ARIA-AES 블록암호의 효율적인 구현

김기쁨* · 신경욱*

*금오공과대학교

An Efficient Implementation of ARIA-AES Block Cipher

Ki-Bbeum Kim* · Kyung-Wook Shin

Kumoh National Institute of Technology

E-mail : kkp@kumoh.ac.kr

요 약

한국 표준 블록암호 알고리듬 ARIA(Academy, Research Institute, Agency)와 미국 표준인 AES (Advanced Encryption Standard) 알고리듬은 128-비트 블록 길이를 지원하고 SPN(substitution permutation network) 구조를 특징으로 가져 서로 유사한 형태를 지닌다. 본 논문에서는 ARIA와 AES를 선택적으로 수행하는 ARIA-AES 통합 프로세서를 효율적으로 구현하였다. Verilog HDL로 설계된 ARIA-AES 통합 프로세서를 Virtex5 FPGA로 구현하여 정상 동작함을 확인하였고, 0.18㎛ 공정의 CMOS 셀 라이브러리로 100KHz의 동작주파수에서 합성한 결과 39,498 GE로 구현되었다.

키워드

ARIA, AES, Block Cipher, S-Box, Hardware sharing

Ⅰ. 서 론

ARIA(Academy, Research Institute, Agency) 알고리듬[1]은 2004년 한국 산업 규격(KS, Korea Standard) 표준으로 지정된 블록 암호 알고리듬으로 2001년 NIST(National Institute of Standards and Technology)에 의해 미국 표준으로 제정된 AES(Advanced Encryption Standard) 알고리듬[2]와 함께 스마트카드, 전자여권, 서버급 암호장비 등 기밀성이 요구되는 다양한 정보 보호 분야에서 사용되고 있다.[3]

ARIA와 AES 알고리듬은 서로 유사한 형태로 SPN(substitution permutation network) 구조를 가지고 마스터키 길이 128/192/256-비트를 지원하는 128-비트 블록 암호이다. ARIA와 AES 알고리듬의 치환계층에서 사용되는 S-box는 동일한 유한체 $GF(2^8)$상의 역원 연산을 이용하여 구현된다.

본 논문에서는 블록 암호 ARIA와 AES 알고리듬 기능을 선택적으로 수행하는 ARIA-AES 통합 프로세서의 효율적인 하드웨어 공유 구조를 제안하고, 이를 Verilog-HDL로 모델링 하여 설계하여 FPGA 구현을 통해 하드웨어 동작을 검증하였다.

Ⅱ. ARIA[1], AES[2] 알고리듬

블록 암호 알고리듬 ARIA 알고리듬은 대칭키 알고리듬으로 128-비트 블록 단위로 암·복호화 하며 128/192/256-비트 마스터키 길이를 지원한다. 라운드 수는 마스터키 길이에 따라 12/14/16로 이루어져 있으며 involution SPN(substitution and permutation network) 구조이다. 라운드는 AddRoundKey, Substitution, Diffusion의 3가지 함수로 이루어져 있으며 홀수와 짝수 라운드에 각기 다른 치환 계층을 사용하고, 최종 라운드는 확산 계층 대신 라운드 키 덧셈으로 대체된다.

AES 알고리듬은 ARIA와 동일한 대칭키 블록 암호로 128-비트 블록 단위로 암·복호화 하며 128/192/256-비트 마스터키 길이를 지원한다. 라운드 수는 마스터키 길이에 따라서 10/12/14로 이루어져 있으며 SPN(substitution and permutation network) 구조이다. 라운드는 AddroundKey, SubByte, ShiftRows, Mixcolums 의 4가지 함수로 이루어져 있으며 복호화는 암호화 과정의 역순으로 최종라운드에서 암호화의 경우 Mixcolums 연산을 복호화의 경우 InvMixcolums 연산을 사용하지 않는다.

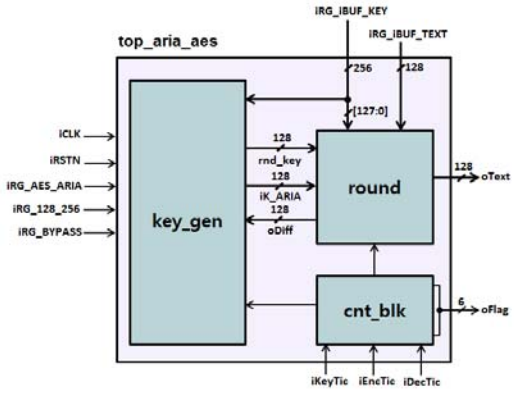


Fig. 1. Architecture of ARIA-AES processor

III. ARIA-AES 통합 프로세서 설계

설계된 ARIA-AES 통합 프로세서는 128/256-비트 마스터키 길이를 지원하고, ARIA와 AES 알고리듬을 선택적으로 수행한다. ARIA 알고리듬의 경우 마스터키 길이에 따라 13/17 클록 사이클이 소모되며, AES 알고리듬의 경우 마스터키 길이에 따라 11/15 클록 사이클을 소모한다. ARIA-AES 통합 프로세서의 전체 구조는 그림 1과 같으며 ARIA와 AES 알고리듬의 라운드 연산과 키 스케줄링 연산을 선택적으로 수행하는 통합 라운드 블록(round), 통합 라운드 키 생성 블록(key_gen) 및 제어블록(cnt_blk) 등으로 구성된다.

ARIA와 AES의 라운드 연산을 선택적으로 수행하는 통합 라운드 블록(round)은 그림 2와 같으며 라운드 연산의 중간 결과를 저장하는 128-비트 상태 레지스터 rState, ARIA와 AES의 치환계

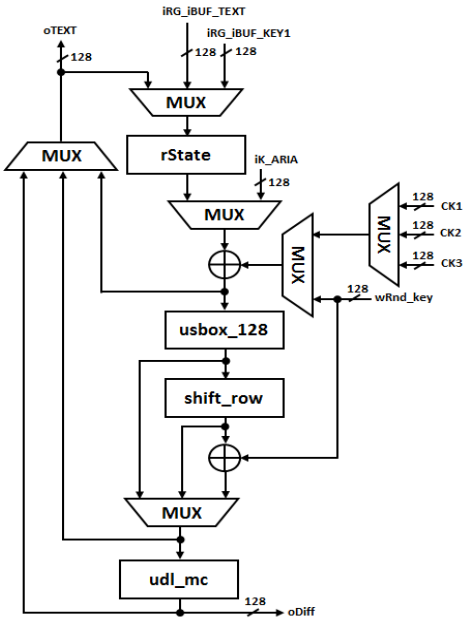


Fig. 2. Round Block of ARIA-AES processor

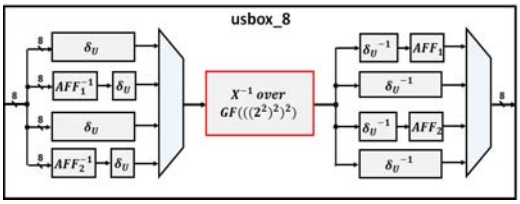


Fig. 3. Structure of usbox_8

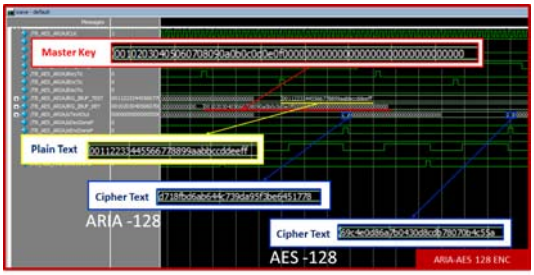
층을 선택적으로 수행하는 통합 치환계층 usbox_128, ARIA의 라운드 변환의 과정에서는 수행되지 않으며 AES의 라운드 변환 과정에서 바이트 단위로 이동 연산을 수행하는 shift_row, ARIA와 AES의 확산계층을 선택적으로 수행하는 통합 확산계층 udl_mc, 그리고 라운드 키 가산과 ARIA의 키 초기화 과정에서 사용되는 128-비트 XOR 게이트 2개 등으로 구성된다.

통합 치환계층 usbox_128의 구조는 usbox_8 4개를 포함하는 usbox_32 4개로 구성되어 있다. usbox_8의 구조는 그림 3과 같으며, 유한체 $GF(2^8)$상의 역원을 다항식 기저(polynomial basis) 방식을 사용하여 복합체 $GF(((2^2)^2)^2)$상의 역원인 X^{-1} 구현 하였으며, X^{-1} 연산 기능을 공유하면서 S_1, S_2, S_1^{-1}, S_2^{-1} 의 Affine 변환을 선택적으로 수행할 수 있도록 설계하였다. δ_u는 $GF(2^8)$상의 원소를 $GF(((2^2)^2)^2)$ 상의 원소로 매핑 시키는 동형(isomorphic) 함수이고, δ_u^{-1}는 $GF(((2^2)^2)^2)$ 상의 원소를 $GF(2^8)$상의 원소로 매핑 시키는 역변환 함수이다. AFF_1, AFF_2, AFF_1^{-1}, AFF_2^{-1}는 S_1, S_2, S_1^{-1}, S_2^{-1}의 Affine 변환을 나타낸다.

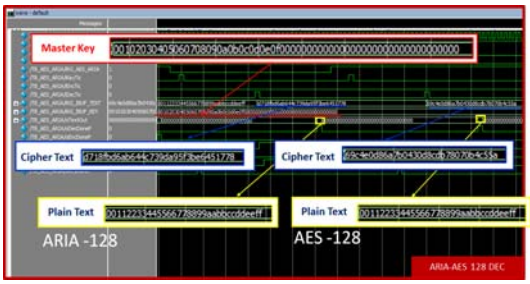
IV. 기능검증 및 FPGA검증

설계된 ARIA-AES 통합 프로세서의 동작을 시뮬레이션으로 검증했으며, 검증결과는 그림 4-(a),(b)와 같다. 그림 4-(a)는 ARIA와 AES의 암호화 기능검증 결과로 128-비트의 마스터키 “0010 2030 4050 6070 8090 a0b0 c0d0 e0f0”과 128-비트의 평문 “0011 2233 4455 6677 8899 aabb ccdd eeff”를 사용하여 ARIA-128과 AES-128을 순차적으로 암호화한 결과 “d718 fbd6 ab64 4c73 9da9 5f3b e645 1778”, “69c4 e0d8 6a7b 0430 d8cd b780 70b4 c55a”이 출력되었고, 이를 복호화 한 결과 그림 4-(b)와 같이 원래의 평문 “0011 2233 4455 6677 8899 aabb ccdd eeff”이 출력됨을 확인할 수 있다.

기능 검증이 완료된 ARIA-AES 통합 프로세서를 FPGA 디바이스에 구현하여 하드웨어 동작을 검증하였다. 그림 5는 FPGA 검증 결과를 보이고



(a)



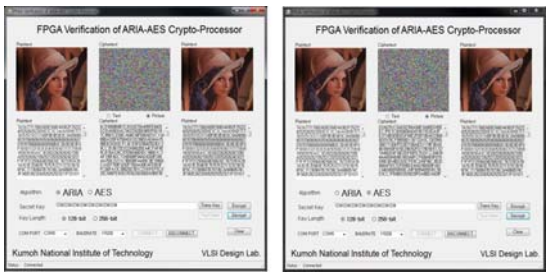
(b)

Fig. 4. Simulation results of ARIA-AES processor
(a) ARIA-AES 128 Enc (b) ARIA-AES 128 Dec

있으며, ARIA-128과 AES-128의 FPGA 검증 결과를 나타내고 있다. GUI 프로그램을 통해 ARIA-AES 통합 프로세서의 암호화/복호화 결과가 화면에 표시되어 그림 5-(a)는 ARIA-128의 결과, 그림 5-(b)는 AES-128의 결과로 좌측 이미지를 암호화 한 후 복호화 하여 좌측의 원본 이미지가 복원되어 FPGA에 구현된 ARIA-AES 통합 프로세서가 올바르게 동작함을 확인할 수 있다.

V. 결 론

블록암호 알고리듬 ARIA와 AES를 선택적으로 수행하는 AIRA-AES 통합 하드웨어를 효율적으로 구현하였다. 치환계층(S-box)과 확산계층의 하드웨어 자원공유를 통해 ARIA와 AES를 독립적으로 구현하는 경우에 비해 하드웨어 복잡도를 크게 줄였다. 0.18㎛ 공정의 CMOS 셀 라이브러리로 합성한 결과, 100 KHz의 동작 주파수에서 39,498 GE로 구현이 되었으며, 최대 동작 주파수 80 MHz 클록 속도를 기준으로 ARIA는 마스터키 길이에 따라 853/731 Mbps 처리율로 수행되고, AES는 마스터키 길이에 1024/853 처리율로 수행된다.



(a) (b)

Fig. 5. FPGA verification of ARIA-AES processor
(a) ARIA-128 (b) AES-128

ACKNOWLEDGMENTS

· This paper was supported by Kumoh National Institute of Technology.
· The authors are thankful to IDEC for EDA software support.

참고문헌

[1] KS X 1213:2004, 128 bit Block Encryption Algorithm ARIA, Korean Agency for Technology and Standards (KATS), 2004.
[2] FIPS-197, Advanced Encryption Standard, National Institute of Standard and Technology(NIST), November, 2001.
[3] 안하기, 신경욱, “AES Rijndael 블록 암호 알고리듬의 효율적인 하드웨어 구현”, 정보보호학회논문지, 제 12권 2호, 53-64, 2002.