초경량 블록암호 PRESENT-80/128의 하드웨어 구현

조욱래* · 김기쁨* · 신경욱*

*금오공과대학교

A Hardware Implementation of Ultra-Lightweight Block Cipher PRESENT-80/128

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

*Kumoh National Institute of Technology

E-mail : jodnrfo2@kumoh.ac.kr

요 약

80/128-비트의 마스터키를 지원하는 초경량 블록암호 PRESENT-80/128의 하드웨어 구현에 대해 기술한다. PRESENT 알고리듬은 SPN (substitution and permutation network)을 기반으로 하며 31번의 라운드 변환을 갖는다. 64-비트 데이터 패스를 갖는 단일 라운드 변환 회로를 이용하여 31번의 라운드가 반복처리 되도록 하였으며, 암호화/복호화 회로가 공유되도록 설계하였다. Verilog HDL로 설계된 PRESENT 프로세서를 Virtex5 XC5VSX-95T FPGA로 구현하여 정상 동작함을 확인하였다. 최대 275 Mhz 클록으로 동작하여 550 Mbps의 성능을 갖는 것으로 예측되었다.

ABSTRACT

This paper describes a hardware implementation of ultra-lightweight block cipher algorithm PRESENT-80/128 that supports for two master key lengths of 80-bit and 128-bit. The PRESENT algorithm that is based on SPN (substitution and permutation network) consists of 31 round transformations. A round processing block of 64-bit data-path is used to process 31 rounds iteratively, and circuits for encryption and decryption are designed to share hardware resources. The PRESENT-80/128 crypto-processor designed in Verilog-HDL was verified using Virtex5 XC5VSX-95T FPGA and test system. The estimated throughput is about 550 Mbps with 275 MHz clock frequency.

키워드

PRESENT, ultra-lightweight block cipher, cryptography, block cipher, security, internet of things

Ⅰ. 서 론

모든 사물들이 무선 네트워크로 연결되어 정보를 처리하고 제공하는 사물인터넷 (internet of thing; IoT) 기술이 급속히 보편화되고 있다. 무선 환경에서는 기지국 영역 내에 있는 모든 단말기들이 다른 사람의 정보를 수신할 수 있으므로, 허가된 수신자 이외에 제 3자가 정보를 알지 못하게 하는 데이터 기밀성과 사용자인증 등 정보보안 기술이 필수적으로 요구된다.[1]

지금까지 많은 정보보안 알고리듬 들이 개발되고 실용화되어 왔으나, IoT 보안을 위해서는 저전력, 저면적 특성이 매우 중요한 요소이다. 최근 IoT 보안에 적합한 다양한 경량 보안 알고리듬들이 개발되고 있다.[2-3] 독일의 보훔대학교에서 개발된 비밀키 방식의 블록암호 알고리듬 PRESENT는 SPN (substitution and permutation network) 구조를 기반으로 하여 초경량 구현이 가능하다는 장점을 갖는다. PRESENT는 선형공격, 불능 차분 공격 등의 보안공격에 대한 안정성이 입증되었고, 초경량 구현이 가능하여 RFID, IoT의 보안에 적합한 것으로 평가되고 있다. [4]

본 논문에서는 IoT 환경에 적합하도록 최적화된 PRESENT 암호 코어를 설계하였으며, FPGA 구현을 통해 하드웨어 동작을 검증하였다. 저면적과 저전력 구현을 위해 암호화/복호화, 라운드키 생성을 위한 라운드 블록의 하드웨어 자원 공유를 통해 최적화하였다.

Ⅱ. PRESENT 블록암호 알고리듬[4]

PRESENT는 64-비트의 평문/암호문 블록을 마스터키 (80-비트 또는 128-비트)로 암호화/복호화하여 64-비트의 암호문/평문을 생성하는 대칭키 방식의 블록암호 알고리듬이다. SPN 구조를 기반으로 하는 PRESENT는 31번의 라운드 변환을 통해 평문/암호문을 출력한다.

PRESENT의 암·복호화 과정은 그림 1과 같으며, 암호화 과정의 라운드 변환은 그림 1-(a)와 같이 라운드키 가산 (addRoundKey), 비선형 S-box (SBoxLayer), 비트 치환 (PLayer)으로 구성된다. 복호화 과정은 암호화 과정의 역순으로 이루어지며, 라운드키도 역순으로 사용된다. 또한 S-box 역변환을 위한 InvSBoxLayer와 비트 역치환을 위한 InvPLayer가 사용된다. 암호·복호화 과정에서 사용되는 라운드키는 마스터키를 바탕으로 키 스케줄러에 의해 생성된다.

Ⅲ. PRESENT-80/128 코어 설계

본 논문에서는 80/128-비트의 마스터키를 지원하는 PRESENT-80/128 암호/복호 프로세서를 설계하였다. PRESENT-80/128 코어는 라운드 블록, 키 스케줄러 그리고 제어블록으로 구성되며, 키 스케줄러 블록에서 64-비트의 라운드키를 받아 31번의 라운드 변환을 통해 암호화/복호화를 수행한다. 라운드 변환 블록은 그림 2와 같으며, 중간 결과를 저장하는 64-비트 상태 레지스터, 비선형 치환을 수행하는 SIS-box (S-box와 InvS-box의 통합), 64-비트 퍼뮤테이션을 수행하는 PIP_Layer 블록 (P_Layer와 InvP_Layer의 통합) 그리고 64-비트의 라운드키를 가산하는 XOR 게이트 등으로 구성된다.

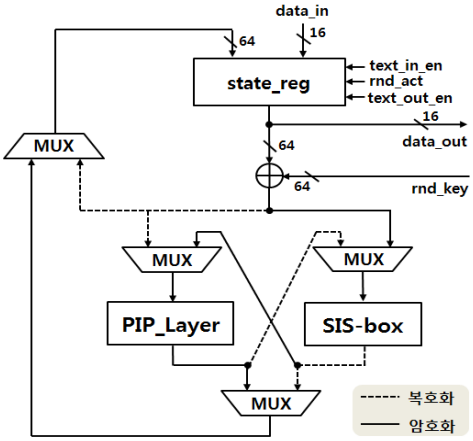
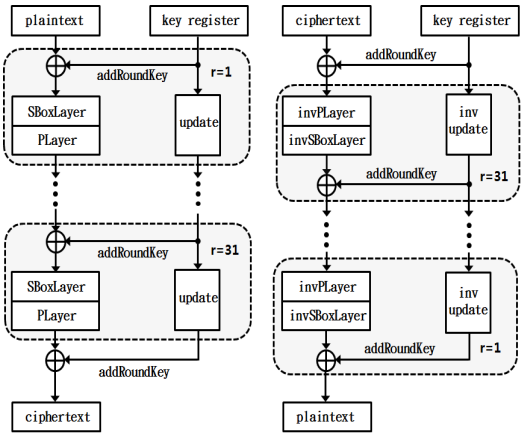


그림 2. 라운드 블록
Fig. 2. Round block

키 스케줄링 블록은 80-비트 또는 128-비트의 마스터키를 받아 라운드 변환에 사용되는 라운드키를 생성하며, 그림 3과 같이 구성된다. 마스터키를 저장하는 레지스터와 갱신된 중간키를 저장하는 레지스터를 가지고 있으며, 순환이동 회로, S-box, XOR 게이트 등으로 구성된다.

마스터키 80/128-비트로부터 상위 64-비트를 초기 라운드키로 내보내며, 라운드키 생성은 다음과 같다. 마스터키가 80-비트인 경우의 키 스케줄은 왼쪽으로 61-비트 순환이동한 후, MSB의 4-비트 [79:76]를 S-box 연산하고, [19:15]의 5-비트를 라운드 수와 XOR하여 라운드키를 갱신한다. 128-비트의 키 스케줄의 경우 80-비트와 유사하게 왼쪽으로 61-비트만큼 순환이동 한 후, [127:124]와 [123:120]를 S-box 연산하고, [66:62]의 5-비트를 라운드 수와 XOR하여 라운드키를 갱신한다.



(a) encryption (b) decryption
그림 1. PRESENT의 암호/복호 과정
Fig. 1. Encryption and decryption of PRESENT

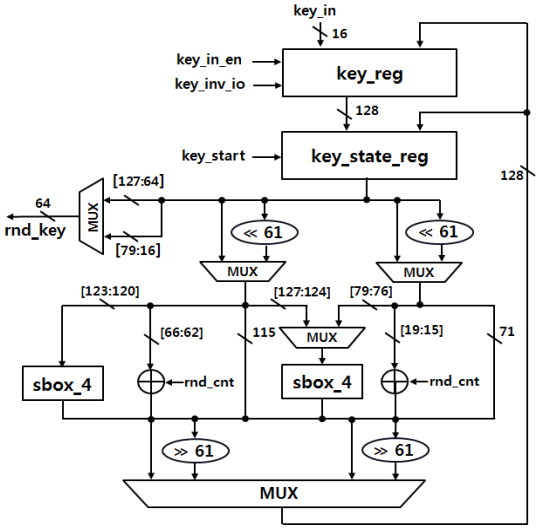


그림 3. 키 스케줄러
Fig. 3. Key scheduler

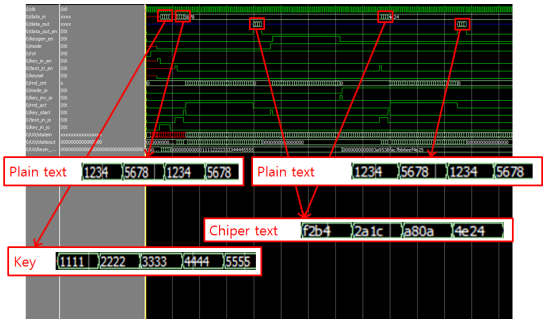


그림 4. PRESENT-80/128 코어의 기능검증 결과
Fig. 4. Simulation results of PRESENT-80/128 core

Ⅳ. 기능검증 및 FPGA 검증

Verilog HDL로 설계된 PRESENT-80/128 코어의 기능검증 결과는 그림 4와 같으며, 64-비트의 평문 "12 34 56 78 12 34 56 78"와 80-비트의 마스터키 "11 11 22 22 33 33 44 44 55 55"를 입력으로 사용하였다. 암호화 결과로 64-비트의 암호문 "f2 b4 2a 1c a8 0a 4e 24"가 출력되고, 이를 다시 복호한 결과는 암호화 입력으로 사용된 평문 "12 34 56 78 12 34 56 78"이 출력되어 논리기능이 정상적으로 동작함을 확인하였다.

시뮬레이션이 완료된 PRESENT-80/128 코어는 FPGA 구현을 통해 하드웨어 동작을 검증하였다. 검증 시스템은 FPGA 보드, PC, UART 인터페이스 등으로 구성되며, Xilinx Virtex5 XC5VSX-95T FPGA가 사용되었다. FPGA 검증결과 화면은 그림 5와 같으며, 이미지를 암호화한 후 이를 다시 복호화하여 원래의 이미지가 출력되어 정상적으로 동작함을 확인하였다. 275 MHz 클록으로 동작 가능하여 550 Mbps의 암호/복호 성능을 가지며, PRESENT-80/128 코어의 특성은 표 1과 같다.

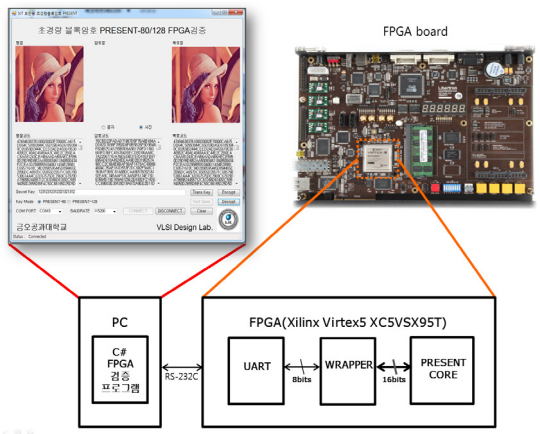


그림 5. PRESENT-80/128 코어의 FPGA 검증 결과
Fig. 5. FPGA verification result of PRESENT-80/128 core

표 1. PRESENT-80/128 코어의 특성
Table 1. Summary of PRESENT-80/128 core

FPGA	Virtex5 XC5VSX-95T
Max. clock frequency	275 MHz
Throughput	550 Mbps
LUT-Flip Flop pairs	802

Ⅴ. 결 론

ISO/IEC 국제표준으로 승인된 80/128-비트 블록암호 알고리듬 PRESENT를 하드웨어로 구현하여 동작을 확인하였다. 암호화/복호화 라운드 연산과 라운드키 생성을 위한 하드웨어 자원이 공유되도록 설계했다. 설계된 PRESENT-80/128 코어는 Virtex5 XC5VSX-95T FPGA 디바이스에서 802 LUT-FF pairs의 경량으로 구현되었으며, IoT, RFID 환경과 같이 저전력, 경량화가 요구되는 응용분야의 정보보호 코어로 활용이 가능하다.

ACKNOWLEDGMENTS

· This work was supported by the 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.

참고문헌

[1] W. Stalling, *Cryptography and Network Security*, Prentice Hall, 1999.
[2] S. Jana, J. Bhaumik, and M.K. Maiti, "Survey on lightweight block cipher," *International Journal of Soft Computing and Engineering*, vol. 3, pp. 183-187, Nov 2013.
[3] O. Ozen et al., "Lightweight block cipher revisisted: Cryptanalysis of reduced round PRESENT and HIGHT," in *ACISP, ser. LNCS*, vol. 5594. Springer, pp. 90-107, 2009.
[4] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin and C. Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher. pp. 33-59, *CHES 2007.*