IPSec을 위한 암호 프로세서의 구현

황재진° 최명렬
한양대학교 전자전기제어계측공학과
{heyjin25°, choimy}@asic.hanyang.ac.kr

The Implementation of the Cryptographic Processor for IPSec

JaeJin Hwang° Myung-Ryul Choi
Dept. of EECI, HanYang University

요 약

인터넷 보안에 대한 중요성이 나날이 증가하고 있으며, 이러한 인터넷 보안 문제의 해결책으로 개발된 IPSec은 IP 계층에서 보안서비스를 제공하기 위하여 AH와 ESP를 사용하여 보안연계(Security Association) 서비스를 제공한다. 본 논문에서는 32-bit 데이터 버스를 이용하여 새로운 AES로 채택된 Rijndael 암호 알고리즘과 HMAC-SHA-1 인증 알고리즘을 통합시킨 IPSec 암호 프로세서를 구현하였다. Xilinx ISE 5.2i를 사용하여 VHDL로 설계하였고, ModelSim으로 시뮬레이션 검증을 수행하였으며, Xilinx사의 Vertex XCV1000E로 구현하였다. 본 논문에서 구현한 IPSec 암호 프로세서는 WLAN이나 VPN, Firewall등에 응용될 수 있을 것이다.

1. 서 론

인터넷(Internet) 사용 인구의 급증과 더불어, 인터넷 보안에 대한 중요성은 나날이 증가하고 있다. IPSec(Internet Protocol Security)은 이러한 인터넷 보안 문제에 대한 하나의 해결책으로 개발되었다. IPSec은 IP 계층에서 보안 서비스를 제공하며, 대규모의 인터넷 환경에 적합한 보안 프로토콜이다. IPSec에서 보안 서비스를 제공하기 위한 프로토콜로는 AH(Authentication Header)와 ESP (Encapsulating Security Payload)가 있다. AH와 ESP는 기존의 IP 헤더(Header)에 추가되는 확장 헤더이다. IP 헤더에 대한 보안 서비스를 적용하기 위하여 AH 헤더를 확장 헤더로 추가하고, IP Payload에 대한 보안 서비스를 적용시키기 위하여 사용자 데이터를 ESP로 캡슐화한 후 헤더에 추가한다.

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

본 논문에서는 인증(Authentication)과 암호화(Encryption)를 수행할 수 있는 IPSec 암호 프로세서를 하드웨어로 구현하였다. 구현한 IPSec 암호 프로세서는 Rijndael 암호 알고리즘과 HMAC-SHA-1 인증 알고리즘으로 구성되며, 32-bit 데이터 버스를 이용하여 구현되었다. Xilinx ISE 5.2i를 사용하여 VHDL로 설계하였으며, ModelSim을 사용하여 시뮬레이션 검증을 수행하였고, Xilinx사의 Vertex XCV1000E로 구현하였다.

2. IPSec Protocol

IPSec은 IP 계층에서 보안 서비스를 제공한다. IPSec에서 보안 서비스를 제공하기 위한 프로토콜은 AH와 ESP가 있는데, AH와 ESP는 기존의 IP 헤더에 추가되는 확장 헤더이다. IP 패킷(Packet)은 헤더와 Payload로 나눌 수 있는데, IP 헤더에 대한 보안 서비스를 적용하기 위하여 AH 헤더를 확장 헤더로 추가하고, IP Payload에 대한 보안 서비스를 적용시키기 위하여 사용자 데이터를 ESP로 캡슐화한 후 헤더에 추가한다. 표 1.에 IPSec에서 제공하는 보안 서비스를 나타내었다.

표 1. IPSec 보안 서비스 [1]

	AH	ESP
Access Control	√	√
Connectionless Integrity	√	√
Data Origin Authentication	√	√
Rejection of Replayed Packets	√	√
Confidentiality		√
Limited traffic flow confidentiality		√

2.1 IP Authentication Header (AH)

IP AH는 IP 데이터그램(Datagram)의 비연결성 무결성(Connectionless integrity)과 데이터 발신 인증(Data origin authentication)을 제공한다.[7] AH의 Authentication Data 필드는 ICV(Integrity Check Value)를 포함한다. ICV는 인증 알고리즘에 의해 생성되는 MAC(Message Authentication Code)이다. MAC를 생성하기 위한 인증 알고리즘에는 HMAC-MD5와 HMAC-SHA-1 등이 있는데, 본 논문에서는 HMAC-SHA-1을 선택하였다.

2.2 IP Encapsulating Security Payload (ESP)

IP ESP는 기밀성(Confidentiality), 데이터 발신 인증(Data origin authentication), 비연결성 무결성(Connectionless integrity), 재전송 방지(Anti-replay), 제한된 흐름 기밀성(Limited traffic flow confidentiality)을 제공한다.[8]

ESP가 AH와 다른 점은 ESP는 암호화를 제공한다는 것이다.

본 논문에서는 ESP가 사용하는 암호 알고리즘으로 Rijndael을 구현하였다. ESP가 인증 기능을 제공하기 위해 사용될 때는 AH처럼 HMAC-MD5나 HMAC-SHA-1을 사용한다.

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

IP AH와 ESP에서 사용되는 인증 알고리즘에는 HMAC-MD5와 HMAC-SHA-1이 있다. MD5는 128-bit의 해쉬값(Hash Value)을 출력하는 반면에, SHA-1은 32-bit 더 긴 160-bit의 해쉬값을 출력하며 공격에 보다 더 강하다.[11] 본 논문에서는 HAMC-SHA-1을 구현하였다. 입력받은 $text$로부터 MAC을 구하는 연산 과정을 표 2.과 그림 3.에 나타내었다.

표 2. HMAC의 연산 과정 [4]

단계	설 명
1	$K = B,\ K_0 = K$
2	$K > B,\ K_0 = H(K) \mid 00 \cdots 00$
3	$K < B,\ K_0 = K \mid 00 \cdots 00$
4	$K_0 \oplus ipad$
5	$(K_0 \oplus ipad) \mid text$
6	$H((K_0 \oplus ipad) \mid text)$
7	$K_0 \oplus opad$
8	$(K_0 \oplus opad) \mid H((K_0 \oplus ipad) \mid text)$
9	$H((K_0 \oplus opad) \mid H((K_0 \oplus ipad) \mid text))$
10	왼쪽에서부터 t-byte 만큼 선택

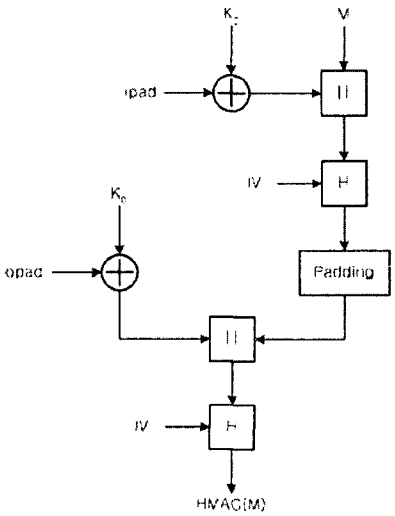

그림 3. HAMC의 구조

4. AES(Rijndael) : 암호(Encryption) 알고리즘

DES가 더 이상 안전성을 보장할 수 없게 되자, NIST에 의해 새로운 AES로 Rijndael이 채택되었다. Rijndael 암호 알고리즘은 알려진 모든 공격에 강하고, 그 응용에 있어서 속도나 하드웨어 구현에 뛰어난 장점을 가지고 있다.[1]

그림 4.에 Rijndael의 구조를 나타내었다. Rijndael 암호 알고리즘은 크게 4개의 연산으로 이루어진다. SubBtye는 S-Box를 이용하여 byte 단위의 치환(Substitution)을 수행한다. ShiftRows는 열(Row)의 순서를 치환(Permutation)시킨다. MixColumn은 $GF(2^8)$ 연산을 이용한 치환(Substitution)이다. AddRoundKey는 bitwise-XOR 연산을 이용하여 라운드 키를 생성한다.

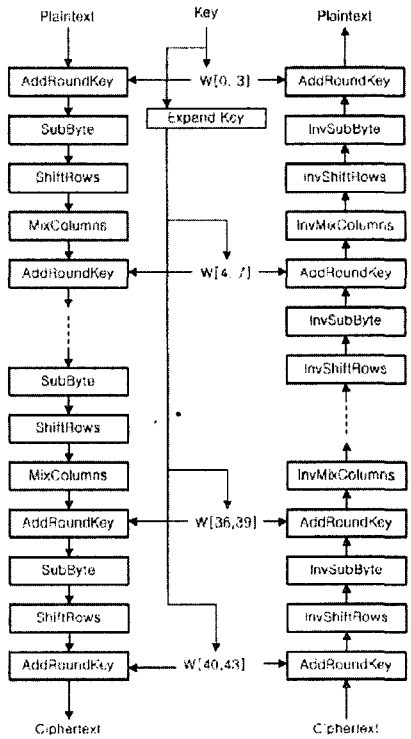

그림 4. Rijndael의 암/복호화 과정 [1]

5. IPSec 암호 프로세서 구현

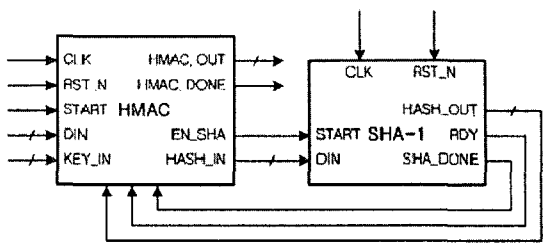

그림 5. HMAC-SHA-1

그림 5.에 구현한 HMAC-SHA-1을 나타내었다. 표 2.의 6단계에서 해쉬 연산을 수행한 다은 9단계에서 한 번 더 SHA-1에 의한 해쉬 연산을 수행해야 하므로 HASH_OUT을 통해 HMAC 블록으로 재입력된다. SHA_DONE으로 마지막 해쉬

연산이 끝났음을 알리고, HMAC는 10단계의 값을 HMAC_OUT으로 출력한다. 그림 6.에 구현한 IPSec 암호 코어 프로세서를 나타내었다.

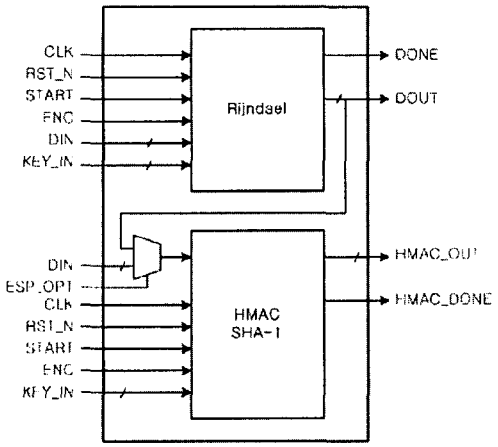

그림 6. IPSec 암호 코어 프로세서

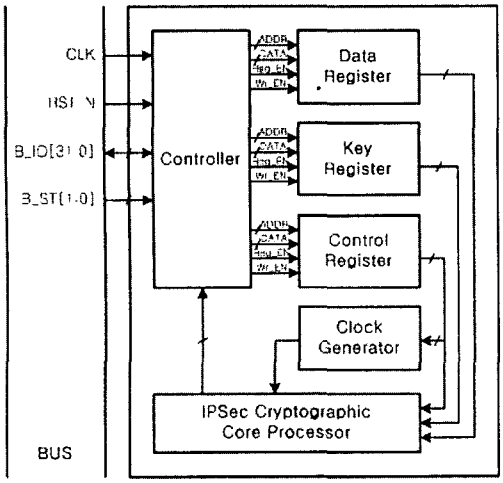

그림 7. 32-bit 데이터 버스용 IPSec 암호 프로세서

그림 7.은 구현한 전체 IPSec 암호 프로세서이다. 32-bit 데이터 버스를 이용하여 구현하였으며, 6개의 블록으로 구성된다. Controller 블록은 각각의 블록에 필요한 제어 신호를 제공한다. Data Register와 Key Register는 Controller로부터 입력된 데이터와 키를 IPSec 암호 코어 프로세서로 전송한다. Control Register는 시작 신호, 암/복호화 모드 선택 신호, 클럭 분주 제어 신호를 IPSec 암호 코어 프로세서에 제공한다. Clock Generator는 클럭 분주 제어 신호에 따라 클럭을 생성한다. IPSec 암호 코어 프로세서는 실질적인 암/복호화를 수행한다.

구현한 HAMC-SHA-1의 최대 동작 주파수는 78.012MHz 이고 처리 속도는 104Mbps 이다. 구현한 Rijndael의 최대 동작 주파수는 86MHz 이고 처리 속도는 216Mbps 이다. 각 블록의 게이트 수는 표 4.에 나타내었다.

표 4. IPSec 암호 프로세서 각 블록의 게이트 수

블 록	게이트 수
Controller	918
Data Register	1,234
Key Register	2,654
Control Register	166
Clock Generator	48
Rijndael	27,482
HMAC-SHA-1	13,311

6. 결 론

본 논문에서는 32-bit 데이터 버스를 이용하여 Rijndael 암호 알고리즘과 HMAC-SHA-1 인증 알고리즘을 통합시킨 IPSec 암호 프로세서를 구현하였다. 구현한 IPSec 암호 프로세서는 IP AH와 ESP의 인증 및 암호화를 수행한다. 또한, 이전의 DES나 3-DES로 구현한 암호 프로세서 보다 더 강인한 보안성을 제공한다. 본 논문에서 구현한 IPSec 암호 프로세서는 Wireless LAN이나 VPN, Firewall 등에 응용될 수 있다.

[참 고 문 헌]

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

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

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

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

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

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

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

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

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

[10] NIST, "Advanced Encryption Standard(AES)", Federal Information Processing Standards Publication 197, Nov 26, 2001

[11] M, McLoone, J. McCanny, "A Single-Chip IPSec Cryptographic Processor", Signal Processing Systems 2002 (SIPS '02) IEEE, 16-18 Oct, 2002.