# AMBA(Advanced Microcontroller Bus Architecture) 기반의 IPSec 암호 프로세서의 구현

## Implementation of IPSec Cryptographic Processor Based AMBA Architecture

황재진*, 최명렬*
JaeJin Hwang*, Myung-Ryul Choi*

**Abstract** - The importance for Internet security has being increased and the Internet Protocol Security (IPSec) standard, which incorporates cryptographic algorithms, has been developed as one solution to this problem. IPSec provides security services in IP-Layer using IP Authentication Header (AH) and IP Encapsulation Security Payload (ESP). In this paper, we propose IPSec cryptographic processor design based AMBA architecture. Our design which is comprised Rijndael cryptographic algorithm and HAMC-SHA-1 authentication algorithm supports the cryptographic requirements of IP AH, IP ESP, and any combination of these two protocols. Also, our IPSec cryptographic processor operates as AMBA AHB Slave. We designed IPSec cryptographic processor using Xilinx ISE 5.2i and VHDL, and implemented our design using Xilinx's FPGA Vertex XCV600E.

**Key Words** : IPSec, 암호 프로세서, Rijndael, HMAC-SHA-1, AMBA Bus

### 1. 서 론

인터넷(Internet) 사용의 빠른 증가와 함께, 인터넷 보안에 대한 중요성 역시 증가하고 있다. IPSec(Internet Protocol Security)은 인터넷 보안 문제에 대한 하나의 해결방안으로 개발되었다.

IPSec은 TCP/IP 스택의 SSL(Secure Socket Layer)이나 TLS(Transport Layer Security)와 같은 애플리케이션 계층보다 더 낮은 수준에서 암호화(Encryption)와 인증(Authentication)을 수행한다. IPSec은 전송되는 데이터를 보호하기 위하여 IP AH(Authentication Header)와 IP ESP (Encapsulating Security Payload)의 두 가지 프로토콜을 제공한다. AH는 전송되는 데이터에 대해 인증과 무결성(Integrity) 서비스를 제공하고, ESP는 암호화 서비스를 제공한다. AH와 ESP는 서로 다른 프로토콜이며, 이 두 프로토콜은 각각 개별적으로 사용될 수도 있고, 무결성과 데이터 보호를 위해 결합되어 사용될 수도 있다.

기존의 범용 프로세서를 기반으로 한 암호 알고리즘의 소프트웨어 구현은 고속 네트워크 환경에 적용하기 어려울 뿐만 아니라, 안전성에서도 취약성을 드러내고 있다. 따라서, 고속의 암호화와 물리적인 안전성을 제공하기 위해서는 암호 알고리즘의 하드웨어 구현은 필수적이다.

본 논문에서는 IPSec에서 암호화와 인증을 수행할 수 있는 IPSec 암호 프로세서를 하드웨어로 구현하였다. 암호화를 수행하기위해서 새로운 AES(advanced Encryption Standard)로 선정된 Rijndael 암호 알고리즘을 설계하였고, 인증을 위하여 HMAC-SHA-1 인증 알고리즘을 설계하였다. 그리고, AMBA AHB 인터페이스를 함께 설계하였다. Xilinx ISE 5.2i를 사용하여 VHDL로 설계하였으며, ModelSim을 사용하여 시뮬레이션 검증을 하였고, Xilinx사의 Vertex XCV600E로 구현하였다.

저자 소개
* 학생회원 : 한양대학교 전자전기제어계측공학과 석사과정
* 정 회 원 : 한양대학교 전자컴퓨터공학부 정교수 · 공학박사

### 2. IPSec Protocol

IPSec은 IP 계층에서 보안 서비스를 제공한다. IPSec은 전송되는 데이터의 보호를 위해 IP AH와 IP ESP의 두 프로토콜을 제공한다. IP AH와 IP ESP는 기존의 IP 헤더에 추가되는 확장 헤더이다. IP AH는 데이터에 인증과 무결성 서비스를 제공하고, IP ESP는 암호화 서비스를 제공한다. IP AH와 IP ESP 두 프로토콜은 개별적으로 사용될 수도 있고, 무결성과 데이터 보호를 위해 결합되어 사용될 수도 있다.

#### 2.1 IP Authentication Header (AH)

IP 패킷(Packet)은 헤더(Header)와 Payload로 구분할 수 있는데, IP 헤더에 대한 보안 서비스를 적용하기 위하여 IP AH 헤더를 확장 헤더로 추가한다. 즉, IP AH는 IP 데이타그램(Datagram)의 비연결성 무결성(Connectionless integrity)과 데이터 발신 인증(Data origin authentication) 서비스를 제공한다. IP AH의 인증 알고리즘으로는 HMAC-MD5와 HMAC-SHA-1이 사용될 수 있는데, 본 논문에서는 보다 강력한 알고리즘으로 알려져 있는 HMAC-SHA-1을 구현하였다.

### 2.2 IP Encapsulating Security Payload (ESP)

IP ESP는 전송되는 데이터에 대해 암호화 서비스를 제공한다. IP ESP는 TCP/UDP 헤더와 IP 패킷에 포함된 애플리케이션 데이터를 암호화한다. 그 외에도 IP ESP는 전송되는 데이터의 무결성을 제공한다. IP AH가 전체 패킷을 보호하는 반면에, IP ESP는 IP 헤더에 대한 보호는 포함하지 않는다. 데이터를 암호화하고 패킷의 모든 필드를 보호하고자 한다면 IP AH와 IP ESP 두 프로토콜을 모두 구현하도록 SA(Security Association)를 구성해야 한다. 본 논문에서는 ESP의 암호화 알고리즘으로 Rijndael 암호 알고리즘을 구현하였다.

## 3. HMAC-SHA-1 인증(Authentication) 알고리즘

신뢰성이 보장되지 않은 매체를 통해 전송된 정보에 대한 무결성 검사는 컴퓨터 통신에서는 필수라 할 수 있다. 비밀키(Secret Key)를 이용하여 정보의 무결성을 제공하는 메카니즘을 MAC(Message Authentication Code)이라 한다. 그리고, 비밀키와 연계하여 암호 해쉬 함수(Cryptographic Hash Function)를 이용하는 MAC을 HAMC(Keyed-Hash Message Authentication Code)라 한다. 암호 해쉬 함수로는 MD5와 SHA-1을 사용할 수 있다. 128-bit의 해쉬 코드를 생성하는 MD5보다 160-bit의 해쉬 코드를 생성하는 SHA-1이 보다 강력한 암호 해쉬 함수로 알려져 있다. 본 논문에서는 무결성을 제공하기 위해서 HAMC-SHA-1을 구현하였다.

입력 받은 데이터 *text*로부터 MAC을 생성하기 위한 HMAC의 연산을 그림 1에 나타내었다. $H$는 연계하는 암호 해쉬 함수를 의미한다.

$$MAC(text)_t = HMAC(K, text) = H((K_0 \oplus opad) \mid H(K_0 \oplus ipad) \mid text))_t$$

그림 1. HMAC 연산

## 4. AES(Rijndael) 암호(Cryptographic) 알고리즘

NIST는 DES가 더 이상 안전성을 보장할 수 없게 되자 새로운 AES(Advanced Encryption Standard)로 Rijndael을 선정하였다. Rijndael 암호 알고리즘은 알려진 모든 공격에 대해 강할 뿐 만 아니라 그 응용에 있어서 속도나 하드웨어 구현에 뛰어난 장점을 가지고 있다.

Rijndael 암호 알고리즘은 SubBtye(Substitute Bytes Transformation), ShiftRows(Shift Row Transformation), MixColumn(Mix Column Transformation), AddRoundKey (Add Round Key Transformation)의 4개의 연산으로 이루어진다. SubByte는 S-Box를 이용하여 Byte 단위의 치환(Substitution)을 수행한다. ShiftRows는 열의 순서를 치환(Permutation)시킨다. MixColumn은 $GF(2^8)$ 연산을 이용한 치환(Substitution)이다. 마지막으로 AddRoundKey는 각각의 라운드키와 bitwise-XOR 연산을 수행한다.

## 5. AMBA AHB Bus Interface

SoC(System-on Chip) 레벨의 설계는 마이크로프로세서와 메모리, 특별한 Logic, input/output device등을 연결하는 Busing System을 필요로 한다. Bus는 물리적으로는 wire로 이루어져 있으며 논리적인 의미에서는 Master와 Slave 사이에 signal이나 데이터 전송에 대한 프로토콜을 의미한다. AMBA(Advanced Microcontroller Bus Architecture) Bus는 이러한 목적에 적합한 ARM사의 On-Chip Bus이다. AMBA Bus는 AHB, APB, ASB 3종류가 있다. 본 논문에서 구현한 IPSec 암호 프로세서는 Slave로 동작하며, AMBA AHB Slave 인터페이스가 함께 구현되었다. 그림 2에 AMBA AHB Slave 인터페이스를 나타내었다.

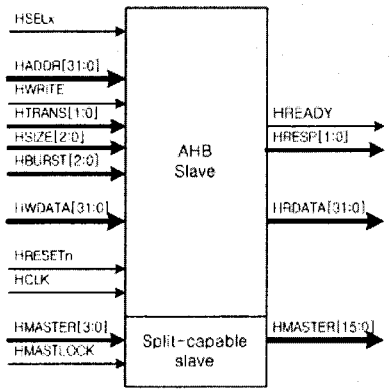


그림 2. AHB bus slave interface

## 6. AMBA 기반의 IPSec 암호 프로세서 구현

그림 3에 구현한 HMAC-SHA-1을 나타내었다. 입력 받은 데이터로부터 MAC을 생성하기 위해서는 두 번의 해쉬 연산을 필요로 하는데, 첫 번째 해쉬 출력은 두 번째 해쉬 연산의 입력이 되기 때문에, 그리고 면적(area)을 감소시키기 위해서 하나의 SHA-1을 공유하도록 설계하였다.

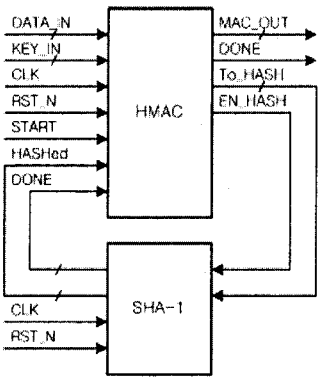


그림 3. HAMC-SHA-1

그림 4는 구현한 IPSec 암호 코어 프로세서이다. Rijndael

암호 프로세서와 HMAC-SHA-1으로 구성된다. IP AH와 IP ESP가 개별적으로 사용되는 경우와 무결성과 데이터 보호를 위해 결합되어 사용되는 경우를 모두 지원 가능하도록 설계하였다.

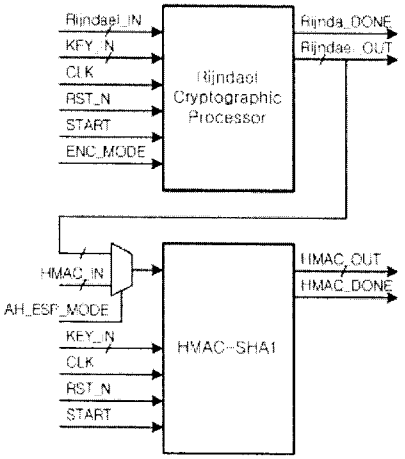


그림 4. IPSec Cryptographic Core Processor

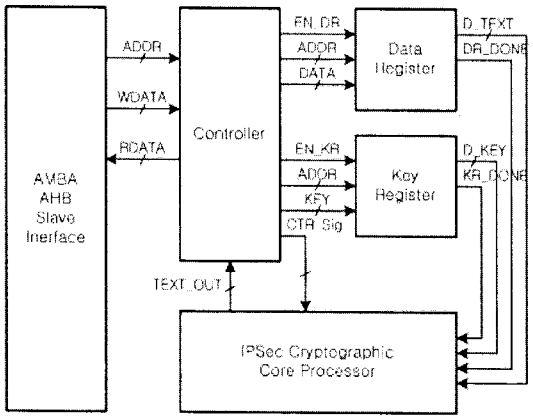


그림 5. AMBA 기반의 IPSec 암호 프로세서

그림 5에 구현한 전체 IPSec 암호 프로세서를 나타내었다. 구현한 IPSec 암호 프로세서는 Slave로 동작하며, AMBA AHB Slave 인터페이스를 갖는다. 컨트롤러 블록은 각각의 블록에 필요한 제어 신호와 데이터를 제공한다. 데이터 레지스터 블록과 키 레지스터 블록은 입력받은 데이터와 키를 IPSec 코어 프로세서로 전송한다. IPSec 코어 프로세서에서는 데이터의 암호화와 복호화 및 해쉬 연산이 이루어진다.

Rijndael 암호 프로세서는 약 27,482 게이트이며, 최대동작주파수는 86MHz이고, 처리량은 216Mbps이다. HMAC-SHA1은 약 13,311 게이트이고, 최대동작주파수는 78MHz, 그리고 104Mbps의 성능을 보였다.

## 7. 결론

본 논문에서는 IPSec에서 요구되는 암호화 및 인증을 수행할 수 있는 AMBA 기반의 IPSec 암호 프로세서를 구현하였다. 구현한 IPSec 암호 프로세서는 Rijndael 암호 알고리즘과 HAMC-SHA-1 인증 알고리즘으로 구성되며, IP AH와 IP ESP가 개별적으로 사용되는 경우와 무결성과 데이터 보호를 위해 결합되어 사용되는 경우를 모두 지원 가능하도록 설계되었다.

Rijndael 암호 알고리즘은 기존에 사용된 DES나 3-DES보다 더 강력한 암호 알고리즘으로 평가받고 있기 때문에 보다 안전하게 데이터 보호를 수행할 수 있다. HAMC-SHA-1 역시 MD5나 SHA-1과 같은 키를 사용하지 않는 해쉬 함수보다 더 강력한 알고리즘으로 평가받고 있다.

본 논문에서 구현한 IPSec 암호 프로세서는 ARM Core나 다른 RISC 프로세서를 사용하는 장비에 장착되어 사용될 수 있다.

향후, 구현한 IPSec 암호 프로세서의 성능을 개선해 나갈 것이며, 공격 방지(Attack Protection)에 대한 연구도 계속 진행할 것이다.

## 참 고 문 헌


[1] W. Stallings, "Cryptography and Network Security : Principle and Practice", 3th Edition, Prentice Hall, 2003.

[2] M.Y. Rhee, "Internet Security : : Cryptographic Principle, Algorithms, and Protocols", John Willey & Sons, 2003.

[3] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[4] S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[5] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[6] J. Daemen, V. Rijmen, "The Rijndael Block Cipher", AES Proposal, Ver 2, March 1999.

[7] US NIST, "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, November 26, 2001.

[8] M. McLoone, J. McCanny, "A Single-Chip IPSec Cryptographic Processor", Signal Processing Systems 2002 (SIPS'02) IEEE, October 2002.

[9] US NIST, "Secure Hash Standard", FIPS PUB 180-1, April 1995.

[10] US NIST, "The Keyed-Hash Message Authentication Code", FIPS PUB 198, March 2002.

[11] H. Krawczyk, M. Bellare, R. Canetti, "HMAC : Keyed-Hashing for Message Authentication", RFC 2104, Feb 1997.

[12] ARM Ltd., "AMBA Specification (Rev 2.0)", 1999.

[13] ARM Ltd., "AHB-Lite", 2001