당하는 연산 블록을 분리한 후, 내부에 pipeline 기법을 적용하여 component를 반복 사용함으로써 약 3배의 면적 감소 효과를 얻을 수 있었다.

본 논문에서 구현한 암호 프로세서는 작은 면적을 요구하는 smart card, 휴대 단말기, 정보가전등에 효과적으로 사용될 것으로 기대된다. 또한 구현한 암호 프로세서는 다양한 응용분야에 적용이 가능한 웹 카메라 보안 시스템 칩으로 구현된다면 현재의 보안 시스템에 유용하게 사용될것으로 기대된다.

참고문헌

[1] 한국정보통신기술협회, 128비트 블록 암호 알고리즘 표준, (TTA.KO-12.0004), 1999. 9

[2] NIST(National Institute of Standards and Technology), "Advanced Encryption Standard(AES) Development Effort", Oct. 2000

[3] NIST(National Institute of Standards and Technology), "FIPS 197 : Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Nov. 2001

[4] 구양서 ,김영철, "블록 암호화 IP의 FPGA검증", 한국정보처리학회 논문집 9권 2호, pp.897-900, 2002. 11.

[5] 최병윤, "AES Rijndael 알고리즘용 암호 프로세서의 설계", 한국통신학회 논문지 26권10B호, pp.1491-1500, 2001. 10

[6] Pawel Chodowiec, "Experimental Testing of the Gigabit IPSec- Compliant Implementations of Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board", Proc. Information Security Conference, Oct. 2001

[7] 동역메카트로닉스연구소 기술정보실 편저, "PCI 버스해설과 인터페이스 카드 설계", 국제테크노 연구소

[8] Edward Sollari & George Willse,"PCI System Architecture (4th Edition)",Addison-Wesley,1999.

[9] PLX9054 Data Sheet, www.plxtech.com

[10] Xilinx FPGA Manual, www.xilinx.com