블록 암호 알고리즘 PRESENT/ARIA/AES를 지원하는 암호 프로세서의 MPW 구현

조욱래* · 김기쁨* · 배기철* · 신경욱*

*금오공과대학교

MPW Implementation of Crypto-processor Supporting Block Cipher Algorithms of PRESENT/ARIA/AES

Wook-lae Cho* · Ki-bbeum Kim* · Gi-chur Bae* · Kyung-wook Shin**

*Kumoh National Institute of Technology

E-mail : jodnrfo2@kumoh.ac.kr

요 약

PRESENT/ARIA/AES의 3가지 블록 암호 알고리즘을 지원하는 암호 프로세서를 MPW(Multi-Project Wafer)칩으로 구현하였다. 설계된 블록 암호 칩은 PRmo(PRESENT with mode of operation) 코어, AR_AS(ARIA_AES) 코어, AES-16b 코어로 구성된다. PRmo는 80/128-비트 마스터키와, ECB, CBC, OFB, CTR의 4가지 운영모드를 지원한다. 128/256-비트 마스터키를 사용하는 AR_AS 코어는 서로 내부 구조가 유사한 ARIA와 AES를 통합하여 설계하였다. AES-16b는 128-비트 마스터키를 지원하고, 16-비트 datapath를 채택하여 저면적으로 구현하였다. 설계된 암호 프로세서를 FPGA검증을 통하여 정상 동작함을 확인하였고, 0.18um 표준 셀 라이브러리로 논리 합성한 결과, 100 KHz에서 52,000 GE로 구현이 되었으며, 최대 92 MHz에서 동작이 가능하다. 합성된 다중 암호 프로세서는 MPW 칩으로 제작될 예정이다.

키워드

MPW, PRESENT, ARIA, AES, Crypto_processor, Block Cipher

Ⅰ. 서 론

사물 간에 무선 네트워크로 연결되어 정보를 주고받는 사물인터넷 (internet of thing; IoT) 기술이 주목받고 있다. 정보를 송수신하는 과정에서 허가된 수신자 이외에 제삼자가 정보를 알지 못하게 하는 데이터 기밀성과 사용자인증 등 정보보안 기술이 필수적으로 요구된다.[1]

독일 보훔대학교에서 개발된 비밀키 방식의 블록암호 알고리즘 PRESENT는 마스터키 길이 80/128-bit를 지원하는 64-bit 블록 암호이다.[2] ARIA와 AES 알고리듬은 서로 유사한 형태로 SPN(substitution permutation network) 구조를 가지고 마스터키 128/192/256-bit를 사용하여 128-bit의 평문/암호문을 암호/복호 하는 블록암호이다.[3-4]

본 논문에서는 PRESENT 블록암호 알고리즘에 ECB, CBC, OFB, CTR의 4가지 운영모드를 적용한 PRmo 코어와, 효율적인 하드웨어를 위해 ARIA와 AES 알고리즘을 통합한 AR_AS 코어, 16-bit datapath의 AES 코어를 통합 설계하여 MPW 칩으로 구현하였다.

2장에서는 다중 블록 암호 프로세서의 코어구조를, 3장에서는 기능검증 및 MPW 칩 제작을 설명하며 4장에서 결론으로 마무리 짓는다.

Ⅱ. 다중 블록 암호 프로세서의 코어 구조

설계된 다중 암호 프로세서는 PRESENT/ARIA/AES의 3가지 블록 암호 알고리즘을 지원하며, 그림 1과 같이 PRmo(PRESENT with mode of operation), AR_AS(ARIA_AES), AES-16b로 이루어져 있다. 프로세서의 핀 개수 감소를 위해

16-bit씩 시분할 방식으로 입/출력이 되도록 설계하였다. AR_AS는 128/256-bit 입/출력이므로 iRegister(aria_text_reg ,aria_key_reg), oRegister (aria_out_reg)의 I/O 데이터 변환을 위한 레지스터가 필요하다.

PRESENT 알고리즘은 80/128-bit의 마스터키를 지원하며, SPN(substitution and permutation network) 구조로 경량화 구현이 가능하다는 장점을 갖는다. 암호 코어 PRmo는 4가지 운영모드(ECB, CBC, OFB, CTR)와 80/128-bit의 2가지 마스터키 길이를 지원하도록 설계되었다. 한 라운드 변환이 단일 클록으로 처리되며 64-bit 데이터가 입력되어 출력되기까지 총 32 클록이 소요된다.

ARIA와 AES를 통합하여 설계한 AR_AS 코어는 128/256-bit 마스터키 길이를 지원하며, ARIA와 AES 알고리즘을 선택적으로 수행한다. ARIA의 경우 마스터키 길이에 따라서 13/17 클록을 소모하며, AES의 경우 마스터키 길이에 따라 11/15 클록을 소모한다. ARIA와 AES 알고리즘의 라운드 연산과 키 스케줄링 연산을 선택적으로 수행하는 통합 라운드블록, 통합 라운드 키 생성 블록, 제어블록 등으로 구성된다.

128-bit 마스터키를 사용하여 128-bit 평문/암호문을 암호/복호하는 16-bit datapath AES 코어를 설계하였다. 기본적인 알고리즘 연산 순서를 적용한 라운드 블록은 암호화/복호화의 각 단계별 순서가 다르기 때문에 하드웨어 복잡도를 최소화하기 위해서 암호화 할 때 가환성이 있는 Shift-Row와 SubByte의 순서를 변경하여 설계하였다.

III. 기능검증 및 MPW 칩 제작

설계된 암호 프로세서를 FPGA 보드에 구현하여 하드웨어 동작을 검증하였다. 검증 시스템은 PC, FPGA 보드, UART 인터페이스로 구성되며, FPGA보드는 Xilinx Virtex5 XC5VSX95T가 사용되었다. 그림 2는 FPGA 검증 결과를 보이고 있으며, C# 기반의 GUI 환경을 통해 암호 프로세서의 암호화/복호화 결과를 나타낸다. 좌측의 이미지를 FPGA로 전송하여 암호 프로세서에서 암호화한 결과는 중앙의 이미지와 같다. 다시 암호화된 중앙의 이미지를 FPGA로 전송하여 복호화한 결과는 우측의 이미지와 같고, 우측의 이미지와 좌측의 원본이미지가 같으므로 암호 프로세서가 올바르게 동작함을 알 수 있다.

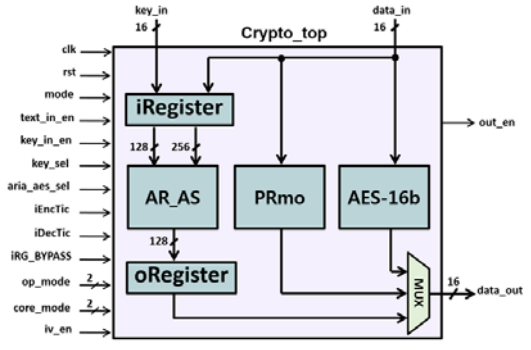

Fig. 1. Crypto_processor implementing multiple block cipher

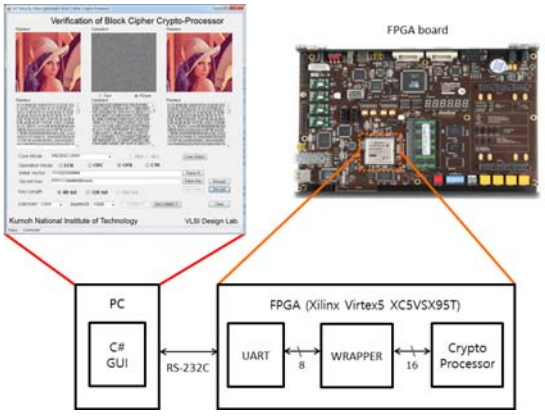

Fig. 2. Result of FPGA verification

본 논문에서 설계한 다중 블록 암호 프로세서는 MPW 칩으로 제작될 예정이다. 그림 3은 암호 프로세서를 MPW 칩으로 설계하기 위해 사용한 툴과 진행 과정을 나타낸다. Front-end 단계에서는 RTL-modeling을 한 뒤 Modelsim을 이용하여 기능검증을 하였고, DesignCompiler로 로직 합성을 하였으며, Formality로 RTL 코드와 gate-level netlist가 일치하는지 검증하였다. Primetime을 이용하여 STA(Static Timing Analysis)를 수행하고, pre-layout simulation을 진행하였다. Back-end에서는 Astro를 이용하여 게이트 수준의 회로를 P&R(Placement and Routing)하였고, 레이아웃의 타이밍을 검증하기 위해 StarRCXT로 기생 커패시턴스와 저항 값을 추출하여 레이아웃에 대한 STA와 Post-layout simulation을 수행하였다. 그

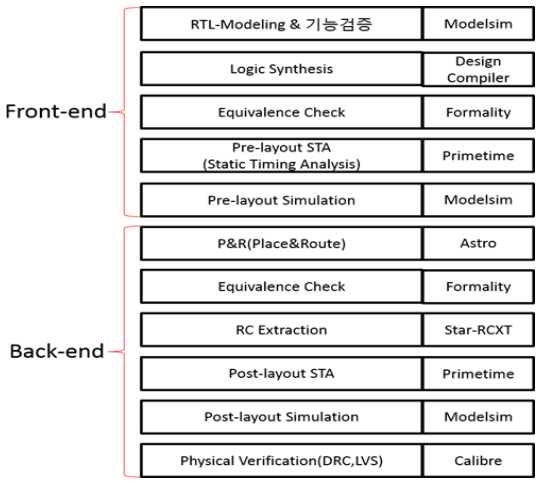

Fig. 3. Design flow of MPW chip

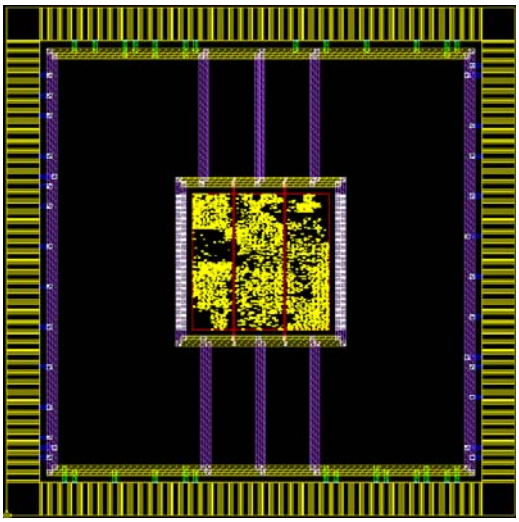

Fig. 4. Layout of MPW chip

림 4는 최종 레이아웃 사진이며, 설계된 블록 암호 프로세서의 면적은 960um×960um이다.

Ⅳ. 결 론

본 논문에서는 PRESENT/ARIA/AES를 지원하는 블록 암호 프로세서를 PC, UART 인터페이스 기반의 FPGA 검증을 통하여 정상 동작함을 확인하였다. magnachip/sk hynix 0.18um 표준 셀 라이브러리로 논리 합성한 결과, 100 KHz에서 52,000 GE로 구현이 되었으며, 최대 92 MHz에서 동작이 가능하다. 블록 암호 프로세서의 최종 레이아웃 면적은 960um×960um이며, MPW 칩으로 제작 될 예정이다.

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] W. Stalling, *Cryptography and Network Security*, Prentice Hall, 1999.

[2] 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*.

[3] KS X 1213:2004, 128 bit Block Encryption Algorithm ARIA, Korean Agency for Technology and Standards (KATS), 2004.

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