# VPN에 특화된 암호가속 칩의 설계 및 제작

이완복, 노창현

중부대학교

# Design of a Cryptographic Processor Dedicated to VPN

Wan-Bok Lee, Chang-Hyun Roh

Joongbu University

E-mail : wblee@joongbu.ac.kr

## 요 약

본 논문에서는 SSL과 VPN에 적합하도록 개발된 암호 프로세서의 설계에 대해서 소개한다. 제작한 칩은 국내 표준 블록 알고리즘인 SEED를 포함하여 3DES, AES 등의 블록 암호 알고리즘을 지원하며, 163비트 타원곡선 공개키 알고리즘을 지원하고 있다. 또한 암호 연산이 고속으로 이루어질 수 있도록 PCI Master 방식의 인터페이스를 탑재하고 있다.

## ABSTRACT

This paper introduces a case study of designing a cryptographic processor dedicated to VPN /SSL system. The designed processor supports not only block cipher algorithms, including 3DES, AES, and SEED, but also 163 bit ECC public key crypto algorithm. Moreover, we adopted PCI Master interface in the design, which guarantees fast computation of cryptographic algorithms prevalent in general information security systems.

## 키워드

암호가속칩, VPN, 암호프로세서

## Ⅰ. 서 론

VPN이란 양 단간의 비밀성을 보장하기 위해 물리적으로 분리된 회선을 사용하는 기존의 전용선과 달리, 인터넷과 같은 공중망을 기반으로 하여 암호화 통신 기술을 통해 양단간의 안전한 정보 교환이 가능하도록 하는 차세대 네트워크 인프라 기술이다[1][2].

ADSL, VDSL 등의 광대역 네트워크 서비스의 확대와 무선랜, CDMA 등 무선 네트워크 인프라의 확보는 VPN 시장의 성장에 필수적인 요소이다. VPN은 기존의 전용선을 대체하여 공중망을 통한 저렴한, 하지만 전용선에 준하는 품질을 확보할 수 있는, 네트워크 기반을 확보할 수 있도록 해 줌으로써 기업이 네트워크 인프라 확보를 위한 경비를 크게 절감할 수 있도록 하였다. 비단 경비 절감의 차원뿐만 아니라 인터넷을 이용할 수 있는 곳이면 어디에서든 VPN을 통한 접속이 가능하므로 기업 네트워크에 유동성을 확보할 수 있게 되었다. 이러한 장점으로 인해 VPN에 대한 수요는 급증하고 있으며 최근에 와서는 KT, 데이콤, 하나로 통신 등의 ISP 업체들이 VPN을 차세대 네트워크 인프라로 인식하고 그 서비스 사업을 준비하고 있다.

그러나, VPN 시스템은 기본적으로 통신하는 모든 데이터 패킷들을 암호화하는 메카니즘에 의해 보안성을 구축하기 때문에, 저렴한 가격에 고성능의 장비를 개발하려면 암호가속화에 특화된 칩을 제작하는 것이 필수적으로 요구되는데 그 배경은 다음과 같다.

**- 고성능 암호가속 성능:**

암호화 연산의 기본구성은 단순한 연산 모듈로 되어 있으나, 암호화 강도를 높이기 위해 많은 반복 연산을 동원하고 있어, 범용 프로세서로는 연산의 속도를 높이는데 한계가 있다. 이러한 연산

적인 특성은 범용 프로세서에서 소프트웨어적으로 처리하는 것 보다 전용 칩(ASIC)으로 개발하였을 때 그 효율성이 극대화 된다.

**- 임베디드 프로세서의 제한된 성능:**
저렴에 가격에 널리 보급되어야 하는 각종 임베디드 시스템이나 핸드헬드 디바이스에 탑재되는 프로세서는 보편적으로 저전력, 작은 탑재 메모리 등의 제약으로 계산 성능이 별로 뛰어나지 않은 경우가 많다. 이러한 프로세서로서는 많은 계산량이 소요되는 암호화 연산을 충분히 빠르게 계산할 수가 없다.

**- 저가형 네트워크 보안 장비의 개발:**
저가형 네트워크 보안 장비의 개발을 위해서는 전용 ASIC의 개발이 필수적이다. 아래 <표 1>은 보안장비를 위한 전용 프로세서를 사용하는 경우와 x86 프로세서를 사용하여 저가형 VPN 장비를 제작하였을 때의 성능과 제품 원재료비를 비교한 것이다.

<표 1> 전용 프로세서 사용 시의 원가 절감

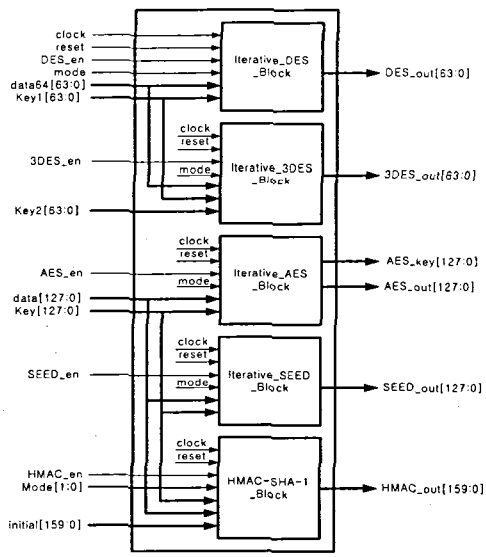
| | VPN 성능 | 제품 원재료비 |
|---|---|---|
| x86 프로세서 사용 | 5Mbps 이내 | 45만원 |
| VPN 전용 프로세서 사용 | 20Mbps | 15만원 이내 |

## II. 고속 IPSec 암호처리 시스템 설계

본 논문에서는 IP패킷의 기밀성(Confidentiality), 무결성(Integrity), 인증(Authentication)을 제공하는 SSL/VPN을 위한 고속 암호 처리 칩 구현에 관하여 기술한다. 우선 암호 및 인증엔진을 개발하여 이를 FPGA를 이용하여 검증했으며, 검증 완료 후 현재는 삼성 FAB 공정을 통하여 개발하였다. 개발된 인증 엔진 기밀성 서비스를 위한 암호엔진은 DES, 3DES, SEED, 그리고 AES 알고리듬[3] 등을 사용하여 설계하였고, 인증 및 무결성 보안 서비스를 위한 인증엔진은 HMAC(The Keyde-Hash Message Authentication Code)-SHA-1을 기본으로 설계하였다. 또한 공개키 알고리즘인 ECC도 지원하도록 하였다. 설계 툴로서는 Verilog을 사용하여 구조적 모델링을 행하였으며, Xilinx사의 ISE 5.2i 툴을 이용하여 논리 합성을 수행하였다. FPGA 구현을 위해서 Xilinx사의 ISE 5.2i 툴과 Modelsim을 이용하여 타이밍 시뮬레이션을 수행하였다. 또한 암호 연산이 고속으로 이루어질 수 있도록 메인프로세서와의 인터페이스를 위해 32bit/33MHz의 PCI 인터페이스를 내장하고 있다.

### 2.1. 블록 암호 시스템의 설계

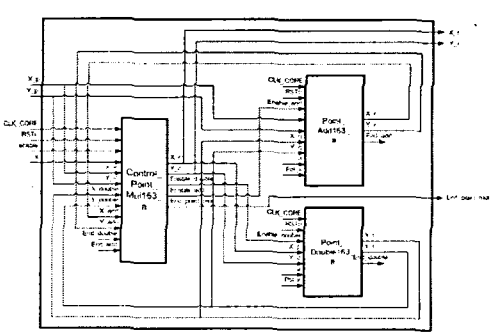
대표적인 블록 암호 알고리즘인, DES, 3DES, SEED, AES 그리고 HMAC을 하나의 블록으로 구성하여 설계하였으며, 각 알고리듬 모듈들은 각각의 Enable 신호에 의하여 작동하도록 설계하였다. 다음 그림 1은 구성한 전체 암호 프로세서의 구조를 나타낸다.




<그림 1> 블록 암호 가속 모듈의 구조

### 2.2. 타원 곡선 암호 프로세서의 설계

ECC 프로세서는 제안된 Serial-Cell_array 곱셈기와 유한체 역원기를 구성하여 그림 2와 같이 설계하였다. 이 그림에서 점 덧셈연산을 수행하는 Point_Add163_a 블록과 두배점 연산을 수행하는 Point_Double163_a 블록, 그리고 Control 블록으로 구성된다. 유한체 역원과 나눗셈 연산은 역원 알고리즘에서 추가의 곱셈연산을 하지 않고도 나눗셈 연산이 가능한 Modified 확장 유클리드 알고리즘을 사용하였다.



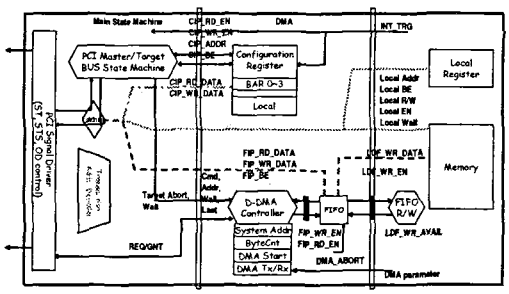
<그림 2> ECC 암호 프로세서 모듈의 구조

Control_Point_Mul163_a는 타원곡선 상의 점이 같은 점인지 다른 점인지 판별해서 점 덧셈 연산

또는 두배점 연산을 할 것인지를 결정하고, 연산이 다 수행되면 결과를 X_r, Y_r로 내보낸다[4]. Point_Double163_a는 기약다항식 Pol_x, 임의의 공개점 X_p, Y_p, 타원곡선 계수 a를 입력으로 타원곡선 상의 같은 두 점의 덧셈 연산을 수행한다. Point_Add163_a는 기약다항식 Pol_x, 임의의 공개점 X_p, Y_p, 타원곡선 계수 a를 입력으로 타원곡선 상의 다른 두 점의 덧셈 연산수행 한다. 하위구조에 대해서는 지면관계상 생략한다.

### 2. 3. PCI I/F의 설계

설계된 PCI I/F는 32-bit, 33MHz PCI Master/Target Interface, Configuration Register, single memory & I/O cycle, burst memory transfer by using internal FIFO, Conf read/write, Mem read/write, I/O read/write, single DMA channel, BUS parking과 Address Stepping을 지원하며, Master 기능으로는 DMA read/write, FIFO Read/Write와 Multiple Data Xfer가 있으며, Target 기능으로는 Conf. Reg Read/Write, Memory Read/Write, Local Reg Read/Write와 Single Data Xfer 기능이 있다. 그림 3은 PCI I/F의 전체 구조를 나타낸다.




<그림 3> PCI Interface 구조

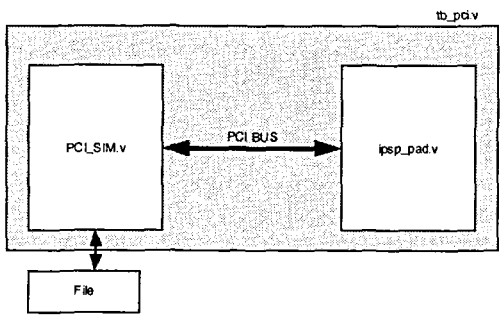
## III. 구현 및 성능 평가

본 연구에서 개발한 전용 암호 패킷 처리 ASIC의 암호 및 인증시스템 및 PCI I/F의 각 모듈은 ASIC 개발에 앞서 Xilinx ISE 5.2i 툴을 이용하여 Verilog 설계 및 합성을 수행하였다. 또한, 설계 검증을 위한 타이밍 시뮬레이션을 Modelsim을 이용하였고, Xilinx FPGA XC2V8000을 타겟으로 FPGA를 구현하였다.

### 3. 1. 시뮬레이션을 통한 성능 평가

#### 3.1.1. 기능 시험 결과

그림 4는 기능 시험을 위한 블록도를 나타낸다. 개발된 암호 연산 코어외에 system clock, reset를 generation 하는 모듈을 추가한 다음, pci test model과 암호연산 모듈을 연결하는 top module을 붙여서 시뮬레이션하였다. 초기화가 끝이 나면 LOC_ST event를 발생하는데 이때부터 packet 암호화를 시작한다. Input Data는 tot_in.dat 파일에서 읽어오면 descriptor 또한 내부에서 만들어주는 것이 아닌 미리 만든 파일(tot_in.dscr)에서 읽어 작동한다. 총 167 packet을 처리하여 기능 시험을 완료하였다.




<그림 4> 기능 시험 블록도

#### 3.1.2. 성능 시험 결과

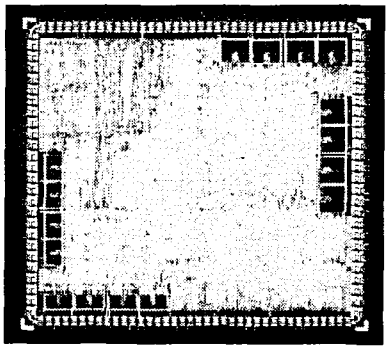
다음은 암복호 및 인증 엔진에 대한 성능평가 결과를 나타낸다. Xilinx사의 CAD 툴 이용하여 합성 및 시뮬레이션을 수행하였고, target library는 VertexII를 이용하였다.

<표 2> 시뮬레이션 실험 결과

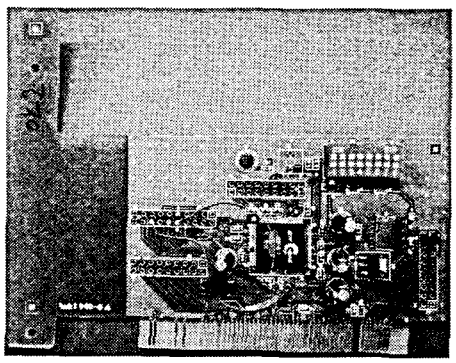
| | No. of gates (Silces) | Throughput (Frequency) | Used slices |
|---|---|---|---|
| DES | 28107 (1041) | 320Mbps (80Mhz) | 2% |
| 3DES | 63720 (2360) | 106Mbps (80Mhz) | 5% |
| AES | 128304 (4752) | 546Mbps (47Mhz) | 9% |
| SEED | 166725 (6175) | 218Mbps (30Mhz) | 13% |
| HMAC -SHA-1 | 140130 (5190) | 233Mbps (37Mhz) | 11% |
| 합계 | 526986 (19518) | | |

### 3.2. ASIC 공정 및 패키징

설계된 로직은 TSMC 0.18um 공정을 이용하여 제작되었으며, LQFP128로 패키징하였다. 전체 칩의 크기는 14x14x1.4mm이며, 그 레이아웃 사진이 그림 5에 나타나 있다. 이 칩을 장착하여 아래 그림6과 같이 PCI 보드를 쉽게 제작할 수 있었다.



<그림 5> 레이아웃 사진



<그림 6> 제작한 PCI 카드

## IV. 결 론

본 논문에서는 SSL과 VPN에 적합하도록 개발된 암호 프로세서의 설계에 대해서 소개하였다. 개발된 프로세서는 암호 패킷처리를 위한 기능들로 구성되어 있다. 가장 큰 특징은 국내 전용 알고리즘인 SEED를 탑재하고 있어서 국내 공공기관이나 금융기관의 장비 개발에 적용이 손쉬울 뿐 아니라 차세대 블록알고리즘인 AES를 탑재하여 해외 경쟁력도 확보하고 있다.

개발된 프로세서는 네트워크 보안 장비의 구성에 있어서 주 프로세서 외에 별도의 암호화 코프로세서로 탑재되어 제품의 성능을 높이는데 사용된다. 따라서 x86 프로세서와 같은 범용 프로세서나 본 과제의 결과물 중 하나인 네트워크 프로세서의 코프로세서로 이용되어 저가격에 고수준의 암호장비를 제작하는 경우에 활용될 수 있다.

## 참고문헌

[1] Ray Stanton, Global Head, "Securing VPNs: comparing SSL and IPsec", *Computer Fraud & Security*, Vol. 2005, No. 9, pp. 17-19, Sep. 2005.

[2] S. Kent, R, Atkinson "Security Architecture for the Internet Protocol". Internet RFC November 1998.

[3] NBS, Data Encryption Standard, FIPS Pub. 46, U.S, National Bureau of Standards, Washington DC. Jan. 1977.

[4] James Goodman and Anantha P. Chandrakasan, "An energy-efficient reconfigurable public-key cryptography processor", *IEEE Journal of Solid-State Circuits*, 36(11), Nov. 2001.