JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 7 : 1296~1302 Jul. 2016

IoT 응용을 위한 초경량 블록 암호 알고리듬 PRESENT의 하드웨어 설계

조욱래 · 김기쁨 · 신경욱*

A Hardware Design of Ultra-Lightweight Block Cipher Algorithm PRESENT for IoT Applications

Wook-Lae Cho · Ki-Bbeum Kim · Kyung-Wook Shin*

School of Electronic Engineering, Kumoh National Institude of Technology, Gumi, Kyungbuk 39177, Korea

요 약

경량 암호기술 표준인 ISO/IEC 29192-2에서 블록암호 표준으로 지정된 초경량 블록암호 알고리듬 PRESENT의 하드웨어 구현에 대해 기술한다. 암호 전용 코어와 암호/복호 기능을 갖는 두 종류의 PR80 크립토 코어를 80 비트의 마스터키를 지원하도록 설계하였다. 설계된 PR80 크립토 코어는 블록암호의 기본 ECB (electronic code book) 운영 모드를 수행하며, 마스터키 재입력 없이 평문/암호문 블록들을 연속적으로 처리할 수 있도록 설계되었다. PR80 크립토 코어는 Verilog HDL을 사용하여 소프트 IP로 설계되었으며, Virtex5 FPGA에 구현하여 정상 동작함을 확인하였다. 설계된 코어를 0.18㎛ 공정의 CMOS 셀 라이브러리로 합성한 결과, 암호 전용 코어와 암호/복호 코어는 각각 2,990 GE와 3,687 GE로 구현되어 적은 게이트를 필요로 하는 IoT 보안 응용분야에 적합하다. 암호 전용 코어와 암호/복호 코어의 최대 동작 주파수는 각각 500 MHz와 444 MHz로 평가되었다.

ABSTRACT

A hardware implementation of ultra-lightweight block cipher algorithm PRESENT that was specified as a block cipher standard for lightweight cryptography ISO/IEC 29192-2 is described in this paper. Two types of crypto-core that support master key size of 80-bit are designed, one is for encryption-only function, and the other is for encryption and decryption functions. The designed PR80 crypto-cores implement the basic cipher mode of operation ECB (electronic code book), and it can process consecutive blocks of plaintext/ciphertext without reloading master key. The PR80 crypto-cores were designed in soft IP with Verilog HDL, and they were verified using Virtex5 FPGA device. The synthesis results using 0.18㎛ CMOS cell library show that the encryption-only core has 2,990 GE and the encryption/decryption core has 3,687 GE, so they are very suitable for IoT security applications requiring small gate count. The estimated maximum clock frequency is 500 MHz for the encryption-only core and 444 MHz for the encryption/decryption core.

키워드 : 경량 블록암호, PRESENT, IoT 보안, 정보보안, 대칭키 암호

Key word : Lightweight Block Cipher, PRESENT, IoT Security, Information Security, Symmetric Key Encryption

Received 30 March 2016, **Revised** 05 April 2016, **Accepted** 21 April 2016

* **Corresponding Author** Kyung-Wook Shin(E-mail:kwshin@kumoh.ac.kr Tel:+82-54-478-7427)
School of Electronic Engineering, Kumoh National Institute of Technology, Gumi 39177, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.7.1296 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

다양한 기기들이 인터넷에 연결되어 다양한 정보가 교환, 공유 및 처리되는 사물인터넷(Internet of Things; IoT) 기술에 의해 기존에 존재하지 않던 새로운 서비스가 창출되고 있으며, 사물인터넷은 정보화 사회의 고도화를 실현하는 핵심 기반기술로 자리 잡아 가고 있다. 무선망으로 연결된 다수의 센서 노드와 단말기들 간에 다양한 형태의 데이터가 수집되어 처리되고, 전송 및 공유되는 IoT 기술의 특성상 여러 가지 보안위험에 노출될 수 있다. 예를 들어, IoT 서비스를 통해 유통되는 데이터에 개인 정보가 포함될 수 있으며, 암호화되지 않은 상태로 유통될 경우 악의적인 공격자에 의한 정보 유출 및 조작이 이루어져 심각한 보안 위협이 발생할 수 있다. IoT의 보안 위협은 애플리케이션, 네트워크, 단말 등 전체 구성요소에 걸쳐 발생할 수 있으며, 서버와 단말에 대한 불법적인 접근을 통한 가용성 침해, 정보의 조작 및 탈취를 통한 기밀성/무결성 공격, 프라이버시 침해 등이 대표적인 보안 위협이다[1-3].

IoT 보안은 기존의 유무선 인터넷 보안과 유사하게 대칭키 블록암호 방식과 공개키 암호 방식을 기반으로 한다. 센서 네트워크, RFID 태크와 같이 제한된 자원을 사용하는 IoT 환경에서는 저전력 소모와 작은 하드웨어 구현이 중요하며, AES[4], SEED[5], ARIA[6] 등 기존의 블록암호 알고리즘은 IoT 보안에 적합하지 않은 것으로 평가되고 있다. 2000년대 중반부터 센서 네트워크와 IoT 보안에 적합한 경량 암호기술(lightweight cryptography)에 대한 연구가 활발하게 진행되어 왔으며, HIGHT[7], PRESENT[8], KATAN/KTANTAN[9], CLEFIA[10] 등 다양한 경량 블록암호 알고리듬들이 제안되었다. 또한, 국제표준화기구인 ISO(International Organization for Standardization)와 IEC(International Electrotechnical Commission)에서는 경량 암호기술 표준을 ISO/IEC 29192로 규정하였으며, ISO/IEC 29192 part-2는 제한된 자원을 갖는 IoT 환경에 적합한 경량 블록암호 알고리즘으로 PRESENT와 CLEFIA를 규정하고 있다[11].

암호화는 컴퓨터에 저장되거나 또는 네트워크를 통해 전달되는 정보를 제 삼자가 가로채어 내용을 노출시키거나 의도적으로 조작하는 보안 공격으로부터 정보를 보호하기 위한 수단으로 사용되며, IoT 시스템을 구현하는 핵심 기술 요소 중 하나로 평가되고 있다. 보안 알고리듬은 소프트웨어 또는 하드웨어로 구현되며, 물리적인 안전성과 저전력 소모가 중요한 시스템에서는 전용 하드웨어 구현 방식이 사용된다. 최근에는 IoT, 스마트카드, NFC 보안을 위한 저전력·저면적 하드웨어 구현 결과들이 발표되고 있다[12-16].

본 논문에서는 독일 보훔루르 대학에서 개발한 64 비트 블록 암호 알고리듬 PRESENT를 IoT 환경에 적합하도록 경량화하여 설계하고, FPGA 구현을 통해 하드웨어 동작을 검증하였다. Ⅱ장에서는 PRESENT 블록암호 알고리듬에 대해 설명하고, Ⅲ장에서는 80 비트 마스터키 길이를 지원하는 PRESENT-80 암호 코어와 암호/복호 코어의 구현에 대해 설명한다. 설계된 회로의 기능 검증 및 FPGA 구현에 대해 Ⅳ장에서 기술하며, Ⅴ장에서 결론을 맺는다.

Ⅱ. PRESENT 블록암호 알고리듬[8]

2012년 2월에 ISO/IEC에 의해 국제표준으로 등록된 PRESENT 알고리듬은 64 비트의 평문/암호문 블록을 마스터키(80 비트 또는 128 비트)로 암호화/복호화하여 64 비트의 암호문/평문을 생성하는 대칭키(비밀키) 방식의 블록암호이다. PRESENT는 SPN (substitution and permutation) 구조를 기반으로 31번의 라운드 변환을 통해 평문/암호문을 출력한다. PRESENT의 암·복호화 과정은 그림 1과 같으며, 암호화 과정의 라운드 변환은

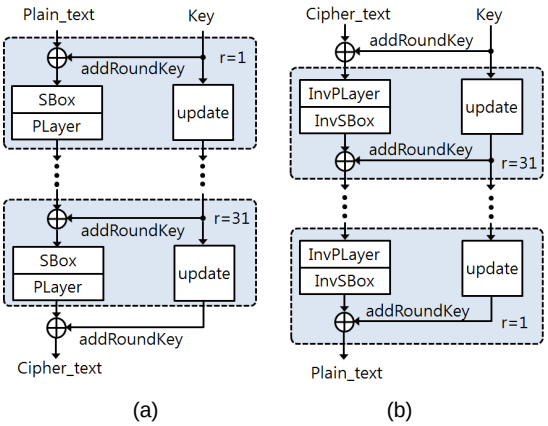


Fig. 1 Block cipher PRESENT algorithm (a) encryption, (b) decryption

그림 1 (a)와 같이 라운드키 가산(addRoundKey), 4 비트 비선형 변환를 수행하는 SBox, 64 비트의 치환를 수행하는 PLayer로 구성된다. 복호화 과정은 그림 1 (b)와 같이 암호화 과정의 역순으로 이루어지며, 라운드키도 역순으로 사용된다. 또한 SBox 역변환을 위한 InvSBox와 비트 역치환을 위한 InvPLayer가 사용된다. 암호·복호화 과정에서 매 라운드 마다 사용되는 라운드키는 마스터키로부터 키 스케줄러에 의해 생성된다.

Ⅲ. PR80 암호/복호 코어 설계

80 비트 마스터키 길이를 지원하는 PRESENT-80 알고리듬을 암호화 기능만 갖는 암호전용 코어(PR80_Enc32b)와 암호화/복호화 기능을 갖는 코어(PR80_EnDe32b)를 설계하였다. 암호 전용 코어는 RFID나 센서 노드와 같이 암호 연산만 사용되는 응용분야에 적합하도록 하드웨어를 최소화하여 설계하였다.

PR80 코어의 블록도는 그림 2와 같으며, 라운드 블록, 키 스케줄러, 제어 블록으로 구성된다. 암호 전용 코어인 PR80_Enc32b는 라운드 블록과 키 스케줄러를 암호화 연산에 필요한 회로만으로 구성하여 게이트 수를 최소화하였다. 키 스케줄러는 라운드 블록 데이터패스와 동일한 비트수의 라운드키를 생성하여 라운드 블록에 공급한다. 마스터키와 평문/암호문은 16 비트의 입출력 포트를 통해 시분할 방식으로 입력된다.

3.1. PR80 암호 전용 코어

암호 전용 코어인 PR80_Enc32b는 64 비트의 평문을 80 비트 마스터키로 암호화하여 64 비트의 암호문을 생성한다. 라운드 블록은 64 비트의 평문 블록을 32 비트 단위로 나누어 처리되도록 32 비트 데이터패스로 설계되었으며, 키 스케줄러는 32 비트의 서브 라운드키를 생성하여 라운드 블록에 공급한다. 한 라운드 연산이 3 클록 주기에 처리되며, 64 비트 평문 블록의 암호화에 총 96 클록 주기가 소요된다.

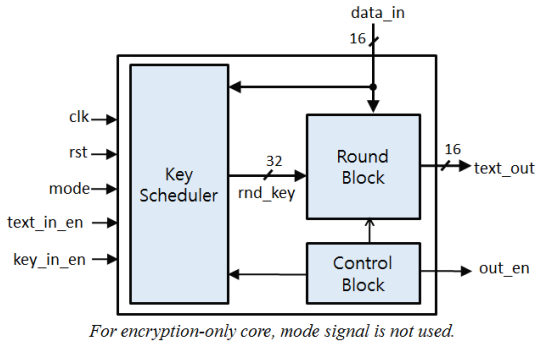


Fig. 2 Block diagram of PR80 crypto-core

라운드 블록은 그림 3 (a)와 같으며, 중간 결과를 저장하는 64 비트의 상태 레지스터(state_reg), 비선형 변환을 수행하는 4 비트 SBox 8개(SBox_32), 64 비트 치환을 수행하는 PLayer(PLayer_64), 그리고 라운드키 가산을 위한 32 비트 XOR 게이트 등으로 구성된다. 라운드키 가산과 SBox 연산은 32 비트 단위로 처리되어 2 클록 주기가 소요되며, PLayer 연산은 치환 특성을 고려하여 64 비트가 한 클록에 처리되도록 설계하였다.

키 스케줄러는 그림 3 (b)와 같으며, 두 개의 80 비트 키 레지스터, 4 비트 SBox(SBox_4), 순환이동 회로, 라운드 상수 가산을 위한 XOR 게이트 등으로 구성된다. key_state_reg는 라운드키 생성을 위한 중간키 값을 저장하는 레지스터이고, master_key_reg는 동일한 마스터키가 연속되는 평문 블록에 적용될 수 있도록 마스터키를 저장한다. key_in_en 신호에 의해 새로운 마스터키가 입력될 때까지 master_key_reg에 저장된 키가 암호화 연산에 반복적으로 사용되며, 매 평문 블록마다 마

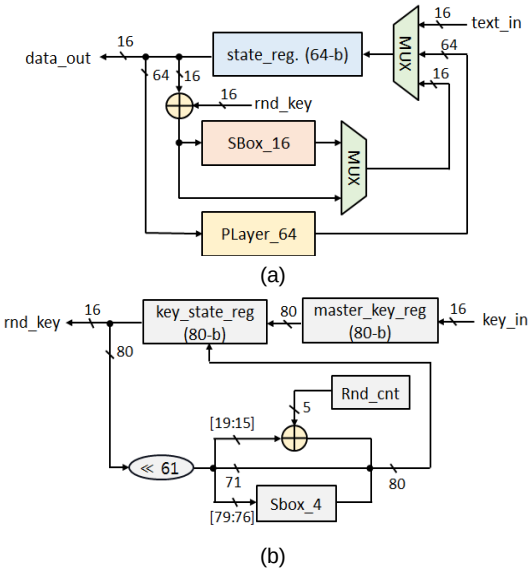


Fig. 3 Encryption-only core with 32-bit datapath (a) round block (b) key scheduler

스터키를 입력하지 않아도 되는 장점을 갖는다.

key_state_reg에 저장된 80 비트의 중간키 값에서 하위 16 비트를 제외한 상위 64 비트가 상위비트 쪽부터 순차적으로 2 클록 주기에 걸쳐 라운드키로 출력된다. 라운드키 출력이 완료된 후, 다음 라운드를 위한 중간키 업데이트에 1 클록 주기가 소요된다. key_state_reg에 저장된 중간키 값을 61 비트 좌측 순환이동시킨 결과로부터 상위 4 비트에 대한 SBox 연산 결과, 라운드 상수와 5 비트 중간키 값 [19:15]의 XOR 연산 결과, 그리고 나머지 71 비트가 key_state_reg에 저장되어 다음 라운드의 라운드키로 출력된다.

3.2. PR80 암호/복호 코어

PR80 암호/복호 코어(PR80_EnDe32b)는 64 비트의 평문/암호문을 80 비트 마스터키로 암호/복호화하여 64 비트의 암호문/평문을 생성한다. 64 비트의 평문/암호문 블록이 32 비트씩 나누어 처리되도록 데이터패스를 32 비트로 설계하였다. 키 스케줄러는 32 비트의 서브 라운드키를 생성하여 라운드 블록에 공급한다. 한 라운드 변환이 3 클록 주기에 처리되며, 64 비트 평문/암호문 블록의 암호/복호화에 총 96 클록 주기가 소요된다.

라운드 블록은 그림 4 (a)와 같이 설계되었으며, 라운드 연산의 중간결과를 저장하는 64 비트의 상태 레지스터(state_reg), 비선형 변환을 수행하는 4 비트 SBox 8개(SBox_32)와 그 역변환을 수행하는 InvSBox 8개(InvSBox_32), 64 비트 치환을 수행하는 PLayer (PLayer_64)와 그 역변환을 수행하는 InvPLayer (InvPLayer_64), 라운드키 가산을 위한 32 비트 XOR 게이트 등으로 구성된다. 라운드키 가산과 SBox 연산은 32 비트씩 처리되어 2 클록 주기가 소요되며, PLayer 연산은 치환 특성을 고려하여 64 비트가 한 클록에 처리되어 한 라운드 변환에 3 클록 주기가 소요된다.

암호화를 위한 라운드 변환 과정은 PR80_Enc32b 코어의 동작과 동일하다. 복호화 모드에서는 InvSBox 연산과 라운드키 가산이 32 비트 단위로 2 클록 주기 동안 처리된 후, 상태 레지스터에 저장된 64 비트에 대해 InvPLayer 연산이 한 클록에 처리되어 한 라운드 변환에 3 클록 주기가 소요된다.

키 스케줄러는 그림 4 (b)와 같은 구조로 설계되었으며, 두 개의 80 비트 키 레지스터, 4 비트 SBox와 InvSBox, 순환이동 회로, 라운드 상수 가산을 위한

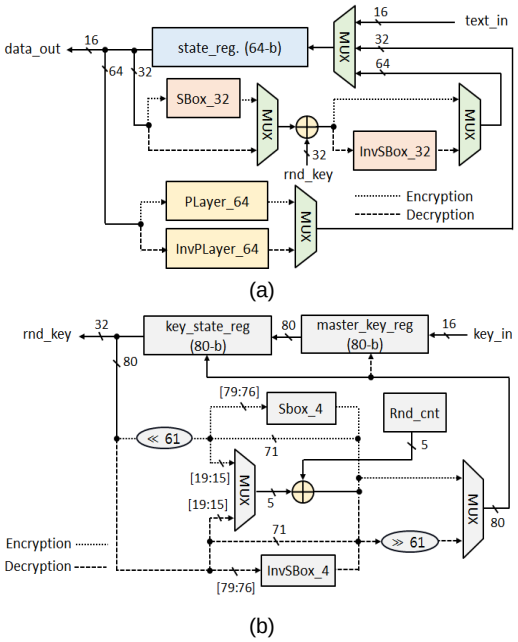


Fig. 4 Encryption/decryption core with 32-bit datapath (a) round block (b) key scheduler

XOR 게이트로 구성된다. key_state_reg에 저장된 80 비트 중간키 값에서 하위 16 비트를 제외한 상위 64 비트가 상위비트 쪽부터 순차적으로 2 클록 주기에 걸쳐 라운드키로 출력된다. 라운드키 출력이 완료된 후, 다음 라운드를 위한 키 업데이트에 1 클록 주기가 소요된다.

암호화를 위한 라운드키 업데이트 과정은 암호 전용 코어인 PR80_Enc32b의 동작과 동일하다. 복호화를 위한 라운드키 업데이트 과정은 1 클록 주기에 걸쳐 진행된다. key_state_reg에 저장된 중간키 값의 상위 4 비트에 대한 InvSBox 연산 결과, 라운드 상수와 5 비트 중간키 값 [19:15]의 XOR 연산 결과, 그리고 나머지 71 비트로 구성되는 80 비트를 61 비트 우측 순환 이동시킨 결과가 key_state_reg에 저장되어 다음 라운드의 라운드키로 출력된다.

Ⅳ. 기능검증 및 FPGA 구현

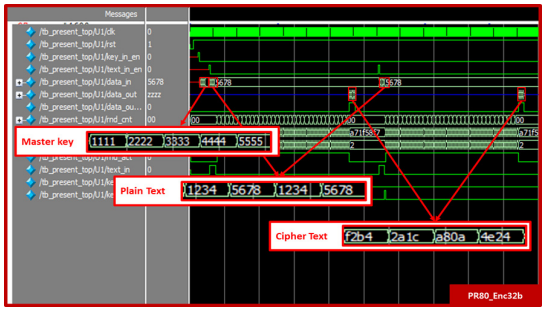
설계된 PR80_Enc32b 코어와 PR80_EnDe32b 코어의 기능검증 결과는 그림 5와 같다. 64 비트의 평문 “1234 5678 1234 5678”와 80 비트의 마스터키 “1111

2222 3333 4444 5555”를 사용한 시뮬레이션 결과를 보이고 있다. 암호화 결과로 암호문 “f2b4 2a1c a80a 4e24”이 출력되었고, 이를 다시 복호화하여 평문 “1234 5678 1234 5678”이 출력됨을 확인할 수 있다.

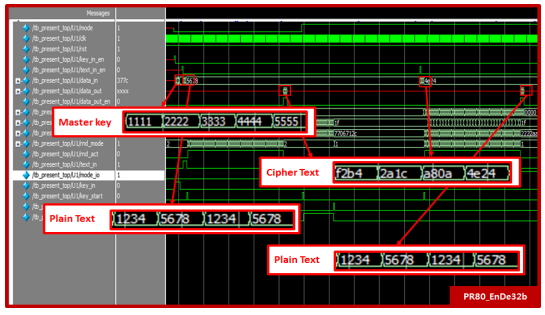
기능검증이 완료된 PR80 코어는 FPGA 구현을 통해 하드웨어 동작을 검증하였다. 그림 6 (a)는 FPGA 보드, UART 인터페이스, 구동 소프트웨어로 구성된 검증시스템 구성도이며, Virtex5 XC5VSX-95T FPGA 디바이스가 사용되었다. FPGA에는 UART와 래퍼(wrapper) 모듈 그리고 PR80 코어가 구현되었으며, PC와 FPGA 사이의 데이터 송수신은 RS232C를 통해 이루어진다. PC에서 FPGA로 전송된 평문/암호문 데이터는 래퍼를 통해 16 비트씩 PR80 코어로 입력되고, 64 비트 블록 단위로 암호화/복호화가 이루어진다. PR80 코어에서 출력되는 암호문/평문은 래퍼에 저장되었다가 UART 통신을 통해 PC로 전송되어 화면에 표시된다.

그림 6 (b)는 FPGA 검증 결과를 보이고 있다. GUI 프로그램을 통해 PR80 코어의 암호화/복호화 결과가 화면에 표시된다. 그림 6 (b)에서 좌측의 원본 이미지를 FPGA로 전송하여 PR80 코어에서 암호화한 결과는 중앙의 이미지와 같으며, 원본 이미지의 내용을 알아볼 수 없도록 랜덤값으로 암호화되었음을 확인할 수 있다. 암호화된 이미지를 다시 FPGA로 전송하여 복호화한 결과는 우측의 이미지와 같으며, 암호화에 사용된 원본 이미지가 복원되었음을 확인할 수 있다. 그림 6 (b)에서 보는 바와 같이, 이미지를 암호화하고 암호화된 이미지를 복호하여 원래 이미지와 일치하는 결과가 출력됨으로써 FPGA에 구현된 PR80 코어가 올바르게 동작함을 확인하였다.

기능 검증이 완료된 PR80 코어를 0.18㎛ CMOS 셀 라이브러리로 논리합성을 하였다. 100 kHz의 동작 주파수에서 PR80_Enc32b 코어와 PR80_EnDe32b 코어는 각각 2,990 GE와 3,687 GE로 구현이 되었으며, 최대 동작 주파수는 각각 500 MHz와 444 MHz로 예측되었다.

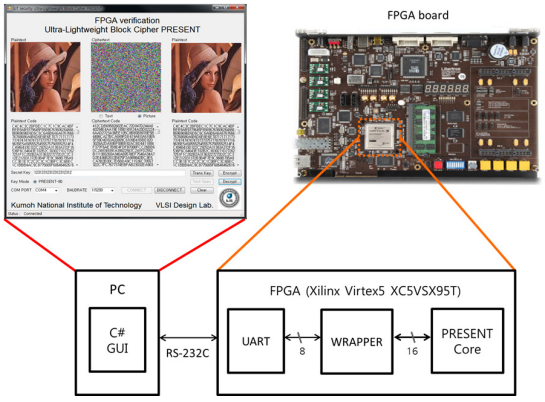


(a)

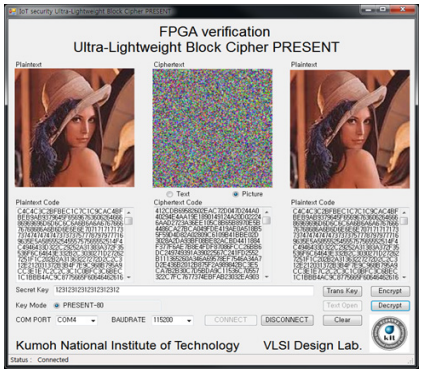


(b)

Fig. 5 Simulation results of PR80 core (a) PR80_Enc32b core (b) PR80_EnDe32b core



(a)



(b)

Fig. 6 FPGA verification result of PR80 core (a) FPGA verification system (b) verification result

Table. 1 Comparison of PRESENT crypto-cores

cores	Key size [bits]	enc/dec	# of cycles	Max Freq. [MHz]	@Max Freq.		@100 kHz	
					Throughput [Mbps]	Area [GE]	Throughput [Mbps]	Area [GE]
PR80_Enc_32b	80	enc	96	500	320	3,878	0.064	2,990
PR80_EnDe_32b	80	enc/dec	96	444	284	5,503	0.064	3,687
Ref. [8]	80	enc	32	N/A	N/A	N/A	0.2	1,570
Ref. [15]	80, 128	enc/dec	32	454	908	N/A	0.2	5,740
Ref. [16]	80	enc	32	209	419	N/A	N/A	N/A

표 1은 본 논문의 설계 결과를 문헌에 발표된 사례와 비교한 것이다. 문헌 [8]의 사례는 암호화만 지원하는 코어이고, 블록 크기와 마스터키 길이만큼의 입력 핀을 갖는다. 또한 마스터키 레지스터를 포함하지 않아 새로운 평문/암호문 블록을 처리할 때마다 마스터키가 입력되어야 한다. 반면에 본 논문의 PR80 코어는 입출력 핀 수를 최소화하기 위해 16 비트 포트를 통해 평문/암호문과 마스터키가 시분할 방식으로 입력된다. 또한 내부에 마스터키 레지스터를 포함하고 있어 동일한 마스터키를 사용하여 연속적인 암호화/복호화 동작이 가능하다. 문헌 [15]의 사례는 80 비트와 128 비트의 두 가지 마스터키 길이와 암호화와 복호화를 모두 지원하며, ECB(Electronic CodeBook), OFB(Output Feed-Back), CBC(Cipher Block Chaining), CTR(Counter)의 4가지 운영모드를 제공하는 PRESENT 코어이다. 문헌 [16]은 PRESENT, Piccolo, PRINT, LED의 4가지 블록암호 알고리듬을 단일 플랫폼에 통합하여 구현한 사례이다. 최대 209 MHz의 클록 주파수에서 419 Mbps의 성능을 갖는다. Altera Cyclone IV 디바이스에서 613 Comb LEs와 153 Seq LEs로 구현되었으며, GE(gate equivalent) 값이 제시되지 않아 본 논문의 설계와 직접적으로 비교할 수 없다.

Ⅴ. 결 론

ISO/IEC 국제표준으로 승인된 64 비트 블록암호 알고리듬 PRESENT를 하드웨어로 구현하였다. 32 비트 데이터패스로 설계된 암호 전용 코어(PR80_ Enc32b)와 암호/복호용 코어(PR80_EnDe32b)는 각각 2,990 GE와 3,687 GE의 적은 게이트 수로 구현되었다. 설계된 PRESENT 코어는 하드웨어 경량화와 저전력 특징을 가져 IoT, RFID 환경과 같이 제한된 자원을 갖는 응용분야의 정보보호 하드웨어 코어로 활용이 가능하다.

ACKNOWLEDGMENTS

- This work was supported by Industrial Core Technology Development Program (10049009, Development of Main IPs for IoT and Image-Based Security Low-Power SoC) funded by the Ministry of Trade, Industry & Energy.
- The authors are thankful to IDEC for EDA software support.

REFERENCES

[1] D.H. Kim, S.W Yoon and Y.P. Lee, “Security for IoT Services,” *Information and Communications Magazine,* vol. 30, no. 8, pp. 53-59, Jul. 2013.

[2] C. Lu. Overview of Security and Privacy Issues in the Internet of Things [Internet]. Available: http://www.cse.wustl.edu/ ~jain/cse574-14/ftp/security.pdf

[3] B.I Jang and C.S. Kim, “A study on the security technology for internet of things,” *Journal of Security Engineering*, vol. 11, no. 5, pp. 429-438, 2014.

[4] FIPS-197, Advanced Encryption Standard, National Institute of Standard and Technology(NIST), Nov. 2001.

[5] TTA Std. TTAK.KO-12.0004/R1, 128-bit Block Cipher Algorithm SEED, Korea Internet & Security Agency, 1999.

[6] KS X 1213:2004, 128 bit Block Encryption Algorithm ARIA, Korean Agency for Technology and Standards

(KATS), 2004.
[7] TTA Std. TTAK.KO-12.0040/R1, 64-bit Block Cipher HIGHT, Korea Internet & Security Agency, 2008.
[8] A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," *Cryptographic Hardware and Embedded Systems (CHES 2007),* LNCS, Springer, vol. 4727, pp. 450-466, 2007.
[9] De Canniere, Christophe, Orr Dunkelman, and Miroslav Knežević. "KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers," *Cryptographic Hardware and Embedded Systems (CHES 2009),* Springer, pp. 272-288, 2009.
[10] Sony Corporation. The 128-bit Block Cipher CLEFIA: Algorithm Specification, [Internet]. Available: http://www.sony.net/Products/cryptography/clefia/download/data/clefia-spec-1.0.pdf.
[11] ISO/IEC Std. 29192-2, Information technology - Security techniques-Lightweight cryptography (part2): Block ciphers, International Organization for Standardization (ISO), 2012.
[12] H.W. Park and K.W. Shin, "An efficient hardware implementation of 64-bit block cipher algorithm HIGHT," *Journal of KIICE*, vol. 15, no. 9, pp. 1933-1999, Sep. 2011.
[13] M.J. Sung and K.W. Shin, "An Efficient Hardware Implementation of Lightweight Block Cipher LEA-128/192/256 for IoT Security Applications," *Journal of KIICE*, vol. 19, no. 7, pp. 1608-1616, Jul. 2015.
[14] G.C. Bae and K.W. Shin, "An Efficient Hardware Implementation of Lightweight Block Cipher Algorithm CLEFIA for IoT Security Applications," *Journal of KIICE*, vol. 20, no. 2, pp. 351-358, Feb. 2016.
[15] K.B. Kim, W.L. Cho and K.W. Shin, "A Design of PRESENT Crypto-Processor Supporting ECB/CBC/OFB/CTR Modes of Operation and Key Lengths of 80/128-bit," *Journal of KIICE*, vol. 20, no. 6, pp. 1163-1170, Jun. 2016.
[16] H. Liao and H.M. Heys, "An Integrated Hardware Platform for Four Different Lightweight Block Ciphers," *Proc. of the IEEE 28th Canadian Conference on Electrical and Computer Engineering*, pp. 701-705, May 2015.

조욱래(Wook-Lae Cho)

2016년 2월 금오공과대학교 전자공학부(공학사)
※관심분야 : 통신 및 신호처리용 반도체 IP 설계, 정보보호용 반도체 IP 설계

김기쁨(Ki-Bbeum Kim)

2016년 2월 금오공과대학교 전자공학부(공학사)
※관심분야 : 통신 및 신호처리용 반도체 IP 설계, 정보보호용 반도체 IP 설계

신경욱(Kyung-Wook Shin)

1984년 2월 한국항공대학교 전자공학과(공학사)
1986년 2월 연세대학교대학원 전자공학과(공학석사)
1990년 8월 연세대학교대학원(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)
2013년 2월~2014년 2월 Georgia Institute of Technology(방문교수)
※관심분야 : 통신 및 신호처리용 SoC 설계, 정보보호 SoC 설계, 반도체 IP 설계