

IEEE 802.11i 보안용 AES 기반 CCM 프로토콜의 효율적인 하드웨어로 구현

*황석기, 이진우, 김채현, 송유수, 신경욱
금오공과 대학교 전자공학부
e-mail : *ultrastone77@kumoh.ac.kr*

An Efficient Hardware Implementation of AES-based CCM Protocol for IEEE 802.11i Wireless LAN Security

*Seok-Ki Hwang, Jin-Woo Lee, Chay-Hyeun Kim,
You-Su Song, Kyung-Wook Shin
School of Electronic eng., Kumoh National Institute of Technology

Abstract

This paper describes a design of AES-based CCM Protocol for IEEE 802.11i Wireless LAN Security. The CCMP core is designed with 128-bit data path and iterative structure which uses 1 clock cycle per round operation. To maximize its performance, two AES cores are used, one is for counter mode for data confidentiality and the other is for CBC(Cipher Block Chaining) mode for authentication and data integrity. The S-box that requires the largest hardware in AES core is implemented using composite field arithmetic, and the gate count is reduced by about 23% compared with conventional LUT-based design. The CCMP core designed in Verilog-HDL has 35,013 gates, and the estimated throughput is about 768Mbps at 66-MHz clock frequency.

I. 서론

최근 모바일 시대의 개막으로 PDA나 노트북, 휴대폰과 같은 휴대용 단말기의 보급이 확산됨에 따라 이들을 장소에 상관없이 인터넷망에 연결시키는 수단으로써 무선 랜이 핵심기술로 자리 잡고 있다. 무선 랜은 무선채

널을 통해 랜을 확장시킬 수 있는 이동성, 휴대성 및 간편성 등의 이점으로 인하여 그 응용분야가 나날이 확산되고 있다. 휴대용 단말기를 이용해 경매나 쇼핑을 하거나 팩스 수신, 기사 송고, 화상 회의, 원격PC제어 등 업무 관련 서비스도 가능하다. 이밖에 실시간 증권 서비스나 은행업무 (잔액 조회, 현금 인출, 입금, 온라인 서비스)와 같은 개인 금융 업무도 언제 어디서나 단말기만 있으면 충분하다. 하지만 무선인터넷의 브로드캐스팅 특성으로 인해 트래픽 감정이 언제라도 가능하기 때문에 데이터를 보호하기 위해서는 기밀성 및 무결성 서비스와 상호인증 서비스가 매우중요하다. 현재 무선 랜 보안 기술로는 유선 랜과 동등한 형태의 WEP(Wired Equivalent Protocol), 모바일 VPN, 기업형 무선랜 보안 장비, 802.1x등 보안성이 강화된 액세스 포인트, WPKI, 그리고 침입탐지시스템(IDS)이 있다. 특히, WEP은 키 스트림의 단순성으로 인한 실시간 공격과 도청으로 인한 평문 노출, 그리고 DoS(Denial of Service) 공격 가능성 등 보안 알고리즘 자체의 취약점이 밝혀지고 있다[1]. 이와 같은 문제점을 해결하기위한 방안으로 IEEE 802.11i 태스크 그룹에서는 RSN(Robust Security Network)을 기존의 WEP 기반 방식과 구별하여 새롭게 정의하였으며 RSN은 TKIP(Temporal Key Integrity Protocol), CCMP(Counter mode with CBC-MAC Protocol) 두 가지의 보안 메커니즘을 제공한다. TKIP 방식은 단기적 관점에서 앞에서 기술된 보안상의 문제점을 소프트웨어적으로 개선하

기 위한 것이며, 장기적인 관점에서는 알고리즘 자체를 보안 강도가 높은 CCMP로 대체하는 방식을 제안하여 2004년 6월에 표준으로 확정하였다[2]. 그림 1과 같이 무선 랜 환경에서 CCMP를 사용할 경우, AES 암호화 알고리즘의 CBC 모드와 Counter 모드를 적용시킴으로써 데이터의 기밀성과 무결성을 보장할 수 있게 된다.

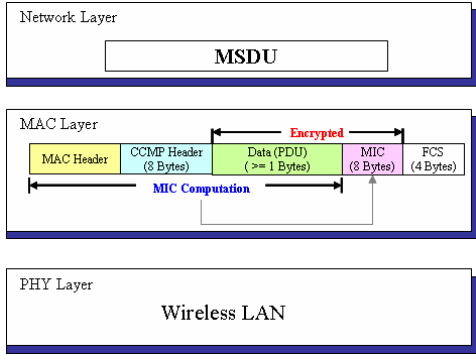


그림 1. 무선 랜 환경에서 적용된 CCMP

본 논문에서는 2장에서는 IEEE 802.11i 무선 랜 보안 표준으로 제정된 CCMP에 대해 기술하고, 3장에서는 AES 기반 CCMP 코어의 설계를, 그리고 4장에선 검증 및 성능 평가를 기술한다.

II. IEEE 802.11i 무선 랜 보안 시스템

CCMP는 CCM 동작모드를 사용하는 AES 암호 알고리즘 기반 프로토콜이며, IEEE 802.11i에서는 AES의 암호 연산만으로 무선 데이터들의 기밀성과 무결성 그리고 사용자 인증이 가능하다고 정의 하고 있다. 또한 CCMP는 AES 암호 알고리즘에서 128비트 키 길이와 128비트 블록크기만을 사용한다.

2.1 Counter with CBC-MAC Protocol (CCMP)

CCM은 데이터의 기밀성을 위한 counter 모드와 데이터의 무결성과 사용자의 인증을 위한 CBC-MAC (Cipher Block Chaining - Message Authentication Code)의 조합으로 구성되어 있다[3]. CBC-MAC 모드를 사용하여 데이터의 무결성과 사용자 인증을 위한 MIC(Message Integrity Code)를 생성하는 과정은 그림 2와 같다. 헤더 정보들을 이용하여 16 바이트 단위로 암호화를 수행하며, 이 후 연속된 평문을 16 바이트 단위로 나누고, 이 값들을 AES의 CBC 모드를 이용하여 계속 암호화한다. 마지막 평문 블록이 16 바이트가 되지 않는 경우에는 0(zero)을 하위에 삽입시켜 16 바이트로 만든 후 암호화 연산을 수행한다. 이 결과로 출력

되는 16 바이트 값 중 상위 8 바이트를 MIC 값으로 사용한다.

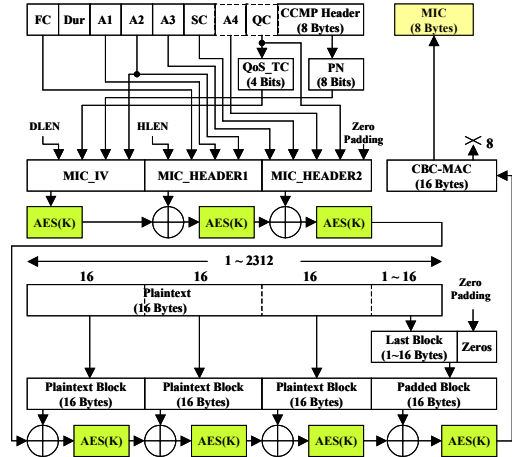


그림 2. CBC 모드를 이용한 MIC 생성 블록도

데이터의 기밀성을 위한 counter 모드 암호화 과정은 그림 3과 같으며, 연속된 평문은 16바이트 단위의 블록으로 나누어진다. 각 평문 블록의 암호화에 사용되는 counter 값은 내부의 계수기에 의해 생성되며, counter에 대한 형식은 문헌[3]에 명시되어 있다. 생성된 counter값들은 AES 코어에 의해 암호화 된 후 해당 평문과 XOR 연산을 거쳐 16 바이트 암호문을 생성하게 된다. 마지막 평문이 16 바이트가 되지 않을 경우 CBC-MAC 모드와 같이 하위에 0(zero)이 삽입되어 암호화 된다. 한편, MIC 값을 암호화 할 때의 counter 값은 최하위 2바이트가 0(zero)으로 채워져 사용된다.

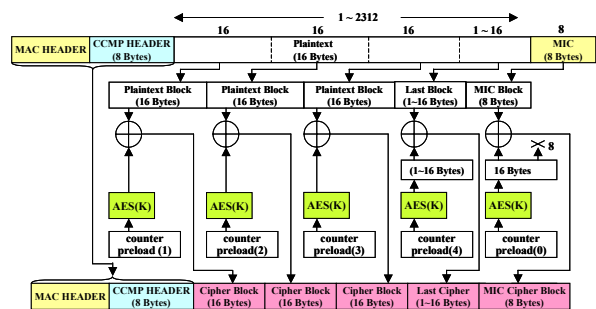


그림 3. CTR 모드를 이용한 암호화 블록도

이와 같은 과정을 통해 암호화된 평문과 MIC 값은 MPDU 헤더, 패킷 오류를 감지하기 위한 FCS(Frame Check Sequence) 등과 함께 그림 4와 같은 형식으로 Encapsulation 되어 송신된다.

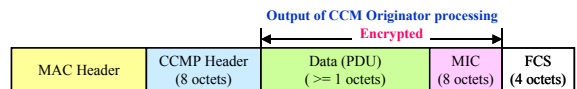


그림 4. CCMP Encapsulation

그림 5는 수신 단에서의 복호화 동작을 나타낸 것으로

수신 단에서는 counter 모드를 이용하여 암호문과 MIC 값을 복호하게 된다. 그리고 복호된 MIC값과 수신 단에서 생성된 MIC값을 비교하여 데이터의 무결성 여부를 판별하게 된다.

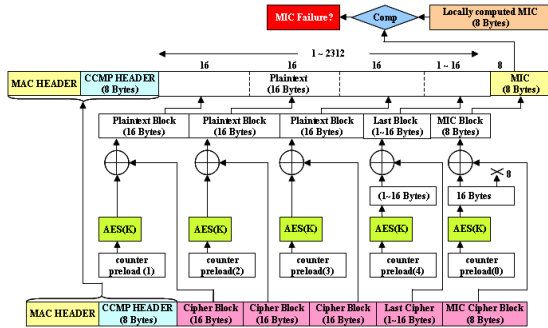


그림 5. 수신단 복호화 블록도

2.2 AES 암호 알고리즘

AES는 non-Feistel 구조를 바탕으로 하고 있으며, 역변환이 가능한 3개의 독립된 라운드 변환으로 구성된 대칭키 암호 알고리즘으로써 FIPS(Federal Information Processing Standard) Pub. 197에 명시 되어 있다. 블록 길이는 128비트이고, 키 길이는 128비트/192비트/256비트 중에서 선택할 수 있으며, 라운드 수(Nr)는 키 길이(Nk)에 따라 10/12/14로 구성된다. AES 알고리즘의 암호화 연산 과정은 그림 6과 같으며, 초기 라운드 키 가산, (Nr-1)번의 반복 라운드 및 최종 라운드의 순서로 처리된다. 최종 라운드를 제외한 (Nr-1)번의 라운드는 ByteSub, ShiftRow, MixColumn 및 KeyAdd 등의 변환으로 구성된다[4]. 암호화 라운드에서 사용되는 라운드 키는 외부에서 입력된 암호 키와 AES 키 생성 알고리즘에 의해 생성된다.

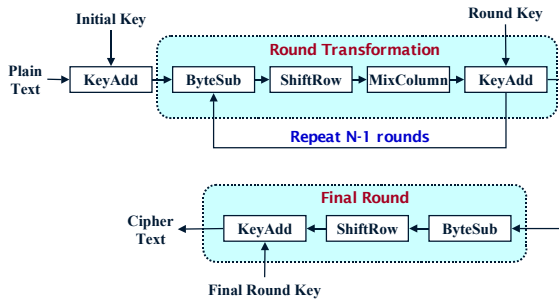


그림 6. AES 알고리즘의 암호화 연산과정

III. AES 기반 CCMP 코어 설계

본장에서는 2장에서 설명된 AES 암호 알고리즘 기반 CCMP의 효율적인 하드웨어 구현에 대해 기술한다.

3.1 아키텍처 개요

설계된 AES 기반 CCMP 코어의 내부 구조는 그림 7과 같으며, 2장에서 설명된 데이터의 기밀성을 위한 CTR 블록, 데이터의 무결성 검증과 사용자 인증을 위한 CBC 블록, 그리고 이들 두 블록에서 필요한 각종 제어 신호를 생성하는 제어 블록 등으로 구성된다. 128 비트 데이터 패스로 구현되어 라운드 연산이 1클록에 처리에 처리되도록 설계되었다.

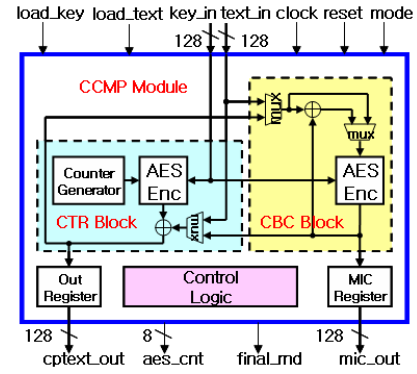


그림 7. AES 기반 CCMP 코어 블록도

CTR 블록과 CBC 블록은 동일한 키 입력을 가지며, 그림 8의 타이밍도에서 보는 바와 같이 load_key의 신호가 활성화 되면 128비트의 키 값을 입력 받는다. load_text 신호가 활성화 되면 128비트의 헤더 값들과 평문들을 입력받으면서 CBC 블록에서는 MIC 값을 생성하게 된다. 이와 동시에 CTR 블록에서는 입력되는 헤더 값들을 이용하여 counter preload 값을 생성한 후 각 평문블록에 대해 암호화를 수행한다. 마지막으로 CBC 블록에서 생성된 MIC 값을 암호화함으로써 하나의 패킷에 대한 CCMP 암호화 연산을 종료하게 된다.

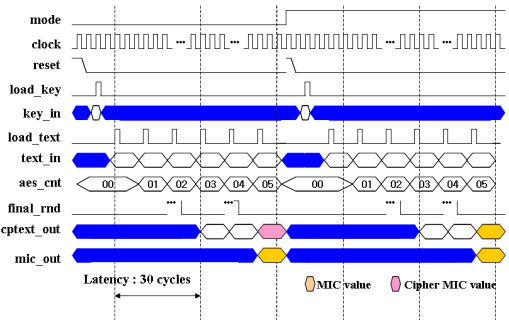


그림 8. CCMP 코어의 동작 타이밍도

3.2 효율적인 하드웨어 구현을 위한 방안

본 논문에서는 하드웨어의 복잡도를 개선하기 위해 AES 라운드 블록에서 가장 많은 게이트를 필요로 하는 S-box에 대해 문헌[5]에 제안된 composite field 연산 방법을 이용하여 설계하였으며, 이를 통해 면적이 최소화 되도록 하였다.

S-box는 입력된 8비트 데이터에 대해 GF(2⁸)상에서

곱의 역원을 구하고 affine transformation이라 정의된 행렬과 곱하고 정해진 상수와 덧셈연산을 한다. $GF(2^4)$ 상에서 곱의 역원은 체(Field)의 변환을 이용하면 구할 수 있다. 본 논문에서는 $GF(2^4)$ 상에서의 곱의 역원 계산회로와 S-box를 그림 9와 같이 설계하였다.

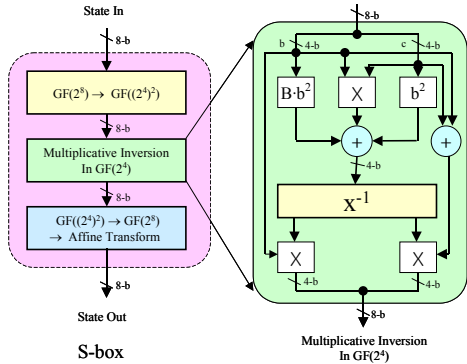


그림 9. 제안된 S-box

그림 9에서 $GF(2^4)$ 상에서의 곱의 역원은 곱셈과 덧셈, 그리고 $GF(2^4)$ 의 역원(x^{-1})으로 계산된다. 덧셈은 XOR 연산, 곱셈은 AND와 XOR 연산만으로 구현되며, $GF(2^4)$ 상의 역원은 Lookup Table로 구현하였다.

IV. 검증 및 성능 평가

설계된 AES 기반 CCMP 코어는 Verilog-HDL로 모델링되었으며 CCMP 표준안[3]에 명시된 테스트벡터를 이용하여 검증하였다. 그림 10에서 보는바와 같이 128 비트의 헤더 값들과 평문 "00112233_44556677_8899aa_bb_ccddeeff" 그리고 128 비트의 암호 키 "00010203_04050607_08090a0b_0c0d0e0f"를 입력벡터로 사용하여 생성된 MIC의 상위 8 바이트 값은 "a2ef_035d_570c_0d9c"가 출력되었다. 이를 다시 복호화 한 결과, 입력 벡터와 동일한 결과가 출력되어 모든 논리기능이 정상적으로 동작하는 것을 확인하였다.

/mic_out	000000	00000000000000000000000000000000	a2ef035d570c0d9cd7aef087a0f096
/text_in	001122	00112233445566778899aabbccddeeff	
/key_in	000102	000102030405060708090a0b0c0d0e0f	

그림 10. CCMP 코어의 Function verification

검증이 완료된 HDL 모델은 0.25-um CMOS Cell 라이브러리와 Synopsys 툴을 이용하여 합성하였으며, 전체 CCMP 코어는 총 35,013게이트로 구현되었다. 한편, S-box를 $GF(2^8)$ 의 LUT로 구현하여 CCMP 코어를 설계한 일반적인 방법은 39,883게이트를 필요로 하며, 따라서 본 논문의 방법은 LUT를 이용하는 방법에 비해 약 23%의 게이트가 감소되었다. 합성된 회로에 대한 타이밍 시뮬레이션 결과, 66-MHz 클럭으로 안전하게

동작하여 768Mbps의 성능이 예상된다.

V. 결 론

본 논문에서는 IEEE 802.11i 무선 랜 보안을 위한 AES 기반 CCMP 코어의 설계에 대해 기술하였다. CCMP 코어는 128 비트 데이터 패스로 구현되어 라운드 연산이 1클럭에 처리되도록 설계되었다. 데이터 기밀성을 위한 counter 모드와 사용자 인증 및 데이터 무결성 검증을 위한 CBC(Cipher Block Chaining) 모드가 두개의 AES 암호 코어로 병렬 처리되도록 함으로써 전체 성능의 최적화를 이루었다. 또한, AES 암호코어에서 하드웨어 복잡도에 가장 큰 영향을 미치는 S-box를 면적이 최소화 되도록 설계하였다. CCMP 코어는 35,013게이트로 구현되었으며, 66-MHz의 클럭으로 안전하게 동작하여 768Mbps의 성능이 예상된다.

참고문헌

- [1] 정병호, 강유성, 김신호, 정교일, "공중 무선랜 망에서 인증 및 키관리 기술 동향", 전자통신 동향 분석 제17권 제 4호, 2002.8
- [2] 강유성, "사용자 중심의 무선 랜 이동보안 기술 표준화 논의 본격화", IT Standard Weekly, 한국정보통신기술협회, 2005-16호
- [3] IEEE Standards 802.11i, "Draft supplement to standard for telecommunications and information exchange between systems - LAN/MAN specific requirements - PART 11 : Wireless Medium Access control(MAC) and physical layer (PHY) specifications : Specification for Enhanced Security", Nov. 2002
- [4] 안하기, 신경욱, "AES Rijndael 블록 암호 알고리즘의 효율적인 하드웨어 구현", 한국 정보보호학회 논문지, 제12권2호, pp.53-64, 2002
- [5] V. Rijndael, "Efficient implementation of the Rijndael S-box", <http://www.esat.kuleuven.ac.be/~rijnmen/rijndael/sbox.pdf>

※ 2005년도 IT SoC 핵심설계인력양성 사업의 SoC 설계실습프로젝트 지원에 의한 연구 결과의 일부임.
 ※ 반도체설계교육센터 (IDEC)의 CAD Tool 지원에 감사드립니다.