4가지 운영모드를 지원하는 초경량 블록암호 PRESENT의 하드웨어 구현

김기쁨* · 조욱래 · 신경욱

*금오공과대학교

A Hardware Implementation of Ultra-Lightweight Block Cipher PRESENT Supporting Four Modes of Operation

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

Kumoh National Institute of Technology

E-mail : kkp@kumoh.ac.kr

요 약

80/128-비트 마스터키 길이와 ECB, CBC, OFB, CTR의 4가지 운영모드를 지원하는 PRESENT 경량 블록암호 프로세서를 설계하고, Virtex5 FPGA에 구현하여 정상 동작함을 확인하였다. PRESENT 크립토 프로세서를 0.18㎛ 공정의 CMOS 셀 라이브러리로 합성한 결과 8,237 GE로 구현되었으며, 최대 434 MHz 클록으로 동작하여 868 Mbps의 성능을 갖는 것으로 예측되었다.

키워드

PRESENT, Ultra-lightweight block cipher, cryptography, IoT security, Mode of Operation

Ⅰ. 서 론

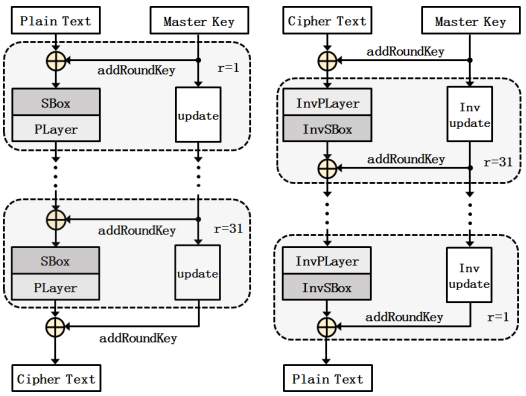
정보통신기술의 지속적인 발전으로 일상생활 환경에서 사물과 인터넷을 통해 다양한 서비스가 제공되는 이른바 사물인터넷(Internet of Things; IoT) 시대로 도약하고 있다. IoT는 인간과 주변 사물과의 상호 연결을 위해 센싱 기술과 각종 유무선 네트워크 기술을 사용하고 있으며, 연결망을 통해 다양한 서비스가 제공된다. 각종 네트워크에 연결된 다량의 센서 노드와 단말기 간에 다양한 데이터가 수집되어 처리되고 전송 및 공유되는 IoT 기술의 특성상 다양한 보안 위험에 노출될 수 있다. IoT 보안을 위해서는 디바이스 간 통신에서 기밀성, 무결성 및 기기 간 인증 측면에서의 보호를 고려해야 한다. 또한 제한된 자원을 갖는 IoT의 특성을 고려하여 저전력 소모와 작은 하드웨어 요구량을 만족하는 알고리듬이 필요하며, 다양한 경량 블록암호들이 제안되고 있다[1].

블록암호의 기본 운영모드인 ECB(Electronic Code Book) 모드는 동일한 값의 평문에 대해 동일한 암호문이 얻어지므로, 보안성이 떨어진다. 이와 같은 문제점을 개선하기 위해 CBC(Cipher Block Chaining), OFB(Output Feed Back), CTR (Counter) 등 여러 가지 운영모드가 사용되며, 운영모드에 따라 블록 간의 의존성과 오류 전파가 평문과 복호문에 미치는 영향이 달라진다[2, 3].

64-비트 블록암호 PRESENT를 80/128-비트의 두 가지 마스터키 길이와 ECB, CBC, OFB, CTR의 4가지 모드를 지원하도록 설계하고, FPGA 구현을 통해 하드웨어 동작을 검증하였다.

Ⅱ. PRESENT 블록암호 알고리듬[4]

PRESENT는 64-비트의 평문/암호문 블록을 80-비트 또는 128-비트의 마스터키로 암호화/복호화하여 64-비트의 암호문/평문을 생성하는 대칭키 방식의 블록암호 알고리듬이다. PRESENT의 암·복호화 과정은 그림 1과 같으며, SPN 구조를 기반으로 하여 31번의 라운드 변환을 갖는다. 암호화 과정의 라운드 변환은 그림 1-(a)와 같이 라운드키를 가산하는 addRoundKey, 비선형 SBox, 비트 치환 PLayer로 구성된다. 복호화 과정은 암호화의 역순으로 이루어지고 라운드키도 역순으로 사용되며, SBox의 역변환을 위한 InvSBox와 비트 역치환을 위한 InvPLayer가 사용된다.



(a) (b)

Fig. 1. Encryption and decryption of PRESENT
(a) encryption, (b) decryption

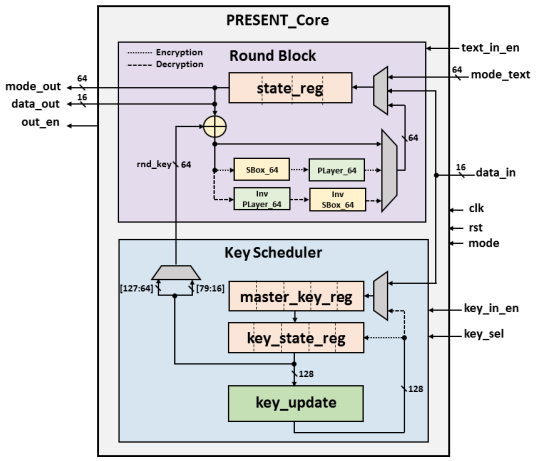


Fig. 3. PRESENT_Core

III. PRESENT 암·복호 코어 설계

설계된 PRESENT 크립토 프로세서의 전체 구조는 그림 2와 같으며, PRESENT_Core, 64-비트 레지스터 iv_reg, 64-비트 레지스터 op_reg, XOR 게이트와 멀티플렉서 그리고 제어블록으로 구성된다. PRESENT_Core가 기본적인 ECB 암호·복호 기능을 수행하며, iv_reg와 op_reg, XOR 게이트 그리고 멀티플렉서에 의해 CBC, OFB, CTR의 운영모드 동작이 수행된다.

PRESENT_Core는 64-비트의 평문(암호문)을 80-비트 또는 128-비트 마스터키로 암호화(복호화)하여 64-비트의 암호문(평문)을 생성하며, 그림 3과 같이 라운드 블록과 키 스케줄러 블록으로 구성된다. 한 라운드 변환이 단일 클록으로 처리되며 64-비트 평문(암호문) 블록의 암호화(복호화)에 총 32 클록이 소요된다. 라운드 블록은 라운드 연산의 중간결과를 저장하는 64-비트 상태 레지스터, 비선형 변환을 수행하는 16개의 4-비트 SBox와 역변환을 수행하는 16개의 InvSBox, 64-비트 치환을 수행하는 PLayer와 그 역변환을 수행하는 InvPLayer, 그리고 라운드키 가산을 위한 XOR 게이트 등으로 구성된다. 키 스케줄러는 80-비트 또는 128-비트의 마스터키를 받아 라운드 변환에 사용되는 라운드키를 생성한다. 마스터키를 저장하는 레지스터와 갱신된 중간키를 저장하는 레지스터 key_state_reg를 가지고 있으며, 순환이동 회로, SBox, XOR 게이트 등으로 구성된다.

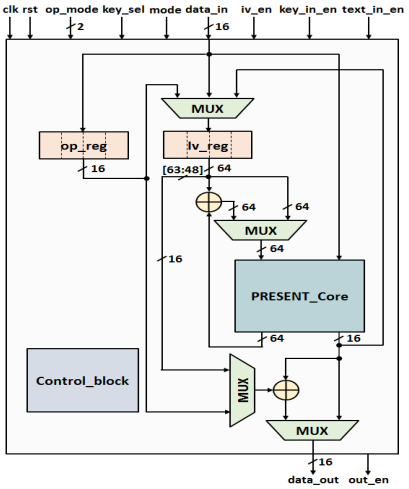


Fig. 2. PRESENT crypto-processor supporting four modes of operation

IV. 기능검증 및 FPGA검증

설계된 PRESENT 크립토 프로세서의 4가지 운영모드 동작을 시뮬레이션으로 검증했으며, 그림 4는 OFB 운영모드 동작의 시뮬레이션 결과이다. 80-비트의 마스터키 “1111 0000 1111 0000 1111”과 IV “1111 2222 3333 4444”를 사용하여 64-비트의 평문 “0000 aaaa 0000 bbbb”와 “1234 5678 1234 5678”을 연속으로 암호화한 결과로 암호문 “3622 d310 63cc f617”, “0a1a 1c0f d0a6 141e”가 출력된다. 암호문을 다시 복호화하면 원래의 평문 “0000 aaaa 0000 bbbb”, “1234 5678 1234 5678”이 출력됨을 확인할 수 있다.

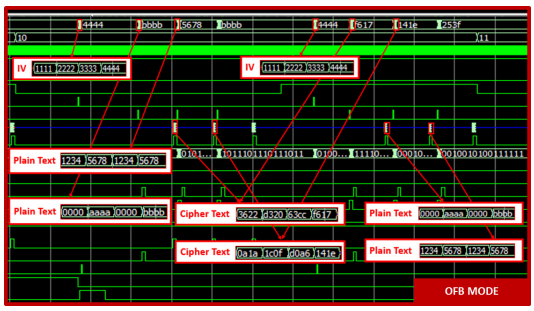
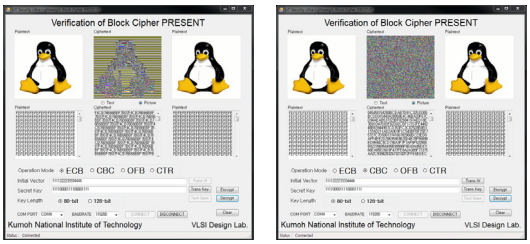


Fig. 4. Simulation results of PRESENT processor



(a) (b)

Fig. 5. FPGA verification result of PRESENT processor (a) ECB mode (b) CBC mode

기능검증이 완료된 PRESENT 크립토 프로세서를 FPGA 디바이스에 구현하여 하드웨어 동작을 검증하였다. 그림 5는 FPGA 검증 결과를 보이고 있으며, GUI 프로그램을 통해 PRESENT 프로세서의 암호화/복호화 결과가 화면에 표시된다. 그림 5-(a),(b)에서 좌측의 원본 이미지를 FPGA로 전송하여 PRESENT 프로세서에서 암호화한 결과는 중앙의 이미지와 같다. 암호화된 이미지를 다시 FPGA로 전송하여 복호화한 결과는 우측의 이미지와 같으며, 암호화에 사용된 원본 이미지가 복원되어 FPGA에 구현된 PRESENT 프로세서가 올바르게 동작함을 확인할 수 있다. 0.18㎛ 표준 셀 라이브러리로 논리합성한 결과, 100 kHz의 동작 주파수에서 8,237 GE로 구현이 되었으며, 최대 동작 주파수는 434 MHz로 예측되었다.

Ⅴ. 결 론

ISO/IEC 국제표준으로 승인된 64-비트 블록암호 알고리듬 PRESENT를 하드웨어로 구현하였다. PRESENT 프로세서는 8,237 GE의 게이트로 구현되어 하드웨어 경량화와 저전력을 특징으로 가져 IoT, RFID 환경과 같이 제한된 자원을 갖는 응용분야의 정보보호 코어로 활용이 가능하다.

ACKNOWLEDGMENTS

- This work was supported by the Industrial Core Technology Development Program (1004 9009, 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.

참고문헌

[1] T. Eisenbarth, "A Survey of Lightweight Cryptography Implementations," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522-533, 2007.

[2] NIST Computer Security Division's (CSD) Security Technology Group (STG), "Block cipher modes," Cryptographic Toolkit, NIST, Apr. 2013.

[3] Dong Hyeon Kim, Kyung Wook Shin, "An Efficient Hardware Implementation of ARIA Block Cipher Algorithm Supporting Four Modes of Operation and Three Master Key Lengths," Journal of Korea Institute of Information and Communication Engineering, vol. 16, no. 11, pp. 2517-2524, Nov. 2012.

[4] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, "PRESENT: An Ultra-Lightweight Block Cipher," *Cryptographic Hardware and Embedded Systems (CHES 07)*, LNCS 4727, Springer, pp. 450-466, 2007.