IEEE 802.11i 무선 랜 보안을 위한 AES 기반 CCMP 코어 설계

준회원 황 석 기*, 김 종 환**, 정회원 신 경 욱**

A Design of AES-based CCMP core for IEEE 802.11i Wireless LAN Security

Seok-Ki Hwang*, Jong-Whan Kim** *Associate Members*,
Kyung-Wook Shin** *Regular Member*

요 약

본 논문에서는 IEEE 802.11i 무선 랜 보안을 위한 AES(Advanced Encryption Standard) 기반 CCMP (Counter mode with CBC-MAC Protocol) 코어의 설계에 대해서 기술한다. 설계된 CCMP 코어는 데이터의 기밀성을 위한 CTR(counter) 모드와 인증 및 데이터 무결성 검증을 위한 CBC 모드의 동작이 두개의 AES 암호 코어로 병렬처리 되도록 설계되어 전체 성능의 최적화를 이루었다. AES 암호 코어에서 하드웨어 복잡도에 가장 큰 영향을 미치는 S-box를 composite field 연산 방식을 적용하여 설계함으로써 기존의 LUT(Lookup Table) 기반의 구현방식에 비해 게이트 수가 약 27% 감소되도록 하였다. 설계된 CCMP 코어는 Excalibur SoC 장비를 이용하여 H/W-S/W 통합 검증을 수행하였으며, 0.35-um CMOS 표준 셀 공정으로 MPW 칩으로 제작하고, 제작된 칩의 테스트 결과 모든 기능이 정상 동작함을 확인하였다. 설계된 CCMP 프로세서는 약 17,000개의 게이트로 구현되었으며, 116-MHz@3.3-V의 클록으로 안전하게 동작하여 353-Mbps의 성능이 예상되어 IEEE 802.11a와 802.11g 표준의 MAC 성능인 54-Mbps를 만족한다.

Key Words : CCMP, Wireless LAN Security, Robust Security Network, Authentication, AES

ABSTRACT

This paper describes a design of AES-based CCMP(Counter mode with CBC-MAC Protocol) core for IEEE 802.11i wireless LAN security. To maximize the performance of CCMP core, two AES cores are used, one is the counter mode for data confidentiality and the other is the CBC 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 27% compared with conventional LUT(Lookup Table)-based design. The CCMP core was verified using Excalibur SoC kit, and a MPW chip is fabricated using a 0.35-um CMOS standard cell technology. The test results show that all the function of the fabricated chip works correctly. The CCMP processor has 17,000 gates, and the estimated throughput is about 353-Mbps at 116-MHz@3.3V, satisfying 54-Mbps data rate of the IEEE 802.11a and 802.11g specifications.

※ 본 연구는 정보통신부의 출연금 등으로 수행한 정보통신연구개발사업의 연구결과의 일부임.
※ IDEC의 CAD Tool 지원에 감사드립니다.
* 씨앤에스테크놀로지(주) (ultra77@cnstec.com), ** 금오공과대학교 ({kwshin}@kumoh.ac.kr)
논문번호 : KICS2005-12-509, 접수일자 : 2005년 12월 27일, 최종논문접수일자 : 2006년 5월 11일

Ⅰ. 서 론

정보화 사회가 급진전되면서 인터넷 서비스를 비롯한 다양한 멀티미디어 서비스의 발달과 함께 정보통신의 수요가 급격히 증가하였다. 또한 셀룰러/PCS를 이용한 이동 통신 서비스가 생활의 일부분으로 보편화되면서 데이터 서비스에 있어서도 이동성과 편리함을 추구하려는 소비자들의 욕구가 증가하였다. 이에 무선 랜은 유선 랜에 비해 상대적으로 낮은 통신 속도, 높은 통신 에러율 등의 제약요인에도 불구하고 이동성, 편리성 등의 장점으로 인하여 기존 유선 랜을 대체하는 킬러 어플리케이션으로 자리 잡았다. 그러나 무선 랜은 유선 랜 환경과 달리 브로드캐스팅 네트워크이므로 액세스 포인트(AP : Access Point)의 beacon 신호를 수신할 수 있는 영역 내에 있는 모든 단말기들은 다른 사람의 송수신 데이터의 내용을 수신할 수 있다. 따라서 무선 랜에서는 데이터의 허가된 수신자 이외에 다른 사람이 메시지 내용을 보지 못하게 하는 데이터 기밀성과 인증 서비스가 매우 중요하다[1]. 현재 사용되고 있는 IEEE 802.11 표준은 무선구간의 보안을 위하여 WEP(Wired Equivalent Privacy) 알고리듬을 사용하고 유선구간에서는 RADIUS(Remote Authentication Dial In User Service)나 TACACS+ (Terminal Access Controller Access Control System) 프로토콜을 이용하여 인증 정보의 보안성을 제공하고 있다. 그러나 WEP 알고리듬에서는 IV(Initialization Vector)가 암호화되지 않고 평문으로 전송되며 암호키를 AP에 접속된 모든 단말이 공유하므로 실시간 공격 및 도청으로 인한 평문 노출의 취약성이 존재한다. IEEE 802.11i 그룹에서는 기존 WEP의 단점을 보완하기 위하여 RSN(Robust Security Network)을 새롭게 정의하였으며 RSN은 TKIP(Temporal Key Integrity Protocol), CCMP (Counter with CBC-MAC Protocol) 보안 메커니즘을 제공한다. TKIP 방식은 단기적 관점에서 앞에서 기술된 보안상의 문제점을 소프트웨어적으로 개선하기 위한 것이며, 장기적인 관점에서 보안 알고리즘 자체를 보안강도가 높은 AES(Advanced Encryption Standard)로 바꾸는 방식을 제안하고 있다[2].

본 논문에서는 IEEE 802.11i 무선 랜 보안 메커니즘의 효율적인 하드웨어 구현방법을 제시하였다. 데이터 기밀성을 위한 CTR(counter) 모드와 사용자 인증 및 데이터 무결성 검증을 위한 CBC(Cipher Block Chaining)모드가 두개의 AES 암호 코어로 병렬 처리되도록 설계하여 성능 최적화를 이루었으며, 하드웨어 복잡도에 가장 큰 영향을 미치는 AES 코어의 S-box를 composite field 연산방식을 적용하여 구현함으로써 기존의 LUT 기반 구현방식에 비해 게이트 감소를 이루었다.

제안된 CCMP코어는 Verilog-HDL로 모델링하여 설계하였으며, 다양한 CAD 툴을 이용하여 기능 및 타이밍 검증을 마친 후, Excalibur SoC 장비에 구현하여 검증하였고, 최종적으로 IDEC의 MPW 칩으로 제작하고 제작된 칩을 테스트 하였다.

본 논문의 Ⅱ장에서는 무선 랜 보안 알고리듬으로 제정된 CCMP의 개요에 대해 기술하며, Ⅲ장에서는 CCMP 코어의 효율적인 하드웨어 구현 방법과 CCMP 코어의 ASIC 구현에 대해 기술한다. Ⅳ장에서는 CCMP 코어의 설계 검증 및 성능평가에 대해 기술하며 끝으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. CCMP의 개요

CCMP는 무선 랜 환경에서 데이터의 무결성과 은닉성을 동시에 보장하기 위하여 미국 국가기술표준국(National Institute of Standards and Technology; NIST)에서 제안한 AES의 모드 운영을 기반으로 하는 프로토콜이다. AES는 128비트 블록단위로 암·복호 연산을 수행하며, 이때 다수개의 블록들을 연관시켜 암호문의 기밀성을 강화시키는 것이 동작모드(mode operation)이다. NIST는 DES를 사용할 때부터 표준 동작모드를 정해두었으며, AES의 채택 후에 "NIST Special Publication 800-38A"[6]의 문서를 통하여 5가지의 표준 동작모드를 제안하고 있다. 5가지의 동작모드는 ECB(Electronic Codebook), CBC(Cipher Block Chaining), CFB (Cipher Feedback), OFB(Output Feedback), CTR (Counter) 등이다. CCMP는 인증 및 메시지의 무결성 검증을 위한 CBC 모드와 메시지의 기밀성을 위한 CTR 모드로 구성되며, 복호연산 없이 암호연산만을 사용하므로 적은 하드웨어로 구현이 가능하다는 특징을 갖는다[3, 7].

2.1 CBC 모드를 이용한 MIC 생성

CBC 모드는 인증과 무결성 검증을 위한 MIC (Message Integrity Code) 값을 생성하는 모드이며, 그림 1은 CBC 모드를 이용한 MIC 생성과정을 보이고 있다. 128비트의 IV가 AES에 의해 암호화되고, 그 결과는 MIC 헤더-1과 XOR 연산된 후 AES

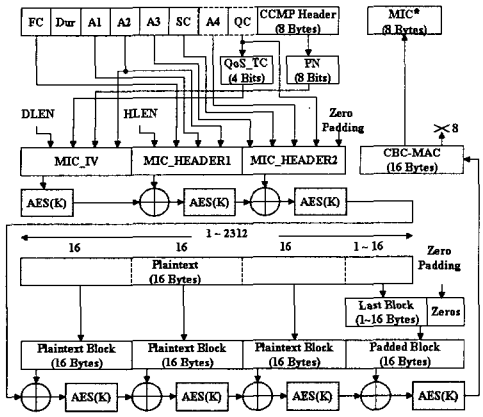


그림 1. CBC 모드를 이용한 MIC 생성

에 의해 암호화되며, 그 결과는 다시 MIC 헤더-2와 XOR 연산된 후 AES에 의해 암호화된다. 그 결과는 입력되는 16바이트의 평문 블록과 XOR 연산된 후 AES에 의해 암호화되고, 그 결과가 다시 다음 데이터 블록의 암호 연산에 IV로 사용되는 방식으로 각 데이터 블록들의 암호화 연산이 chain 형태로 연결되는 방식으로 동작한다. 초기 3개의 IV 값은 CCMP 헤더 및 프레임 헤더 정보들로부터 생성된다. 마지막 평문 블록이 16바이트가 되지 않는 경우에는 하위에 0을 삽입시켜 16바이트를 만든 후 암호화 연산을 수행한다. 최종 출력 16바이트 결과 값 중 상위 8바이트 값이 인증을 위한 MIC 값으로 사용된다. 한편, 수신단에서도 동일한 과정으로 MIC 값을 생성한다.

2.2 CTR 모드를 이용한 암·복호 연산

CTR(counter) 모드는 AES가 차세대 블록 암호 알고리즘으로 채택되면서 새롭게 추가된 모드이며, CTR 모드를 이용한 암호화 과정은 그림 2와 같다. 각 데이터 블록마다 생성된 카운터 값은 AES에 의해 암호화되고, 그 결과를 16바이트의 평문 데이터와 XOR 연산하여 암호문이 생성된다. 암호화 과정에 사용되는 카운터 값은 각 MPDU 마다 서로 다른 초기 값을 가지며, MPDU 내에서는 주어진 초기 값으로부터 1씩 증가된 카운터 값이 사용된다. 마지막 평문 블록이 16바이트가 되지 않는 경우에는 하위에 0을 삽입하여 암호화를 수행하며, 결과 중 유효 바이트 길이만큼만 취하고 나머지는 버리게 된다. 한편, CBC 모드에서 생성된 MIC 값도 CTR 모드를 통해 암호화하며, 이때 카운터 값의 하위 8바이트는 0으로 채워져 사용된다.

CTR 모드 연산에 의해 암호화된 평문과 MIC

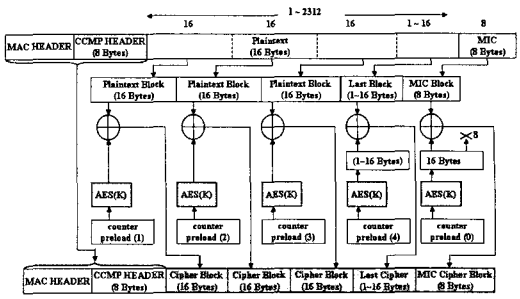


그림 2. CTR 모드를 이용한 데이터 암호화

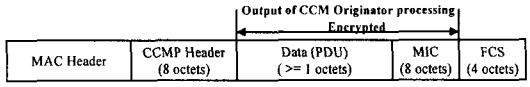


그림 3. CCMP 인캡슐화

값은 MPDU 헤더, 패킷 오류 감지를 위한 FCS (Frame Check Sequence) 등과 함께 그림 3과 같은 형식으로 encapsulation 되어 송신된다.

수신단에서의 복호화 과정은 그림 4와 같으며, CTR 모드 암호화 과정과 유사한 연산을 통하여 평문과 복호된 MIC 값을 출력한다. 복호된 MIC 값과 수신단에서 CBC 모드 연산을 통해 생성된 MIC 값을 비교하여 두 MIC 값이 동일하면 데이터의 무결성이 확인된다. CTR 모드의 암호화 과정과 복호화 과정은 모두 AES 암호 연산만으로 구현된다.

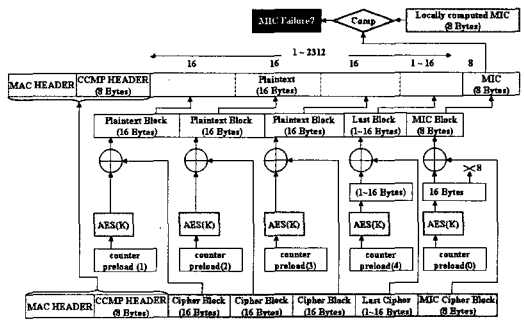


그림 4. CTR 모드를 이용한 데이터 복호화

2.3 AES 암호 알고리듬

AES 암호 알고리듬[4]은 non-Feistel 구조를 바탕으로 하고 있으며, 역 변환이 가능한 3개의 독립된 라운드 변환으로 구성된다. 블록 길이는 128비트이고, 키 길이는 128/192/256비트 중에서 선택할 수 있으며, 라운드 수 (Nr)는 키 길이 (Nk)에 따라 10/12/14로 구성된다. CCMP에 사용되는 AES는 블록 길이와 키 길이가 모두 128비트로 고정되어있다.

AES 알고리듬의 암호화 연산은 그림 5와 같으

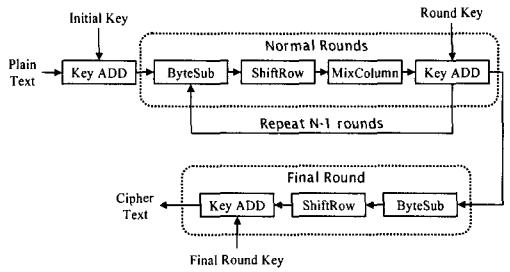


그림 5. AES의 암호화 연산 과정

며, 초기 라운드 키 가산, (Nr-1)번의 반복 라운드 및 최종 라운드의 순서로 처리된다. 최종 라운드를 제외한 (Nr-1)번의 반복 라운드는 4행×4열로 구성되는 State에 대해 ByteSub, ShiftRow, MixColumn 및 KeyAdd 등의 변환으로 구성된다.

Ⅲ. AES 기반 CCMP 코어 설계

3.1 아키텍처 개요

설계된 CCMP 코어는 두개의 AES 암호 코어를 사용하여 데이터의 기밀성을 위한 CTR 모드와 사용자 인증과 무결성 검증을 위한 CBC 모드가 병렬 처리 되도록 설계되었으며, 두 AES 코어는 하나의 키 생성기를 공유하도록 하여 면적이 최소화되도록 하였다. 또한, AES 암호 코어에서 하드웨어 복잡도에 가장 큰 영향을 미치는 S-box를 composite field 연산 방식을 적용하여 설계함으로써 면적의 최적화를 이루었다. 설계된 CCMP 코어의 구조는 그림 6과 같으며, 데이터 기밀성을 위한 CTR 블록, 무결성 검증과 인증을 위한 CBC 블록, 라운드 키 생성 블록, 그리고 각종 제어신호를 생성하는 제어블록 등으로 구성된다.

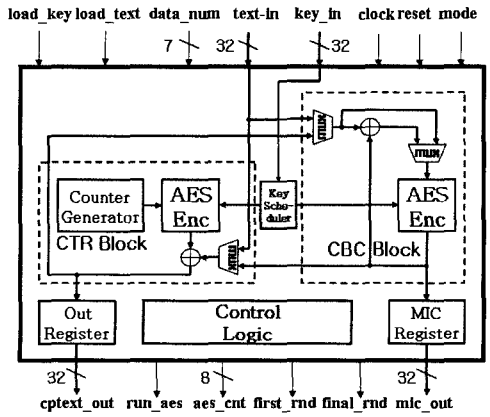


그림 6. 설계된 CCMP 코어의 블록도

표 1. CCMP 코어 입·출력 신호 정의

Signal7	I/O	Width	Description	
load_key	In	1	AH	Enable signal for loading key
load_text	In	1	AH	Enable signal for loading text
reset	In	1	AL	Reset signal
mode	In	1	0	Encapsulation
			1	Decapsulation
clock	In	1	Clock signal	
data_num	In	7	Packet Data number	
key_in	In	32	Temporal Key input	
text_in	In	32	Plain(Cipher) text input	
run_aes	Out	1	Signal indicating that AES is running	
first_rnd	Out	1	Signal indicating the first round of AES	
final_rnd	Out	1	Signal indicating the final round of AES	
aes_cnt	Out	8	Signal indicating the iteration # of AES	
mic_out	Out	32	MIC output	
cptext_out	Out	32	Cipher(Plain) text output	

CCMP 코어의 입·출력 신호를 표 1에 나타내었다. 입·출력 인터페이스는 32비트이며 키와 데이터의 입력을 위한 enable 신호는 'Active High'로 동작하도록 설계하였다. CCMP 코어는 mode='0'일 때 Encapsulation, mode='1'일 때 De-capsulation을 수행하게 된다. data_num는 MPDU(1 ~ 2,312 바이트)를 구성하는 16바이트 데이터 블록의 개수를 지정하는 신호이다.

설계된 코어의 동작은 그림 7에서 보는 바와 같이 load_key의 신호가 활성화되면 128비트의 키 값을 32비트씩 4번에 걸쳐 입력 받는다. load_text 신호가 활성화 되면 128비트의 헤더 값들과 평문들을 각각 4번에 걸쳐 32비트씩 입력받으면 CBC 블록에서는 MIC 값이 계산되고, 동시에 CTR 블록에서는 평문 블록에 대해 암호화를 수행한다. CBC 블록에서 생성된 MIC 값이 암호화되면 주어진 패킷에 대한 CCMP의 암호화 연산이 종료된다. CCMP의 복호화 연산은 암호화 연산과 동일하게 이루어진다.

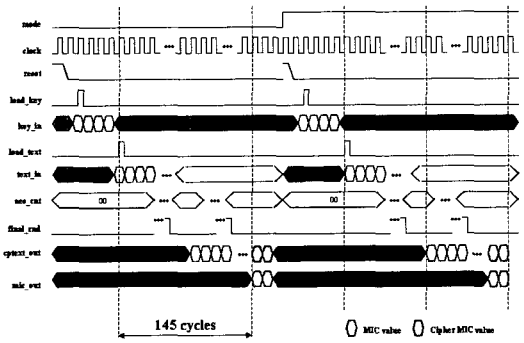


그림 7. CCMP 코어의 동작 타이밍도

CCMP를 하나의 AES 암호기를 사용하여 구현하는 경우, 최대 2,312바이트의 MSDU를 처리하는데 있어서 CBC 모드와 CTR 모드 연산을 위해 최대 (2,312바이트*2)/16바이트=289번의 AES 연산이 수행되어야 한다. 본 논문에서는 CBC 모드와 CTR 모드가 병렬 처리되기 때문에 145번의 AES 연산만으로 수행이 가능하여 고속 처리가 가능하다.

3.2 효율적인 하드웨어 구현 방안

AES 코어에서 가장 큰 하드웨어를 필요로 하는 부분은 S-box 회로이다.[5] 본 논문에서는 composite field 연산방법[8]을 이용한 S-box 구현을 통해 전체적인 하드웨어 면적이 최소화되도록 하였다.

S-box는 8비트 데이터에 대해 $GF(2^8)$상에서 곱의 역원을 구하고 affine 변환이라 정의된 행렬과 곱하고 정해진 상수와 덧셈연산을 수행하는 두 단계로 이루어진다. $GF(2^4)$상에서 곱의 역원은 체(field)의 변환을 이용하면 효율적으로 구할 수 있다. 일반적으로 $GF(2^8)$의 원소들은 계수가 $GF(2^4)$의 원소인 1차 다항식으로 변환이 가능하며 기약 다항식은 x^2+Ax+B으로 표현된다. 임의의 다항식 $bx+c$의 곱에 대한 역원은 식(1)과 같다.

$$(bx+c)^{-1}=b(b^2B+bcA+c^2)^{-1}x+(c+bA)(b^2B+bcA+c^2)^{-1} \quad (1)$$

이때 A와 B는 기약 다항식의 성질을 만족시키는 어떤 값이라도 가능하므로 본 논문에서는 $A=(01)_H$, $B=(08)_H$ 을 사용하였다[8].

곱에 대한 역원 연산과정 전·후에 $GF(2^8)$에서 $GF((2^4)^2)$으로의 변환과 그 역변환 과정이 추가되면 $GF(2^8)$보다 상대적으로 작은 면적의 S-box를 구현할 수 있게 된다. $GF(2^4)$상에서의 곱의 역원

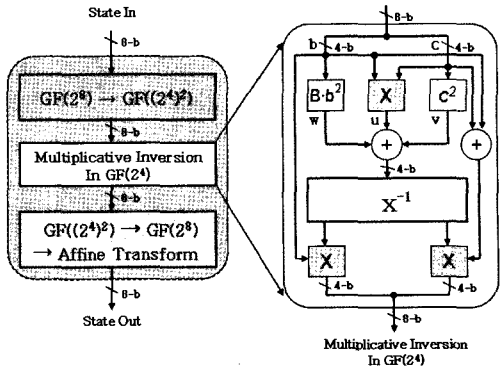


그림 8. composite field 연산을 이용한 S-box의 구현

계산회로와 S-box는 그림 8과 같이 설계되었다. 그림 8에서 $GF(2^4)$상에서의 곱의 역원은 곱셈과 덧셈, 그리고 $GF(2^4)$상의 역원(x^{-1})으로 계산된다.

3.3 CCMP 코어의 ASIC 구현

설계된 CCMP 코어는 다음과 같은 설계 및 검증 과정을 통해 IDEC MPW 공정으로 칩을 제작하였다. Verilog-HDL로 설계된 CCMP 코어의 기능 검증이 완료된 후, 0.35-um CMOS 셀 라이브러리를 이용하여 논리합성을 하였다. 합성 후, CubicWare 툴을 이용하여 합성된 회로에 대한 logical DRC 검사와 각 셀의 지연특성을 지닌 SDF를 추출하였으며, 이를 이용한 STA(Static Timing Analysis)를 통해 타이밍 분석을 하였다. 검증이 완료된 회로는 P&R을 통해 레이아웃을 설계하였으며, post-layout STA에 의한 타이밍 분석과 post-layout 타이밍 시뮬레이션을 수행한 결과 모든 논리기능이 정상적으로 동작함을 확인하였다. 그림 9는 설계가 완료된 CCMP 코어의 레이아웃 도면을 보인 것이다.

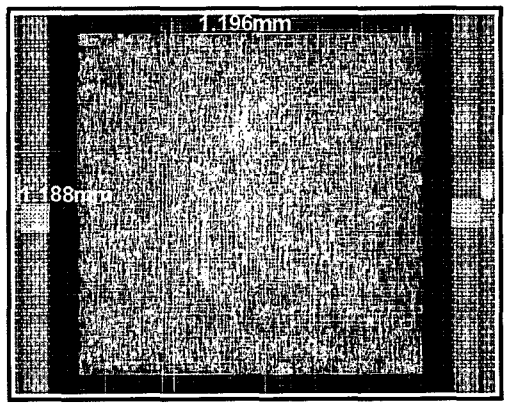
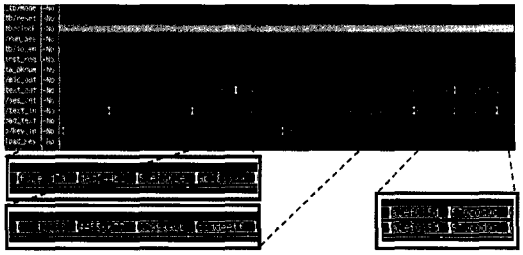


그림 9. CCMP 코어의 레이아웃 도면



Plaintext : 0011_2233_4455_677_8899_aabb_ccdd_eeff
Cipher key : 0001_0203_0405_0607_0809_0a0b_0c0d_0e0f

그림 10. 설계된 CCMP 코어의 post-layout 검증결과

Ⅳ. 설계 검증 및 성능 평가

4.1 설계 검증

설계된 CCMP 코어는 CCMP 표준안[2]에 명시된 테스트 벡터를 이용하여 검증하였다. 128비트의 헤더 값들과 평문 "00112233_44556677_8899aabb_ccddeeff", 그리고 128 비트의 암호 키 "00010203_04050607_08090a0b_0c0d0e0f"를 입력벡터로 사용하여 인증을 위한 MIC 값을 생성한다. 생성된 MIC의 상위 8바이트 값은 "a2ef035d_570c0d9c"가 출력되었으며, 이를 다시 복호한 결과 동일한 MIC 값이 출력되어 논리기능이 정상적으로 동작함을 확인하였다. P&R 후 post-STA가 만족된 netlist로 post-layout 시뮬레이션을 수행하였으며, 그림 10의 post-layout 시뮬레이션 결과가 pre-layout 시뮬레이션 결과와 동일하여 P&R 후에도 논리기능이 정상적으로 동작함을 확인하였다.

4.2 성능 평가

CCMP 코어 설계에 사용된 AES 코어는 0.35-um CMOS 셀 라이브러리로 합성한 결과 약 8,120 게이트로 구현되었다. 합성된 회로에 대한 타이밍 분석 결과, 라운드 변환블록의 최대 지연시간은 8ns로 분석되었으며, AES 코어는 125-MHz@3.3-V로 동작 가능할 것으로 평가되었다. 설계된 AES 코어의 성능은 식 (2)와 같이 정의된다.

$$AES\text{코어의 동작 성능} = (128 \div (N_r + 1)) \times f \quad (2)$$

여기서, f는 주파수, Nr=41은 라운드 수를 나타낸다. 125-MHz@3.3-V로 동작하는 경우 128비트 키 길이에 대한 암·복호율을 식 (2)로부터 계산하면 380-Mbps의 성능을 갖는다. AES 코어의 특성을 표 2에 요약하였다. 한편, LUT 기반의 S-box 구현방법을 적용하는 AES 코어는 최대 지연시간이 약 7.8-ns이고 약 11,053게이트를 필요로 한다. 따라서 composite field 연산을 적용하여 설계된 본 논문의 AES 코어는 기존의 LUT 방식보다 약 27%의 게이트 감소가 얻어졌다.

표 2. AES 코어의 특성

구분	성능
게이트 수	8,114
동작 주파수	125-MHz @3.3-V
평균 클럭 수	4 클럭 / 라운드
동작 성능	380-Mbps
라운드 키 생성	온라인 방식
데이터 입·출력	32비트
S-box 연산방식	Composite field

표 3. 설계된 CCMP 코어의 특성

구분	성능
게이트 수	17,000
동작 주파수	116-MHz @3.3-V
평균 클럭 수	4 클럭 / 라운드
동작 성능	353-Mbps
MPDU 처리율	145 Cycle/2312 Byte
라운드 키 생성	온라인 방식
데이터 입·출력	32비트

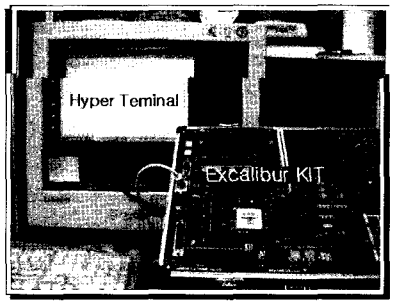


그림 11. CCMP 코어의 H/W-S/W 통합 검증 시스템

CCMP 코어는 논리합성 결과 약 17,000 게이트로 구현되었으며, 최대 지연시간이 8.6-ns로 분석되어 116-MHz@3.3-V로 안전하게 동작할 것으로 예상된다. 따라서 표 3에서 보는 바와 같이 128비트 키 길이에 대한 암·복호 성능을 식 (2)를 이용하여 계산하면 353-Mbps의 성능을 가져 IEEE 802.11a, 802.11g의 MAC layer 성능인 54-Mbps를 충분히 만족시키는 결과이다.

4.3 하드웨어 구현 및 동작 검증

설계된 CCMP 코어는 그림 11과같이 ARM922T

와 FPGA가 내장된 Excalibur SoC 장비를 사용하여 하드웨어/소프트웨어 통합 검증을 하였다. 설계된 CCMP 코어와 AMBA 버스 인터페이스 회로를 Excalibur 내의 FPGA 영역에 구현하고, 테스트 벡터 생성과 UART 통신을 위한 소프트웨어를 연동시켜 FPGA 영역에 구현된 CCMP 코어의 동작을 검증하였다.

CCMP 코어의 encapsulation 모드 동작결과는 그림 12와 같다. 입력된 128비트의 헤더 값과 두개의 128비트 평문 "00112233_44556677_8899aabb_ccdd eeff", "01234567_89abcdef_fedcba98_76543210"와 128비트의 암호 키 "00010203_04050607_08090a0b_0c0d0e0f"가 AHB 버스를 통해 FPGA 내의 Regi_file에 저장된 후, CCMP 코어는 Regi_file의 데이터를 읽어 encapsulation 과정을 수행하고 그 결과를 다시 Regi_file에 저장한다. CCMP 코어에서 encapsulation 과정이 끝나면 ARM 프로세서는 AHB 버스를 통해 Regi_file에 저장된 암호문 "f32e8d7a_dad544b2_53e3862e_ab283399", "1abb5191_5f833b75_b9a3dc89_d339df87"과 MIC 값 "a2ef035d_570c0d9c_df7aebf0_87a0f096"을 읽어 출력한다.

CCMP의 decapsulation 과정에 대한 검증 결과는 그림 13과 같으며, 복호 결과가 encapsulation 과정의 입력 평문과 일치함을 보여주고 있으며, 또한 수신단에서 생성된 MIC 값과 CTR 모드를 통해 복호된 MIC 값이 동일함을 보여 주고 있어 데이터의 무결성이 입증된 것을 확인할 수 있다. 이와 같이 CCMP 코어의 하드웨어/소프트웨어 통합 검증을 통해서 설계된 CCMP 코어의 논리기능이 정상적으로 동작함을 확인하였다.

0.35-um IDEC MPW 공정으로 제작된 칩을 PC와 인터페이스하여 logic analyzer로 테스트한 결과는 그림 14와 같으며, 평문 "00112233_44556677_8899aabb_ccddeeff"에 대해 암호문 "f32e8d7a_dad544b2_53e3862e_ab283399"가 출력되어 논리기능이 정상 동작함을 확인하였다.

V. 결 론

본 논문에서는 무선 랜의 보안 안정성 향상을 위하여 IEEE 802.11i 표준에서 정의하고 있는 CCM 프로토콜의 효율적인 하드웨어 설계에 대해 기술하였다. 설계된 CCMP 코어는 데이터의 기밀성을 위한 CTR 모드와 사용자 인증과 무결성 검증을 위한 CBC 모드의 동작이 두개의 AES 암호 코어로 병렬

```
**************************************************************
*                      CCMP test mpdu                        *
**************************************************************
* A1      = 0f-d2-e1-28-a5-7c DA      A2 = 50-30-f1-84-44-08 SA*
* A3      = ab-ae-a5-b8-fc-ba BSSID   SC = 0x3380            *
* Key ID = 0                                                 *
* TK      = 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f  *
* PN      = 0xb5039776e70c                                   *
* 802.11 Header   = 08 48 c3 2c 0f d2 e1 28 a5 7c 50 30      *
*                   f1 84 44 08 ab ae a5 b8 fc ba 80 33      *
* Plaintext Data1 = 00112233_44556677_8899aabb_ccddeeff      *
* Plaintext Data2 = 01234567_89abcdef_fedcba98_76543210      *
**************************************************************
*                  CCMP : ENCAPSULATION MODE                 *
**************************************************************
* cipher text1 = f32e8d7a_dad544b2_53e3862e_ab283399         *
* cipher text2 = 1abb5191_5f833b75_b9a3dc8b_d339df87         *
* cipher mic   = c4a9ac16_001b1e31_99e3af4a_3e0f0de9         *
* mic          = a2ef035d_570c0d9c_df7aebf0_87a0f096         *
*                                                            *
*              CCMP CORE ENCAPSULATION DONE                  *
**************************************************************

Select : 0.Enc 1.Dec :
```

그림 12. CCMP 코어의 encapsulation 모드 동작 결과

```
**************************************************************
*                      CCMP test mpdu                        *
**************************************************************
* A1      = 0f-d2-e1-28-a5-7c DA      A2 = 50-30-f1-84-44-08 SA*
* A3      = ab-ae-a5-b8-fc-ba BSSID   SC = 0x3380            *
* Key ID = 0                                                 *
* TK      = 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f  *
* PN      = 0xb5039776e70c                                   *
* 802.11 Header   = 08 48 c3 2c 0f d2 e1 28 a5 7c 50 30      *
*                   f1 84 44 08 ab ae a5 b8 fc ba 80 33      *
* Plaintext Data1 = 00112233_44556677_8899aabb_ccddeeff      *
* Plaintext Data2 = 01234567_89abcdef_fedcba98_76543210      *
**************************************************************
*                  CCMP : DECAPSULATION MODE                 *
**************************************************************
* plain text1   = 00112233_44556677_8899aabb_ccddeeff
* plain text2   = 01234567_89abcdef_fedcba98_76543210
* Decrypted mic = a2ef035d_570c0d9c_df7aebf0_87a0f096
* Computed  mic = a2ef035d_570c0d9c_df7aebf0_87a0f096
*                                                            *
*              CCMP CORE DECAPSULATION DONE                  *
**************************************************************

Select : 0.Enc 1.Dec :
```

그림 13. CCMP 코어의 decapsulation 모드 동작 결과

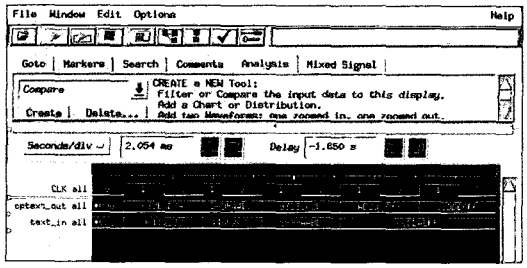


그림 14. 제작된 칩의 테스트 결과

처리 되도록 설계하였다. AES 암호 코어에서 하드웨어 복잡도에 가장 큰 영향을 미치는 S-box를 composite field 연산방식을 적용함으로써 면적의 최적화를 이루었다.

Verilog-HDL로 설계된 CCMP 코어는 ARM922T와 FPGA가 내장되어 있는 Excalibur SoC 장비를 사용한 하드웨어/소프트웨어 통합 검증을 통해 기능을 검증하였다. 0.35-um CMOS MPW 공정으로 칩을 제작하고 테스트한 결과, 모든 기능이 정상 동작함을 확인하였다. 설계된 CCMP 코어는 17,000개의 게이트로 구현되었으며, 최대 116-MHz@3.3-V에서

동작하며 353-Mbps의 성능을 갖는다. 이러한 성능은 IEEE 802.11a와 802.11g에서 정의하고 있는 MAC 성능인 54-Mbps를 충분히 만족한다.

참 고 문 헌

[1] 강유성, 오경희, 정병호, "무선 랜 보안기술의 진화동향 및 전망", *전자통신 동향 분석 제 1 권 제4호* 2003년 8월

[2] 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.

[3] R. Housley, D. Whiting and N. Ferguson, "Counter with CBC-MAC (CCM) : AES Mode of Operation," *Proposed to NIST*, June 2002.

[4] FIPS Publication 197, "Advanced Encryption Standard (AES)," *U.S. Doc/NIST*

[5] 안하기, 신경욱, "AES Rijndael 블록 암호 알고리듬의 효율적인 하드웨어 구현", *한국 정보보호학회 논문지, 제12권2호*, pp.53-64, 2002.

[6] NIST Special Publication 800-38A, "Recommendation for Block Cipher Modes of Operation - Methods and Techniques," *U.S. DoC/NIST*, December 2001.

[7] Draft NIST Special Publicatin 800-38C, "Recommendation for Block Cipher Modes of Operation : the CCM Mode for Authentication and confidentiality," *U.S. Doc/NIST*, May 2004

[8] V. Rijndael, "Eifficient implementation of the Rijndael S-box," *http://www.esat.kuleuven.ac.be/~rijnmen/rijndael/sbox.pdf*

황 석 기(Seok-Ki Hwang) 준회원

2004년 2월 금오공과대학교 전자공학과 졸업

2006년 2월 금오공과대학교 전자공학과 석사

2006년 3월~현재 (주)씨엔에스테크놀로지 반도체 연구소 SoC 3팀 연구원

<관심분야> 정보보호 SoC 설계, 반도체 IP 설계, 비디오 신호처리, 영상 압축

김 종 환(Jong-Whan Kim) 준회원

2005년 2월 금오공과대학교 전자공학과 졸업

2006년 3월~현재 금오공과대학교 전자공학과 석사과정

<관심분야> 정보보호 SoC 설계, 반도체 IP 설계

신 경 욱(Kyung-Wook Shin) 정회원

1984년 2월 한국항공대학교 전자공학과 졸업

1986년 2월 연세대학교 대학원 전자공학과 (공학석사)

1990년 8월 연세대학교 대학원 전자공학과 (공학박사)

1990년 9월~1991년 6월 한국전자통신연구소 반도체연구단 (선임연구원)

1991년 7월~현재 금오공과대학교 전자공학부(교수)

1995년 8월~1996년 7월 University of Illinois at Urbana-Champaign (방문교수)

2003년 1월~2004년 1월 University of California at San Diego (방문교수)

<관심분야> 통신 및 신호처리용 SoC 설계, 네트워크 정보보호 SoC 설계