DICOM 의료정보보호를 위한 면적효율적인 통합 TLS 보안 프로세서의 구현

장우영, 류상준, 김영철
전남대학교 전자정보통신공학과

e-mail: wyjang@neuron.chonnam.ac.kr

Implementation of Area Efficient Integrated TLS Security Processor for DICOM Medical Information Security

Woo-Young Jang, Young-Chul Kim
Dept. of Electronics, Information Communication Engineering
Chonnam National University, Gwangju, Korea

요 약

본 논문은 의료영상진단시스템에서의 의료정보보호를 위한TLS 프로세서의 구현에 관하여 기술하였다. DICOM 3.0 standard의 'Part 15. DICOM Security Profile'에서는 TLS와 ISCL 두 가지의 Secure Transport Connection Profile을 정의하고 있고, 인증, 데이터의 무결성 보장, 프리아버시 보호의 기능을 할 수 있도록 몇가지의 알고리즘을 사용할 것을 정의하고 있다. 그 중 TLS Security Profile에는 Triple DES CBC모드와, RSA and SHA를 정의하고 있다. 그리하여 본 논문에서는 세 알고리즘의 개별적인 동작 검증을 마친 후 통합된 TLS Processor를 설계하고 검증하였다. 일반적인 Mux만을 이용한 설계는 임베디드 시스템 적용에 있어서 면적을 많이 차지하는 단점이 나타났다. 따라서 면적을 많이 차지하는 레지스터를 줄이기 위해서 세 알고리즘 블록이 같은 레지스터를 공유하도록 설계하였다. 그리고 임베디드시스템 개발 키트인 IFC-ETK100장비의 FPGA에 회로를 올리고 검증하였다.

1. 서론

21세기에 들어서면서 각종 첨담 전자 분야 등의 IT기술이 급속도로 발전하면서 의료 분야에서도 원격진료와 원격처방 그리고 가정용 또는 휴대용으로 진료장비에 대한 기술이 연구되어 지고 있고, 의료영상 저장 및 전송시스템(PACS:Picture Archiving Communication) 및 의무기록 전산화 시스템(EMR:Electronic Medical Record), 처방전달 시스템(OCS:Order Communication System)등이 확대 보급되고 있다. 또한 이러한 의료장비들이 이더넷과 같은 각종 유무선 통신장비를 통해 네트워크화 되고 PACS의 등장에 따라 환자 정보, 의료장비 정보, 검진용 의료영상 등의 표준화가 핵심 이슈로 등장 하였으며 수년전부터 미국과 유럽의 선진국 중심으로 표준화가 진행되었다. 그리고 개방형 정보통신망을 통하여 생명과 관계된 중요한 정보들에 다른 사람들이 손쉽게 환자정보를 접근할 수 있게 되었고 이러한 각종 의료정보들에 대한 보호 및 보안기술 개발 및 연구가 아직 국내외적으로 미비한 실정이다. 따라서 전세계적으로 널리 쓰이는 DICOM 의료영상전송 표준에 명시된 정보기술 중 TLS 방식의 보안프로세서에 대한 H/W 칩구현에 대하여 연구하고자 하였다.

※이 논문은 RRC와 IDEC CAD Tool 지원사업의 연구결과에 의해 작성되었습니다.

2. 연구내용

2.1 DICOM TLS Secure Profiles

TLS 보안전송연결의 구현은 Transport Layer Security Version 1.0 프로토콜에 명시된 메카니즘을 따른다. 다음의 표 1은 TLS를 위한 기본적인 메카니즘을 보여준다.

표 1. TLS Secure Profile

Supported TLS Feature	Minimum Mechanism
Entity Authentication	RSA based certificates
Exchange of Master Secrets	RSA
Data Integrity	SHA
Privacy	Triple DES EDE, CBC

이 프로파일은 TLS의 모든 특성을 지원하는 구현을 요구하지 않는다. 그리고 TLS 채널을 형성하는 동안 협상에 의해 동의되어진다면 다른 메카니즘들 또한 사용되어질 수 있다. TLS 연결들을 수용하는 구현상에서 IP 포트들 또는 선택되어지거나 형성된 포트 넘버는 컨포먼스 기술에 명시되어져 있다. 여기서, TLS 보안전송연결 프로파일을 지원하는 시스템은 TLS 위에서 DICOM Upper Layer Protocol을 위해 2762 포트넘버를 등록되어진 포트를 사용한다.

프로파일은 TLS 보안전송연결이 어떻게 성립되어지는지나, peer entity를 인증하는 동안 교환되는 어떤 인증서의 중요성을 명시하고 있지 않는다. 이러한 이슈들은 아마 보안정책이 명시된 몇 사이트를 따르는 어플리케이션 엔터티로 돌려진다. 인증자의 주체는 감사 로그 지원을 위해 어플리케이션 엔터티나 몇 외부제어권 컨트롤 프레임워크에 기반한 엄격한 제어에 의해 사용되어질 수 있다. 한 어플리케이션 엔터티는 보안전송연결을 성립해왔고, 그런 다음에 Upper Layer 협상은 보안 채널을 사용할 수 있다. PDU 크기와 TLS 기록 사이즈 사이의 상호 연결이 전송효율을 높이기 위해 존재할 것이다. TLS 기록 사이즈를 따른 최대크기는 PDU 크기를 따른 최대크기보다 작다.

무결성 체크가 실패할 경우, 연결은 구현명세제공자원인과 함께 Upper Layer로의 A-P-ABORT 지시를 화제화하기 위한 송신자와 수신자 모두를 야기하는 TLS 프로토콜 상에서 해제된다. 사용되어진 제공자 원인은 컨포먼스 기술에 문서화 되어 있다. 여기서 무결성 체크 실패는 채널 보안이 타협되어져 왔음을 가르킨다.

2.2 레지스터 공유 구조 방식의 TLS 기반 보안 프로세서 설계

2.2.1 각 알고리즘 레지스터 사용 분석

가. Triple DES 레지스터

표 2 Triple DES 레지스터의 사용량

암복호시 Key값 register	Round연산 저장 register
64bit*16개 =1024 2개	64bit

나. RSA 레지스터

표 3 RSA 레지스터의 사용량

곱셈연산 shifted register	Top block 값저장 non-shifted register
1026*2개	1026bit

다. SHA 레지스터

표 4 SHA 레지스터의 사용량

각 Step 값저장 register	x block register
160bit	32bit *80개 =2560bit

그림1은 각 알고리즘의 레지스터의 사용량을 나타낸다.

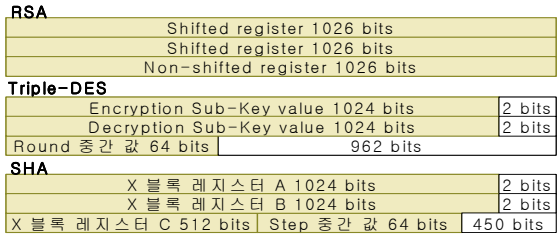

그림 1 각 알고리즘별 레지스터 공유 필요 레지스터

2.2.2 레지스터 공유구조 설계

단순 3단 MUX 구조를 사용하였을 경우 레지스터 사용량이 알고리즘 별로 방대하고, I/O 인터페이스 부분에서 입력 32 bits들을 1024 bit 크기로 만들어 내는데 필요한 추가 레지스터가 필요해서 100만 게이트 급의 FPGA에 구현할 수 없었다. 따라서 앞에서 분석한 각 알고리즘의 레지스터 사용 내용을 토대로 가장 효율적인 레지스터 공유를 시도하였다. 그림 2는 레지스터를 공유하는 구조의 설계의 기본적인 개념도를 나타내고 있다.

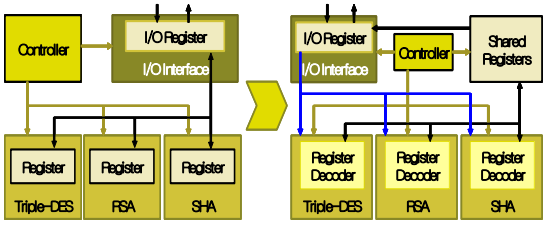

그림 2 레지스터 공유 구조 설계 개념도

2.2.3 레지스터 공유 TLS 기반 보안 프로세서 FPGA 구현 및 검증

설계한 TLS 기반 보안 프로세서를 검증하기 위하여 Xilinx에서 제공하는 ISE 6.0에서 FPGA 검증을 하였다. 타겟 FPGA는 Xilinx Vertex-E xcv1000e-HQ240-6으로 하였다. 플로어 플래닝을 한 결과를 그림 3에서 보여주고 있다.

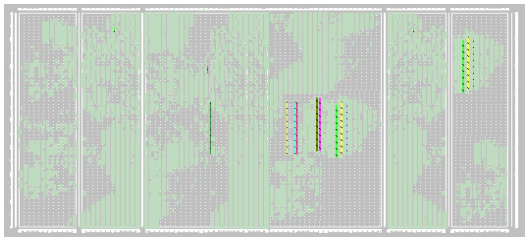

그림 3 FPGA 플로어플래닝 결과

플로어플래닝을 한 후 그림을 보면 FPGA 면적의 상당수를 차지함을 알수 있다. 그 결과 actual ratio는 89%였다.

그리고 그림 4는 배선을 하고난 Routing 결과를 보여주는 그림이다.

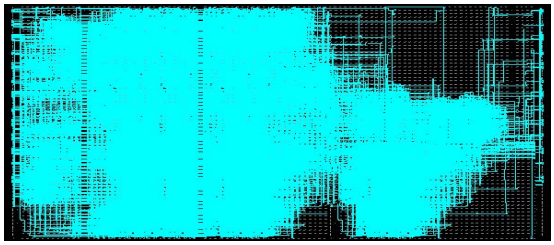

그림 4 FPGA 라우팅 결과

나. 임베디드 시스템 검증

그림 5는 FPGA Add-On Board와 IFC-ETK100 Kit 사이의 동작을 나타내는 그림이다.

그림 5 IFC-ETK100

32 bits Data Bus와 8 bits Address Bus는 IFC-ETK100의 Jupiter 칩과 FPGA Add-On Board의 Xilinx FPGA와 직접 연결되어 동작한다.

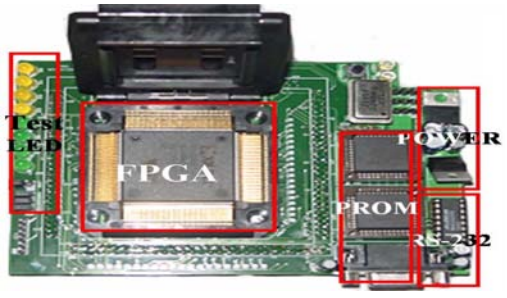

그림 6 FPGA Board

FPGA Add-On Board의 개발된 제품의 형태는 다음의 그림에서 보이고 있는 사진과 같다.

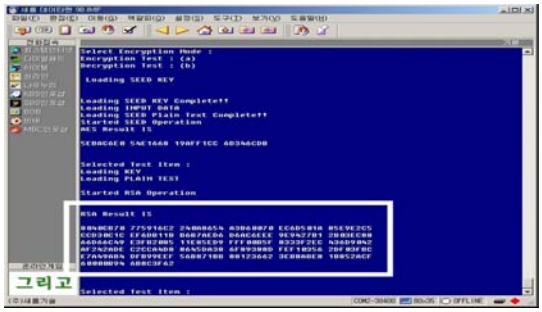

그림 7 RSA 암호 알고리즘의 동작 검증

그림 7는 암호 알고리즘을 보안 IP로 설계한 후 FPGA에 다운시킨 후 회로가 정상 동작하는지를 살펴보는 검증 화면을 보이고 있다. 앞서 설계했던 SHA-1을 비롯하여, DICOM Security Profiles에서 정의된 TLS 기반 암호 알고리즘인 RSA 공개키 알고리즘 IP를 FPGA에 다운 해 보았다.

결과 IFC-ETK100과 FPGA에 들어간 보안 IP들이 잘 동작됨을 하이퍼 터미널을 통하여 확인 할 수 있었다.

다. 개별 메카니즘 설계 Report 비교

통합 TLS 보안 프로세서 설계에 앞서 TLS 보안 전송연결 표준에 명시된 세 가지 알고리즘을 개별적으로 Xilinx FPGA인 Vertex-E 시리즈의 xcv1000e-HQ240-6을 가지고 구현과 검증을 했다. 다음의 표 5은 각 알고리즘 별로 설계 후 report 파일을 분석하여 작성한 비교 테이블이다.

표 5 각 알고리즘별 구현 결과 비교

	구분	Triple DES	RSA	SHA
FPGA Xilinx Vertex-E xcv1000e-HQ240-6	Area(cell)	18,087	31,021	13,252
	Speed(MHz)	29.1	19.6	49.9
	Power(mW)	910	911	907

각 알고리즘들의 구현 결과 RSA가 가장 큰 면적을 가짐을 알 수 있었다. 1024 bits를 기본으로 하는 RSA가 레지스터 사용량이 가장 크다는 것에 기인한다.

라. 레지스터 공유 전후 구조의 설계 Report 비교

TLS 보안전송연결 프로파일에 명시된 세 알고리즘을 먼저 레지스터 공유 없이 단순 3단 MUX 구조를 이용하여 설계한 것과 면적을 줄이기 위하여 레지스터 공유를 통해 설계한 것을 비교 분석해 보았다. 표 6는 두 설계회로를 마찬가지로 FPGA 구현으로 모두

비교한 테이블이다.

표 6 레지스터 공유 전후 구현 결과 비교

	구분	레지스터 공유 전 (3단 MUX)	레지스터 공유
FPGA Xilinx Vertex-E xcv1000e-HQ240-6	Area(cell)	91,822	78,544
	Speed(MHz)	19.2	18.9
	Power(mW)	927	919

3. 결론

본 논문에서는 의료정보보호를 위해 의료영상전송 표준의 하나인 DICOM을 분석하였고, 그에 따라 표준문서의 Security Profile 에 명시된 두 프로파일 중 하나인 TLS 보안전송연결 프로파일의 기준을 따르는 TLS 보안 프로세서를 설계하였다.

그리고 세 알고리즘이 모두 들어간 단순 3단 MUX 구조의 TLS 기반 보안 프로세서를 FPGA 구현 및 검증을 위해 3단 MUX 구조에서 레지스터 공유 구조로 변경하였다. FPGA 구현시, 연구실에서 소장하고 있는 100만 Gates급 Xilinx FPGA Vertex-E xcv1000e-HQ240-6의 레지스터 셀 개수의 한계를 극복하기 위하여 레지스터 공유를 추진하였고, 결국 레지스터 수를 2/5 수준으로 줄여 FPGA에서 구현과 검증에 성공하였다. 세 알고리즘의 각 코어부분은 속도 보다는 면적 축소에 신경을 써서, 다소 속도는 느리지만 100만 Gates급의 FPGA에서도 구현이 가능할 만큼 면적 감소에 성공하였다.

참고문헌

[1] NEMA, DICOM Part 15: Security Profiles, NEMA, Virginia USA, 2000.

[2] William Stallings, Cryptography and Network Security: Principles and Practice, Prentice-Hall, Inc., New Jersey USA, 1999.

[3] NIST, FIPS PUB 180-1, Secure Hash Algorithm, NIST, 1993.

[4] TTA, TTAS.KO12-0011, Hash Function Standard Part2 : Hash Function Algorithm Standard, TTA, 2000.

[5] User Conformance profile : DICOM version 3.0 compliance. Fred prior.ph.d. Dview. Medical images viewer. By: Ben-Sasson Daniel. Feldman Shahar. Yoad Gidron.

[6] Filmless Radiology. Eliot. Siegel Robert M.Kolodner.