콘텐츠 보호용 암호가속카드의 설계 및 구현

Hardware Implementation of A Cryptographic System for Contents Protection

이완복, 노창현, 김주한*
중부대학교, (주)시큐어넥서스*

Lee Wan-Bok, Roh Chang-Hyun, Kim Joo-Han*
Joongbu Univ., XecureNexus Inc.*

요약

고비도의 콘텐츠 정보보호를 실현하기 위해서는 고성능의 암호 가속 성능이 필요하다. 특히, 현재 많이 사용되어 지는 각종 암호 알고리즘들은 많은 계산량을 필요로 하고 소프트웨어로 구현되었을 경우에는 그 성능에 한계가 있기 때문에, 전용의 암호 가속 칩을 이용하여 하드웨어로 구현하는 것이 필요하다. 본 논문에서는 많이 사용되어지는 블록 암호 알고리즘인 3DES, AES, SEED가 실장된 암호 가속 칩을 이용하여 PCI 카드를 설계 제작한 사례를 보이고 있다.

Abstract

Implementing a hardware cryptographic system is strongly required to assure high quality contents security. Not only because the many of the prevalent cryptographic algorithms require much computation time but also software implementations of cryptographic systems do not guarantee high performance, we need to design a hardware cryptographic system with a dedicated crypto-chip. This paper describes a case study of implementing a PCI cryptographic card, which supports cryptographic algorithms such as 3DES, AES, SEED.

1. 서 론

최근 들어 전 세계적으로 급격히 보급된 인터넷은 정치, 경제, 사회, 문화 등 인류 생활 전반에 걸쳐 엄청난 파급효과를 미치고 있다. 특히, 시공간을 초월할 수 있는 인터넷 고유의 특성을 이용하여 온라인 쇼핑, e-learning, 인터넷 뱅킹, VoD 서비스 등의 신규 사업들이 이미 활성화된 상태이다. 반면에 정보통신 기술을 악의적으로 이용하여 인터넷상에 복잡하게 산재한 다양한 정보와 그 통신 내용을 악용하는 부작용도 발생하고 있다. 예를 들어, 얼마 전에 인터넷뱅킹을 해킹하여 타인의 계좌로부터 현금을 불법적으로 인출했었던 사건이나, DNS 서버들이 웜에 마비되어 국내 인터넷 망이 다운되었었던 2003년도 1월의 인터넷 대란과 같은 사건들은 보안 문제가 얼마나 중요한지 다시금 시사해주고 있다.

또한, 정보통신 기술이 안정기로 접어들면서 인터넷상의 콘텐츠를 직간접적으로 거래하는 사업들도 비약적으로 늘어나고 있다. 한국 소프트웨어진흥원이 발표한 자료에 의하면 온라인 게임, e-learning, 애니메이션, 모바일 콘텐츠 등을 포함한 디지털콘텐츠 산업의 시장규모는 매년 30%~50%씩 고성장하고 있다[1]. 향후 광대역통합망(BcN)이 보급되기 시작하면, 통합된 네트워크를 통해 콘텐츠 유통과 이용환경이 COPE(Created Once, Published Everywhere) 형태로 변화하면서 콘텐츠의 중요성이 더해질 전망이다. 그러한 환경에서는 Contents Provider(CP)가 하나의 유선 콘텐츠를 무선통신용, 디지털방송용 콘텐츠 등으로 변환하여 다양한 유통채널을 통해 판매

할 수 있을 것으로 예상되는데, 안전한 사업 모델을 위해서는 워터마킹과 암호화, 인증 및 추적 기술 등을 이용하여 콘텐츠를 안전하고도 효율적으로 유통시키고, 콘텐츠 저작권을 보호해야 할 것이다. 이러한 배경에서 태생한 것이 DRM 기술인데, 그 바탕은 암호기술이 핵심을 이루고 있다[2]. 그러므로, 빠르고도 안전한 콘텐츠 유통과 보급을 보장하기 위해서는 저렴한 비용으로 빠른 암호연산을 할 수 있는 암호가속기가 마련되어야 한다. 이러한 암호가속기는 비단 DRM에만 국한되어 콘텐츠 유통 판매 시장에만 적용될 수 있는 것이 아니라, VPN을 비롯한 인터넷 보안 등의 분야에도 활용될 수 있다.

그러나, 암호연산은 많은 계산량을 요구하고, 치환 및 비트쉬프트 연산들이 많기 때문에, 소프트웨어적으로 높은 성능을 내기 어려운 특성이 있으며, 하드웨어로 구현할 시 더욱 높은 속도를 보장할 수 있다. 이러한 배경에서 Hifn[3], Broadcom, Analog Device사 등 다수의 해외 업체들이 암호가속 칩을 개발한 바 있다. 그러나, 이들 칩은 국내 표준 블록 암호 알고리즘을 제공하지 않으며, 암호엔진을 공개하지도 않기 때문에, 국내 시장에 적용하거나 임베디드 프로세서 내에 암호엔진을 추가하는 것이 어렵다. 본 연구에서는 이러한 배경에서 국내 (주)시큐어넥서스에서 개발한 암호가속칩 XCP-01을 이용하여 암호가속 보드를 제작하고 그 성능을 테스트한 결과를 소개한다.

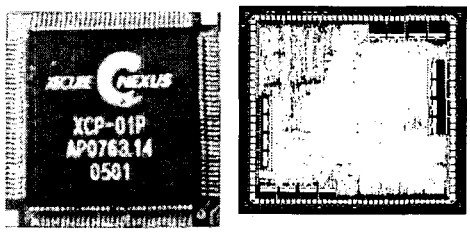
논문의 구성은 다음과 같다. 2장에서는 본 논문에서 사용한 암호가속 칩 XCP-01과 이를 이용해 개발한 암호가속 보드에 대해 설명한다. 3장에서는 제작한 암호가속 보드의 성능을 평가하였으며, 4장에서 결론을 맺는다.

II. 암호가속 보드의 설계

1. 암호가속 엔진

본 논문에서 사용한 암호가속 엔진은 (주)시큐어넥서스에서 개발한 암호칩 XCP-01이며 칩 외양은 [그림 1]과 같다. 이 칩은 DES, 3DES, AES, SEED 네 종류의 블록 암호알고리즘을 지원하며, 먼저 Xilinx FPGA를 이용해 개발되었으며, 추후 0.18um 공정으로 다시 개발되었는데, [그림 1]에서 개발된 칩의 외형을 보이고 있다[4].

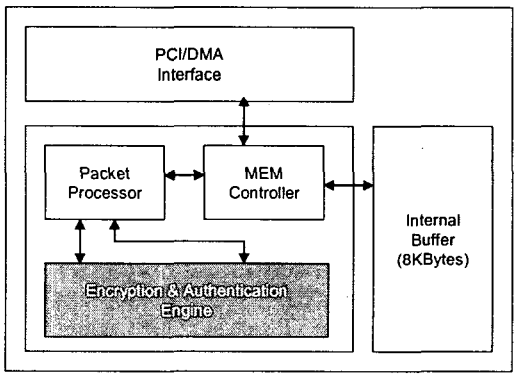
개발한 칩은 암호 연산이 고속으로 이루어질 수 있도록 메인프로세서와의 인터페이스로 32bit/33MHz의 PCI 인터페이스를 지원하고 있다.



(a) 외형 (b) 레이아웃 사진

▶▶ 그림 1. XCP-01: 암호가속 엔진이 탑재된 칩.

상기 암호가속 칩은 내부적으로 PCI/DMA Interface 블록, Packet Process 블록, MEM Contorller 블록, Encryption & Authentication Engine 블록 과 Internal Buffer 블록의 총 5개의 블록으로 구성되어진다. [그림 2]는 암호 가속 엔진의 구조를 나타낸다.



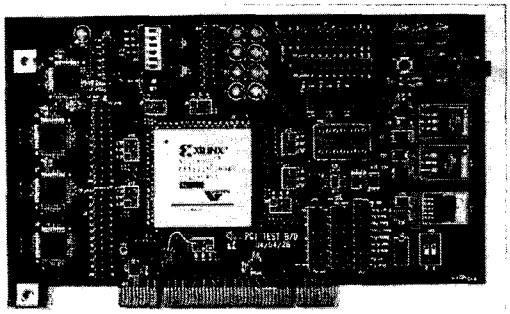
▶▶ 그림 2. 암호가속 엔진의 구조도

PCI/DMA Interface 블록은 PCI와 DMA를 통하

여 입출력되는 데이터의 인터페이스를 담당하며, MEM Contorller 블록은 PCI/DMA Interface블록으로부터 들어온 데이터를 Packet Process 블록과 Internal Buffer블록 사이에 데이터를 전달하거나 저장하는 역할을 하며, Packet Process 블록은 Encryption & Authentication Engine 블록의 입력 데이터 형식에 맞추어 데이터를 전달하거나 Encryption & Authentication Engine 블록에서 출력된 데이터를 조합하는 역할을 한다. Internal Buffer 블록은 내부에서 사용되는 임시 데이터 저장 장소이다.

2. 암호가속 보드의 설계

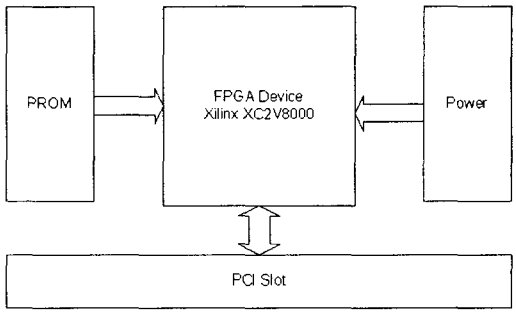
제작한 카드의 외형은 [그림 3]에 보여지고 있다. 제작한 암호가속 카드는 Xilinx FPGA를 이용한 것과 위 XCP-01칩을 이용한 것 두 가지가 있는데, 본 연구에서는 FPGA를 이용하여 제작한 카드를 사용하고 있다.



▶▶ 그림 3. 제작한 암호 가속카드의 외형

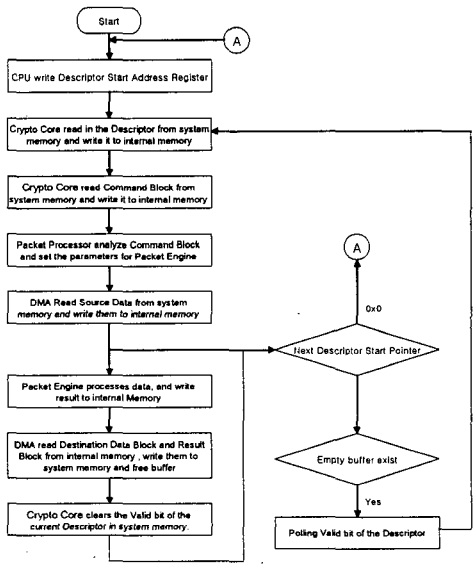
암호가속 카드는 크게 PROM, PCI I/F와 암호 및 인증 알고리듬이 One Chip으로 구성된 자일링스 디바이스, 전원을 공급하는 Power와 PCI Slot으로 구성되어 있다. 그림 4는 암호가속 카드의 블록도를 나타낸다.

[그림 5]는 암호가속 보드의 동작 흐름에 대하여 나타낸다. 그림에서 알 수 있듯이 CPU에서 디스크립터



▶▶ 그림 4. 암호가속 카드의 블록 구성도

의 시작을 알리는 레지스터 값을 세팅함으로써 암호가속 보드의 동작이 시작된다. 암호 코어는 시스템 메모리와 DMA를 통해 디스크립터, 커맨드, 데이터를 차례로 읽어와 내부 메모리에 저장하고 Packet Processor에 전달한다. Packet Processor은 암호 코어 블록에 데이터를 전달하고 처리된 결과를 내부 메모리에 저장한다. 암호 코어는 처리가 완료되면 다음 디스크립터를 받을 수 있도록 시스템 메모리의 현재 디스크립터의 시작 비트를 클리어 한다. 결론적으로, 암호가속 카드는 호스트 CPU의 도움을 최소로 받으면서 암호 패킷을 처리할 수 있도록 DMA를 최대한 활용하고 있다.

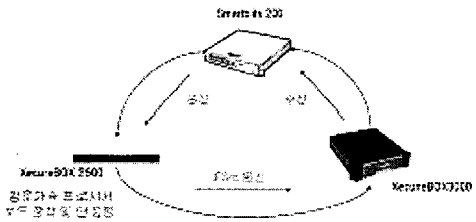


▶▶ 그림 5. 암호 가속 보드의 동작 흐름도

III. 성능 평가

1. 측정 환경의 구축

설계된 암호 시스템의 성능을 평가하기 위해 FAB 공정에 사용되기 직전에 동작성 검증이 끝난, Xilinx FPGA를 이용하여 [그림 3]과 같은 보드를 구성하고, [그림 6]과 같은 환경에서 VPN Tunnel을 구축하였을 시의 성능을 측정하였다.



▶▶ 그림 6. 성능 측정 환경.

1.1 측정 대상 장비

암호화 전용 프로세서 FPGA 보드를 장착한 (주)시큐어넥서스의 IPSec 전용 장비로 세부 내역은 다음과 같다.

- XecureBOX 2500 Gateway
- x86 기반, Intel Pentium III 1.0GHz CPU, 128Mb Memory, Three Ethernet I/F, Two PCI Slot
- 암호화 전용 프로세서 FPGA를 통해 IPSec 프로세싱을 수행하도록 수정 개발됨

1.2 상대 통신 장비

측정 대상이 되는 장비와 통신하는 상대 통신 장비는 측정 대상의 성능에 영향을 미치지 않을 만큼 상위의 성능을 가져야 하며, 세부 내역은 다음과 같다.

- XecureBOX 3000 Gateway
- x86 기반, Intel Pentium IV 2.8GHz CPU, 256Mb Memory

1.3. 측정 장비

NetCom Systems 사의 Smartbits 200을 측정 장비로 채택하였다.

2. 실험 결과

이상의 환경에서 각 알고리즘 별로 성능을 측정한 결과는 표 1과 같다.

[표 1] 알고리즘별 성능 측정

알고리즘	패킷 크기	성능
DES	64 bytes	19.6 Mbps
	1400 bytes	81.7 Mbps
DES/MD5	64 bytes	16.1 Mbps
	1400 bytes	73.7 Mbps
DES/SHA-1	64 bytes	14.3 Mbps
	1400 bytes	66.5 Mbps
3DES	64 bytes	8.1 Mbps
	1400 bytes	49.3 Mbps
3DES/MD5	64 bytes	6.2 Mbps
	1400 bytes	44.9 Mbps
3DES/SHA-1	64 bytes	5.7 Mbps
	1400 bytes	40.7 Mbps
AES	64 bytes	22.8 Mbps
	1400 bytes	83.5 Mbps
AES/MD5	64 bytes	17.4 Mbps
	1400 bytes	75.1 Mbps
AES/SHA-1	64 bytes	15.7 Mbps
	1400 bytes	67.2 Mbps
SEED	64 bytes	7.6 Mbps
	1400 bytes	39.4 Mbps
SEED/MD5	64 bytes	5.9 Mbps
	1400 bytes	37.1 Mbps
SEED/SHA-1	64 bytes	5.7 Mbps
	1400 bytes	36.3 Mbps

IV. 결 론

본 논문에서는 DRM, VPN 등의 보안 시스템에서 사용되고 있는 데이터 암복호화 과정을 고속으로 처리할 수 있는 암호가속 보드를 설계하고 평가한 결과

를 소개하였다. 개발한 보드의 큰 특징은 주요 블록 암호 알고리즘인 DES/3DES만이 아니라, 국내 전용 알고리즘인 SEED를 탑재하고 있어서 국내 공공기관이나 금융기관의 장비 개발에 적용이 손쉬울 뿐 아니라 차세대 블록알고리즘인 AES를 탑재하여 해외 경쟁력도 확보하고 있다.

향후, 콘텐츠 패키징, 콘텐츠 복호화 등에 활용되어 저수준의 프로세서를 탑재한 장비에서도 본 암호가속 보드의 도움을 받아 고속의 암복호화 연산이 가능할 것으로 기대된다.

▌참 고 문 헌▐

[1] ---, 2003년도 국내 디지털콘텐츠산업 시장조사 보고서, 한국소프트웨어진흥원.

[2] Ahmet M. Eskicioglu, "Protecting Intellectual Property in Digital Multimedia Networks", IEEE Computer, pp.39-45, July 2003,

[3] HIFN Inc. Available at http://www.hifn.com.

[4] 이완복, 노창현, "VPN에 특화된 암호가속 칩의 설계 및 제작", 한국해양정보통신학회 2005년 추계종합학술대회, 2005년 10월(to appear).