무선 USB 인증/보안용 프로세서 IP 설계

양현창* · 신경욱*

A Design of Authentication/Security Processor IP for Wireless USB

Hyun-Chang Yang* · Kyung-Wook Shin*

이 논문은 2007년도 IT SoC 핵심설계인력양성사업의 연구결과의 일부입니다.

요 약

무선 USB 시스템의 호스트-디바이스 간에 4-way handshake 상호 인증을 위한 PRF(Pseudo Random Function)-256, PRF-64 및 데이터 암/복호 기능을 수행하는 저면적 고속 인증/보안 프로세서 (WUSB_Sec) IP를 설계하였다. PRF-256과 PRF-64는 CCM(Counter mode with CBC-MAC) 연산을 기반으로 구현되며, CCM은 AES(Advanced Encryption Standard) 암호 코어 2개를 사용하여 CBC 모드와 CTR 모드가 병렬로 처리되도록 설계되었다. WUSB_Sec 프로세서의 핵심 블록인 AES 암호 코어는 합성체 $GF(((2^2)^2)^2)$ 연산 기반의 S-Box로 설계되었으며, SubByte 블록과 키 스케줄러가 S-Box를 공유하도록 설계하여 약 10%의 면적을 감소시켰다. 설계된 WUSB_Sec IP는 약 25,000 게이트로 구현되었으며, 120MHz에서 동작하여 480Mbps의 성능을 갖는다.

ABSTRACT

A small-area and high-speed authentication/security processor (WUSB_Sec) IP is designed, which performs the 4-way handshake protocol for authentication between host and device, and data encryption/decryption of wireless USB system. The PRF-256 and PRF-64 are implemented by CCM (Counter mode with CBC-MAC) operation, and the CCM is designed with two AES (Advanced Encryption Standard) encryption cores working concurrently for parallel processing of CBC mode and CTR mode operations. The AES core that is an essential block of the WUSB_Sec processor is designed by applying composite field arithmetic on $GF(((2^2)^2)^2)$. Also, S-Box sharing between SubByte block and key scheduler block reduces the gate count by 10%. The designed WUSB_Sec processor has 25,000 gates and the estimated throughput rate is about 480Mbps at 120MHz clock frequency.

키워드

Wireless USB, AES, Authentication, Security, CCM, PRF

Ⅰ. 서 론

USB (Universal Serial Bus) 인터페이스는 1996년에 USB1.0 규격이 발표된 이후 2000년에 USB2.0 규격으로 발전하여 PC, 각종 휴대형 단말기, 디지털 가전기기의 인터페이스로 폭넓게 사용되고 있다. USB는 케이블을 이용한 접속형과 USB 메모리 카드와 같은 포트 접속형이 보편적으로 사용되고 있다. 최근, USB 케이블을 사용

* 금오공과대학교 전자공학부

접수일자 2008. 06. 18

하지 않는 무선 USB (Wireless USB) 기술이 개발되고 있으며, 이는 유선 USB의 보안성과 고속의 장점을 무선기술의 편리성에 접목함으로써 모바일 기기 사용자에게 편리한 무선 연결성을 제공한다[1].

무선 USB는 UWB (Ultra Wide Band) 기반의 무선 기술과 USB 기술을 결합한 것으로서, PC 주변기기, 가전기기 및 휴대형 멀티미디어 단말기 등 다양한 분야에 적용될 것으로 기대되고 있다. 특히, 하나의 무선 USB 디바이스를 복수의 PC (또는 사용자)로 공유해서 사용하거나, 복수의 USB 디바이스들을 클러스터로 결합하여 동작시킬 수 있어 기존의 유선 USB2.0에서 제공되지 않는 기능을 구현할 수 있다는 특징을 갖는다. USB 메모리와 같이 PC의 USB 포트 전원으로 동작하는 제품에는 기존의 유선 USB가 계속 사용될 것으로 예상되나, 무선 USB는 프린터, 외장형 하드디스크, MP3, PMP 등 각종 오디오/비디오 기기와 같이 독립 전원으로 동작하는 분야에 폭넓게 사용될 것으로 예상되며, 향후 1 ~ 2년 내에 무선 USB 허브 기능이 탑재된 제품들이 보편화될 것으로 예상된다.

무선 USB는 인텔, 마이크로소프트, HP 등 7개 회사가 주축이 된 Wireless USB Promoter Group에서 표준화를 진행하여 2005년에 무선 USB1.0 규격[2]을 발표하였다. 무선 USB1.0 규격은 USB2.0 규격에 준거하고, 무선 전송 및 접속절차에 관하여 규정하고 있다. 이 규격은 전송거리 3m 이내에서 최대 480Mbps, 10m 이내에서 110Mbps의 전송속도를 제공한다. 무선 USB의 전송기술은 WiMedia Alliance[3]에서 표준화하는 MB-OFDM (Multi-Band Orthogonal Frequency Division Multiplexing) 방식의 UWB 무선 플랫폼[4]을 이용함으로써 안정된 초고속 무선연결을 지원한다. 표 1은 무선접속 규격의 비교를 보이고 있으며, 무선 USB는 무선 랜, 블루투스 등에 비하여 근거리에서 고속 전송의 장점을 갖는다.

표 1. 무선접속 규격의 비교
Table 1. Comparison of wireless access standards

규격 명	Wireless USB1.0	IEEE 802.11g/a	Bluetooth 2.0
주파수 대역 [GHz]	3.1~10.6	2.4/5	2.4
전송속도 [Mbps]	480/110	Max 54	Max 3
통신거리 [m]	3/10	100	1~100

무선 USB는 기존의 USB와 많은 부분을 공유하지만 보안기능이 향상되었다는 측면에서 매우 다르다. 무선 USB는 호스트와 디바이스 사이의 인증되지 않은 엑세스를 차단하기 위하여 상호 인증 시스템을 사용한다. 디바이스가 호스트에 연결을 요청하면 신원확인, 인증, 인가의 3단계 과정을 거쳐 접속을 위한 인증이 이루어진다. 인증이 완료되면 암호 처리부에 의해 데이터가 암호화되어 전송된다. 최근의 IT 기술동향을 고려할 때, 무선 USB용 솔루션은 RF와 베이스밴드가 단일 칩에 집적되는 SoC 형태로 구현될 것으로 예상된다. 특히, 무선 USB의 상호 인증 및 데이터 보안 알고리듬은 소프트웨어 구현 보다는 전용 하드웨어로 구현되어야 하며, 저전력, 고속, 저면적 등이 핵심 요소가 될 것이다.

본 논문에서는 무선 USB 접속인증과 데이터 보안을 위한 보안 프로세서(WUSB_Sec)를 설계하였다. WUSB_Sec의 핵심 블록인 CCM은 2개의 AES 암호코어를 이용하여 CBC 모드와 CTR 모드를 병렬로 구현하였다. CCM의 핵심 블록인 AES 암호 코어는 S-Box를 합성체 $GF(((2^2)^2)^2)$ 연산 기반으로 설계하고, SubByte 블록과 키 스케줄러가 S-Box를 공유하도록 설계하여 최소화된 면적으로 구현하였다.

Ⅱ. 무선 USB 보안 프로토콜

무선 USB의 호스트와 디바이스가 무선 환경에서 접속되기 위해서는 상호 간에 정당한 사용자임을 입증하는 인증과정이 선행되어야 한다. 무선 USB1.0 표준에서는 표 2와 같은 4-way handshake[2] 프로토콜을 통해 호스트-디바이스 간의 상호인증과정을 수행하도록 규정하고 있다.

표 2. 무선 USB 시스템의 상호인증을 위한 4-way handshake 프로토콜
Table 2. 4-way handshake authentication protocol for wireless USB system

Step	Description	
1	4-way handshake 초기화	· Host → Device : TKID, HNonce
2	호스트의 디바이스 인증	· PRF-256, PRF-64 · Device → Host : TKID, DNonce, MIC-D
3	디바이스의 호스트 인증	· PRF-256, PRF-64 · Host → Device : TKID, HNonce, MIC-H
4	인증 완료	· Device → Host : Authentication Complete

그림 1은 무선 USB 시스템의 상호인증을 위한 4-way handshake 프로토콜의 개념도이다. 호스트와 디바이스 간의 인증을 위한 첫번째 단계는 호스트에서 디바이스로 TKID (Temporal Key ID)와 128-bit random nonce인 HNonce (Host Nonce)를 전송함으로써 상호인증을 시작한다.

인증을 위한 두번째 단계에서는 디바이스가 호스트로부터 받은 TKID, HNonce와 HID (Host ID), DID (Device ID), DNonce (Device Nonce), CK (Connection Key)를 자원으로 사용하여 PRF-256 (Pseudo-Random Function)을 실행하여 KCK (Key Confirmation Key)와 PTK (Pairwise Temporal Key)를 생성한다. 생성된 KCK는 상호인증에 사용되는 MIC (Message Integrity Code) 값을 생성하는 PRF-64에 키로 사용되며, PTK는 상호인증 후의 데이터 전송을 위한 암/복호 연산에 키로 사용된다. 디바이스에서 PRF-64에 의해 MIC-D 값이 생성되면 TKID와 DNonce, MIC-D 값이 호스트로 전송된다.

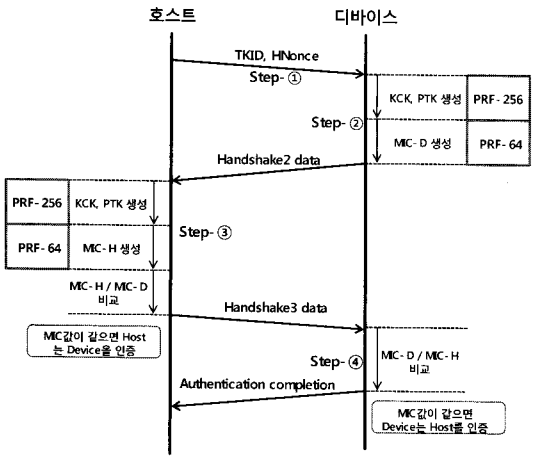

그림 1. 무선 USB 시스템의 4-way handshake 상호 인증 프로토콜
Fig. 1. 4-way handshake authentication protocol for wireless USB system

상호 인증을 위한 세번째 단계는 디바이스로부터 자원을 전송받은 호스트가 동일하게 PRF-256, PRF-64 과정을 수행하여 MIC-H를 생성하고, 디바이스로부터 받은 MIC-D 값과 비교한다. 이 때 두 MIC 값이 동일하면 호스트는 디바이스를 인증하게 되고, 만약 두 MIC 값이 일치하지 않으면 인증이 거부된다. 디바이스에 대한 인증이 성공적으로 이루어졌다면, 호스트가 TKID와 HNonce, MIC-H 값을 다시 디바이스로 전송한다. 인증의 마지막 단계는 디바이스가 호스트로부터 받은 MIC-H 값과 생성된 MIC-D 값을 비교하여 동일한 값을 확인함으로써 호스트를 인증하게 된다. 이와 같은 4 단계 인증절차를 통해 호스트와 디바이스는 상호인증과정을 완료하게 된다. 인증이 완료되면 CCM의 CTR 모드에 의해 데이터가 암호화되어 전송되고, 수신부에서는 암호화된 데이터를 CTR 모드로 복호한다. 상호인증을 위한 PRF-256과 PRF-64는 CCM을 기반으로 구현된다.

III. 하드웨어 설계

II장의 무선 USB 보안 프로토콜에서 설명된 바와 같이, 무선 USB1.0 규격에 제시된 호스트-디바이스 간의 상호인증 프로토콜은 PRF-256과 PRF-64 함수를 기반으로 하며, 이들은 CCM 연산으로 구현된다. 데이터 암호/복호에는 CCM의 CTR 모드가 사용된다.

본 논문에서 설계된 무선 USB 인증/보안 프로세서 WUSB_Sec는 그림 2와 같이 하나의 CCM 코어와 제어 회로로 구성되어 표 3과 같은 4가지 동작모드를 선택적으로 수행한다. 또한, 데이터 복호과정에서 계산된 MIC 값과 수신된 MIC의 복호값을 비교하여 일치 여부를 확인함으로써 데이터의 무결성(integrity)을 검증한다.

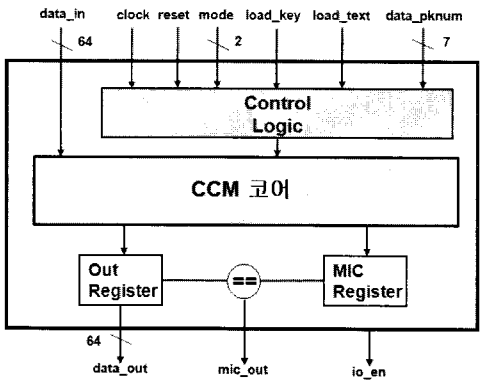

그림 2. WUSB_Sec 프로세서의 블록도
Fig. 2. Block diagram of WUSB_Sec processor

표 3. WUSB_Sec 프로세서의 동작 모드
Table 3. Operation modes of WUSB_Sec processor

동작모드	기능
PRF-256	PRF-64에 사용되는 KCK 생성 암/복호에 사용되는 PTK 생성
PRF-64	상호인증을 위한 MIC 값 생성
CTR 암호	Data 암호
CTR 복호	Data 복호

PRF-256은 그림 3과 같이 4번의 CCM 연산에 의해 32 바이트의 key stream을 생성하며, 이를 위해 TKID, HNonce와 HID (Host ID), DID (Device ID), DNonce (Device Nonce), CK (Connection Key)가 사용된다. PRF-256에 의해 생성된 key stream 중, 상위 16 바이트는 PTK로 사용되고 하위 16 바이트는 KCK로 사용된다. 생성된 PTK는 데이터 암/복호 연산의 키로 사용되며, KCK는 MIC 값을 생성하는 PRF-64에 키로 사용된다. PRF-64는 그림 4와 같이 TKID, HNonce와 HID, DID, DNonce, KCK를 사용하여 1번의 CCM 연산으로 8 바이트의 MIC 값을 생성하며, 이는 호스트와 디바이스 간에 상호인증에 사용된다.

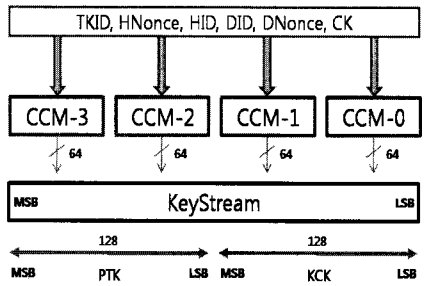

그림 3. PRF-256 연산
Fig. 3. PRF-256 computation

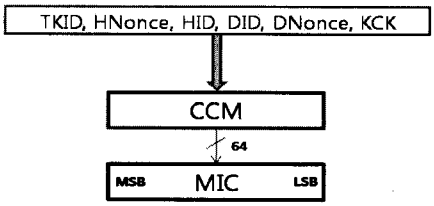

그림 4. PRF-64 연산
Fig. 4. PRF-64 computation

1) CCM 코어

CCM[5,6]은 WUSB_Sec 프로세서의 PRF-256, PRF-64 그리고 데이터 암/복호 기능을 수행하는 핵심 부분이며, CBC (Cipher Block Chaining) 모드를 이용하여 인증을 위한 MIC을 생성하고, CTR 모드를 이용하여 데이터를 암/복호한다. CTR 모드 암호화는 counter 값을 AES 암호 알고리듬으로 암호한 후 평문과 XOR 연산을 통해 암호문을 출력하며, 복호화는 암호연산에 사용된 것과 동일한 counter 값을 AES 암호 알고리듬으로 암호한 후 암호문과 XOR 연산을 통해 평문을 출력한다. 이와 같이 CTR 모드는 AES 암호 연산만을 이용하여 암호/복호화 연산을 수행하므로 하드웨어 구현시 작은 면적으로 구현할 수 있다는 장점을 갖는다. MIC 값을 생성하는 CBC 모드는 초기값 벡터 IV와 입력 평문을 XOR 연산한 후 AES 암호 알고리듬으로 암호화하고, 그 결과 값을 다음 암호연산의 IV로 사용하는 chain 형태의 연산구조를 갖는다.

WUSB_Sec 프로세서에 사용된 CCM 코어는 그림 5와 같은 구조로 설계되었으며, 두 개의 AES 암호 코어를 사용하여 MIC 생성을 위한 CBC 모드와 데이터 암/복호를 위한 CTR 연산이 병렬처리 되도록 하였다. 128 비트의 키 값과 평문(암호문) 블록들은 각각 64 비트씩 순차적으로 입력된다. CBC 블록에서 MIC 값이 생성되는 동안에 CTR 블록에서는 입력된 패킷헤더 정보를 이용하여 counter preload 값을 생성하고 각 평문 블록에 대해 암호화를 수행한다. 또한, CBC 블록에서 생성된 MIC 값은 CTR 블록에서 암호화되어 하나의 패킷에 대한 CCM의 암호화 연산이 완료된다. CCM의 복호연산은 암호연산과 동일한 과정으로 진행되고, 마지막에 CTR 모드에서 MIC을 복호화하여, CBC 연산에 의해 얻어진 MIC 값과의 비교를 통해 무결성을 검증한다.

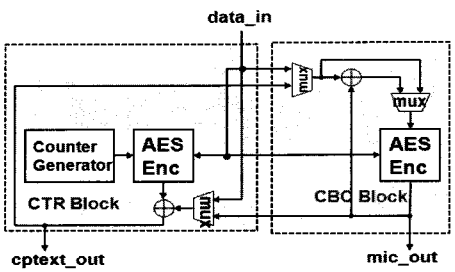

그림 5. CCM 코어의 블록도
Fig. 5. Block diagram of CCM core

2) AES 암호 코어

그림 5의 CCM 코어 내부에 사용된 AES 암호 코어는 블록길이와 키 길이가 모두 128비트이고, 10번의 라운드 연산으로 구성되는 AES 암호 알고리듬[7,8]을 구현한다. AES의 암호연산 과정은 그림 6과 같으며, 초기 라운드 키 가산 후, 9번의 반복 라운드 변환과 최종 라운드 변환의 과정으로 처리된다. 최종 라운드 변환을 제외한 9번의 반복 라운드는 SubByte, ShiftRow, MixColumn, KeyAdd의 연산으로 구성되며, 최종 라운드 변환에는 MixColumn 연산이 제외된다.

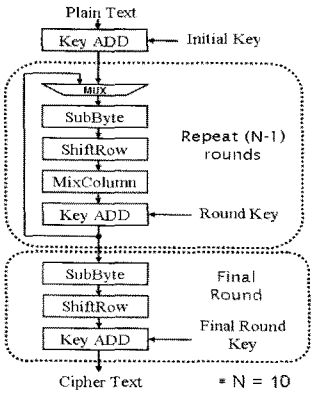

그림 6. AES 암호화
Fig. 6. AES encryption

설계된 AES 암호 코어는 10번의 라운드 변환을 처리하는 라운드변환 블록, 라운드 키 생성기, 제어블록 등으로 구성되며, 그림 7과 같이 설계되었다. 외부와의 인터페이스는 64비트씩 이루어지며, 라운드변환 블록의 데이터 패스를 64 비트로 구현하여 라운드변환이 3클록주기에 처리되도록 하였다.

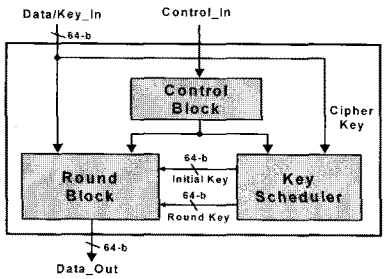

그림 7. AES 암호 코어의 블록도
Fig. 7. Block diagram of AES encryption core

그림 8은 설계된 AES 암호 코어의 동작 타이밍도이다. ldkey_en 신호에 의해 128 비트의 암호키가 2 클록주기 동안 입력되고, ldtext_en 신호에 의해 128 비트의 평문(암호문)이 2 클록주기 동안 입력된다. 그 후, 10번의 라운드 변환에 30 클록주기가 소요된 후, 암호문(평문)이 2 클록주기 동안 출력된다.

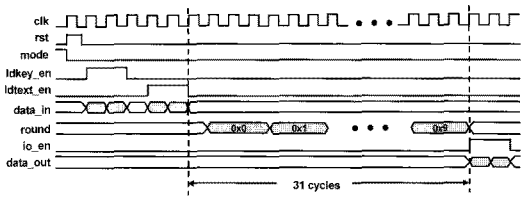

그림 8. AES 암호 코어의 동작 타이밍도
Fig. 8. Timing diagram of AES encryption core

AES 코어는 WUSB_Sec의 동작속도와 전력소모 등 성능에 큰 영향을 미치는 부분이며, 다음과 같은 설계 최적화를 이루었다. AES 코어의 데이터 패스를 64 비트로 구현하는 경우, 그림 9-(a)와 같이 라운드변환 블록에는 8 바이트의 S-Box가 사용되며, 키 생성기에는 4 바이트의 S-Box가 사용된다. 1 바이트의 S-Box는 256 바이트의 LUT (look-up table로 구현되므로, S-Box에 의한 면적이 매우 커지게 된다. 본 논문에서는 그림 9-(b)와 같이 라운드 키 생성기에 별도의 S-Box를 사용하지 않고, 라운드 변환 블록에 사용되는 S-Box를 공유하도록 설계함으로써 4 바이트의 S-Box (즉, 4×256 바이트의 LUT)를 제거하여 면적이 최소화되도록 하였다.

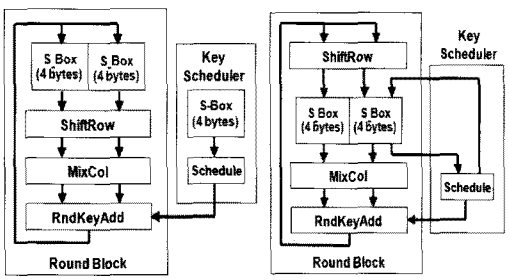

그림 9. S-Box 공유를 이용한 라운드변환 블록의 최적화
Fig. 9. Optimization of round transformation block using S-Box sharing

바이트 단위의 비선형 치환 연산인 SubByte 연산은 AES 코어에서 가장 큰 하드웨어 면적을 차지하는 부분이며, 따라서 설계 최적화를 위한 다양한 고려가 필요하다. SubByte 블록을 구성하는 $GF(2^8)$상의 곱의 역원(multiplicative inverse) 연산을 LUT로 직접 구현하는 경우, 256 바이트 크기의 LUT가 필요하다. 본 논문에서는 체 변환을 이용하여 $GF(2^8)$을 $GF(((2^2)^2)^2)$ 으로 변환[9,10]한 후, $GF((2^2)^2)$ 상의 유한체 곱셈을 통해 회로를 최적화하는 방법을 적용하여 설계하였다.

AES 알고리듬에 사용되는 유한체 (finite field) $GF(2^8)$는 식(1)과 같이 $GF(2)$와 기약다항식(irreducible polynomial) $P_0(x), P_1(x), P_2(x)$를 이용하여 합성체 $GF(((2^2)^2)^2)$로 변환될 수 있다. 식(1)에서 $\phi \in GF(2^2)$와 $\lambda \in GF((2^2)^2)$는 $P_1(x)$, $P_2(x)$가 각각 $GF(2^2)$과 $GF((2^2)^2)$ 상에서 irreducible 조건을 만족한다. 따라서 ϕ, λ는 식(2)에 주어진 16가지 조합 중 하나가 되며, 본 논문에서는 $\phi = \{10\}_2$, $\lambda = \{1100\}_2$을 선택하였다.

$$\begin{cases} GF(2) \Rightarrow GF(2^2), & P_0(x) = x^2 + x + 1 \\ GF(2^2) \Rightarrow GF((2^2)^2), & P_1(x) = x^2 + x + \phi \\ GF((2^2)^2) \Rightarrow GF(((2^2)^2)^2), & P_2(x) = x^2 + x + \lambda \end{cases} \quad (1)$$

$$\begin{array}{lll} \phi = \{10\}_2 & \lambda = \{1000\}_2, & \lambda = \{1100\}_2 \\ \phi = \{11\}_2 & \lambda = \{1001\}_2, & \lambda = \{1101\}_2 \\ & \lambda = \{1010\}_2, & \lambda = \{1110\}_2 \\ & \lambda = \{1011\}_2, & \lambda = \{1111\}_2 \end{array} \quad (2)$$

$GF((2^4)^2)$상의 원소를 $(P_H \mathrm{x} + \mathrm{P_L})$로 표현하면 (단, $P_H, P_L \in GF(2^4)$) x가 $P_2(x)$의 근일 때, 확장 유클리디언 알고리듬에 의해 $GF((2^4)^2)$상의 곱의 역원은 식(3)과 같이 표현된다.

$$\begin{aligned} [P_H \mathrm{x} + \mathrm{P_L}]^{-1} = \mathrm{P_H}\,[\mathrm{P_H^2}\,\lambda + (\mathrm{P_H} + \mathrm{P_L})\mathrm{P_L}\,]^{-1}\,\mathrm{x} \\ + (P_H + P_L)\,[P_H^2\,\lambda + (P_H + P_L)\,P_L\,]^{-1} \end{aligned} \quad (3)$$

따라서 $GF(2^8)$ 상의 곱의 역원은 식(3)에 의해 합성체 $GF(((2^2)^2)^2)$를 이용하여 그림 10과 같이 구현하였다.

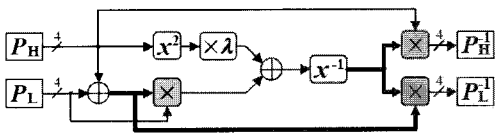

그림 10. $GF(((2^2)^2)^2)$를 이용한 곱의 역원 회로
Fig. 10. Multiplicative inverse block using $GF(((2^2)^2)^2)$

Ⅳ. 설계검증 및 성능평가

WUSB_Sec 프로세서는 Verilog HDL로 설계되었으며, ModelSim을 이용하여 기능을 검증하였다. 그림 11은 CCM 블록에 사용된 AES 암호 코어의 기능검증 결과이다. 암호 키 "00010203 04050607 08090a0b 0c0d0e0f"를 사용하여 평문 "00112233 44556677 8899aabb ccddeeff"를 암호화한 결과, 암호문 "69c4e0d8 6a7b0430 d8cdb780 70b4c55a"가 출력되었으며, 기존에 설계된 AES 암호/복호코어[8]와 동일한 값이 출력되어 설계된 AES 암호 코어가 정상동작 함을 확인하였다.

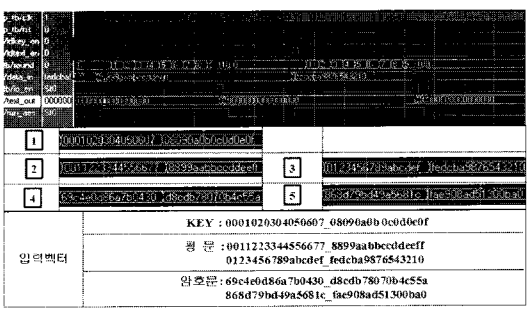

그림 11. 설계된 AES 암호코어의 기능검증 결과
Fig. 11. Functional simulation result of the AES encryption core

그림 12는 WUSB_Sec 프로세서를 구성하는 CCM 코어의 기능검증 결과이다. 입력 평문에 대한 암호연산을 통해 암호문이 얻어지고, 암호문을 다시 복호연산의 입력으로 사용하여 복호한 결과가 암호연산에 사용된 평문과 동일함을 확인하였다. 또한, 생성된 MIC 값과 복호된 MIC 값이 동일함을 확인하여 논리기능이 정상적으로 동작함을 확인하였다.

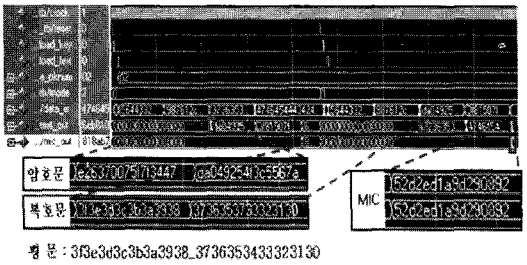

그림 12. CCM 코어의 기능검증 결과
Fig. 12. Functional simulation result of the CCM core

그림 13은 WUSB_Sec 프로세서의 PRF-256과 PRF-64에 대한 기능검증 결과이다. mode=2인 경우에 PRF-256이 수행되어 4번의 CCM 연산을 통해 32 바이트의 암호화된 MIC 값이 출력되고, mode=3인 경우에는 1개의 MIC 값이 정상적으로 출력됨을 확인하였다.

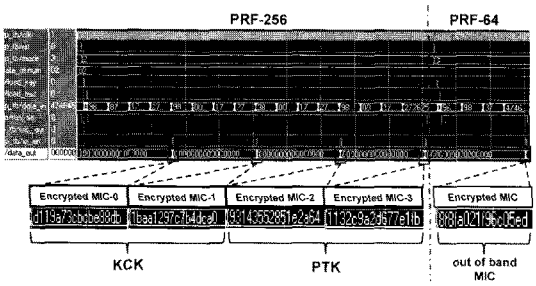

그림 13. PRF-256, PRF-64 연산의 기능검증 결과
Fig. 13. Functional simulation result of the PRF-256 and PRF-64 computations

검증이 완료된 HDL 모델을 0.35㎛ 셀 라이브러리를 이용하여 합성한 결과, 약 25,000 게이트로 구현되었다. 또한 타이밍분석 결과, 설계된 WUSB_Sec 프로세서의 최대 지연시간은 8.3ns로 나타나 120MHz로 동작 가능하며, 480Mbps의 성능을 갖는 것으로 평가되었다. 합성 후 표준셀 라이브러리를 이용하여 Auto P&R을 수행하여 레이아웃을 설계하였으며, 그림 14는 레이아웃 도면이다. 코어부분의 면적은 약 1.5×1.5㎟이고, 코어 이용률은 약 76%로 나타났다. 표 4는 설계된 WUSB_Sec 프로세서의 특성을 요약한 것이다.

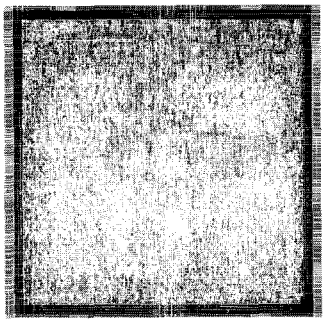

그림 14. WUSB_Sec 프로세서의 레이아웃 도면
Fig. 14. Layout of the WUSB_Sec processor

표 4. WUSB_Sec 프로세서의 특성
Table 4. Summary of the WUSB_Sec processor

구분	성능
게이트 수	25,000
동작 주파수	120MHz @3.3V
동작 성능	480Mbps
동작 모드	PRF-256, PRF-64 데이터 암호/복호
공정	0.35um CMOS
코어 사이즈	1.5x1.5 ㎟
코어 사용률	76%

V. 결 론

본 논문에서는 무선 USB1.0 규격에 정의된 호스트와 디바이스간의 상호 인증과 데이터의 암/복호를 수행하는 WUSB_ Sec 프로세서의 효율적인 하드웨어 설계에 대하여 기술하였다. 설계된 WUSB_Sec 프로세서는 AES 암호연산 코어 2개로 병렬처리 되도록 설계하였으며, AES 암호 코어에서 하드웨어 복잡도에 가장 큰 영향을 미치는 S-Box를 합성체 연산방식을 적용함과 아울러 라운드 변환블록과 키 생성기의 S-Box가 공유되도록 설계함으로써 면적의 최적화를 이루었다. 설계된 WUSB_Sec 프로세서는 120MHz 동작주파수에서 480Mbps의 성능을 가질 것으로 예상되어 무선 USB1.0 규격을 만족하며, 따라서 무선 USB 허브 및 디바이스용 SoC 설계에 보안 IP로 사용될 수 있을 것이다

참고문헌

[1] 이현정, 김종원, 허재두, "무선 USB 표준 및 기술동향", 주간기술동향 1204호, 정보통신연구진흥원, 2005. 7.

[2] Wireless Universal Serial Bus Specification Revision 1.0, May 12, 2005.

[3] WiMedia Alliance, http://www.wimedia.org/

[4] UWB Forum, http://www.uwbforum.org/

[5] NIST Special Publication 800-38C, "Recommendation for Block Cipher Modes of Operation : The CCM Mode for Authen- tication and Confidentiality", May 2004.

[6] 황석기, 김종환, 신경욱, "IEEE 802.11i 무선 랜 보안을 위한 AES 기반 CCMP 코어 설계", 한국통신학회 논문지, 제31권 제6A호, pp. 640-647, 2004.

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

[8] 안하기, 신경욱, "AES Rijndael 블록 암호 알고리듬의 효율적인 하드웨어 구현", 한국 정보보호학회 논문지, 제12권 2호, pp. 53- 64, 2002.

[9] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-box optimization", *Proc. ASIACRYPT 2001,* pp. 239-254, Dec. 2001.

[10] X. Zhang, K. K. Parhi, "High-Speed VLSI Architectures for the AES Algorithm", *IEEE Trans. Systems.,* VOL. 12, No. 9, Sep 2004.

※ 반도체설계교육센터(IDEC)의 CAD Tool 지원에 감사드립니다.

저자소개

양현창(Hyun-Chang Yang)

2006년 금오공과대학교 전자공학부 졸업 (공학사)
2008년 8월 금오공과대학교 대학원 전자공학과 졸업(공학석사)
2008년 9월 ~ 현재 (주)엠텍비전
※관심분야 : 암호 알고리듬, 시스템 및 네트워크 보안, 영상처리

신경욱(Kyung-Wook Shin)

1984년 2월 한국항공대학교 전자공학과(공학사)
1986년 2월 연세대학교 대학원 전자공학과(공학석사)
1990년 8월 연세대학교 대학원 (공학박사)
1990년 9월 ~ 1991년 6월 한국전자통신연구소 반도체 연구단(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, 정보보호 SoC 설계, 반도체 IP 설계