JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 4 : 795~803 Apr. 2017

4가지 운영모드와 128/256-비트 키 길이를 지원하는 ARIA-AES 통합 암호 프로세서

김기쁨 · 신경욱*

A Unified ARIA-AES Cryptographic Processor Supporting Four Modes of Operation and 128/256-bit Key Lengths

Ki-Bbeum Kim · Kyung-Wook Shin*

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

요 약

블록암호 ARIA와 AES를 단일 회로로 통합하여 구현한 이중표준지원 암호 프로세서에 대해 기술한다. ARIA-AES 통합 암호 프로세서는 128-비트, 256-비트의 두 가지 키 길이를 지원하며, ECB, CBC, OFB, CTR의 4가지 운영모드를 지원하도록 설계되었다. ARIA와 AES의 알고리듬 공통점을 기반으로 치환계층과 확산계층의 하드웨어 자원이 공유되도록 최적화 하였으며, on-the-fly 키 스케줄러가 포함되어 있어 평문/암호문 블록의 연속적인 암호/복호화 처리가 가능하다. ARIA-AES 통합 프로세서를 0.18㎛ 공정의 CMOS 셀 라이브러리로 합성한 결과 54,658 GE로 구현되었으며, 최대 95 MHz의 클록 주파수로 동작할 수 있다. 80 MHz 클록 주파수로 동작할 때, 키 길이 128-b, 256-b의 ARIA 모드에서 처리율은 각각 787 Mbps, 602 Mbps로 예측되었으며, AES 모드에서는 각각 930 Mbps, 682 Mbps로 예측되었다. 설계된 암호 프로세서를 Virtex5 FPGA로 구현하여 정상 동작함을 확인하였다.

ABSTRACT

This paper describes a dual-standard cryptographic processor that efficiently integrates two block ciphers ARIA and AES into a unified hardware. The ARIA-AES crypto-processor was designed to support 128-b and 256-b key sizes, as well as four modes of operation including ECB, CBC, OFB, and CTR. Based on the common characteristics of ARIA and AES algorithms, our design was optimized by sharing hardware resources in substitution layer and in diffusion layer. It has on-the-fly key scheduler to process consecutive blocks of plaintext/ciphertext without reloading key. The ARIA-AES crypto-processor that was implemented with a 0.18㎛ CMOS cell library occupies 54,658 gate equivalents (GEs), and it can operate up to 95 MHz clock frequency. The estimated throughputs at 80 MHz clock frequency are 787 Mbps, 602 Mbps for ARIA with key size of 128-b, 256-b, respectively. In AES mode, it has throughputs of 930 Mbps, 682 Mbps for key size of 128-b, 256-b, respectively. The dual-standard crypto-processor was verified by FPGA implementation using Virtex5 device.

키워드 : ARIA, AES, 블록암호, 운영모드, 암호 프로세서, 정보보안

Key word : ARIA, AES, block cipher, mode of operation, cryptographic processor, information security

Received 07 December 2016, **Revised** 08 December 2016, **Accepted** 29 December 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, Kyungbuk 39177, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.4.795 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근, 스마트폰과 사물인터넷(Internet of Things; IoT)의 보급이 급속히 확대되면서 무선 네트워크 기반의 정보 유통이 폭발적으로 늘어나고 있다. 특히, 사람과 사물이 네트워크를 통해 하나로 연결되는 초연결 사회(hyper-connected society)가 실현됨에 따라 다양한 보안위협에 대응할 수 있는 정보보안 기술이 중요 이슈로 부각되고 있다. 정보보안이란 여러 가지 보안위협으로부터 정보를 보호하는 방법 또는 기술을 의미하며, 정보의 내용이 제3자에게 노출되지 않도록 하는 기밀성(confidentiality), 정보의 저장 및 송수신 과정에서 훼손 및 변조를 방지하는 무결성(integrity), 사용자, 기기의 정당성과 정보의 출처를 확인하는 인증(authentication) 등 다양한 측면을 갖는다[1].

정보보안 시스템의 구현을 위해서는 대칭키(비밀키) 암호, 공개키(public key) 암호, 해시(hash) 함수 등 다양한 기술들이 복합적으로 사용된다. 암호화와 복호화에 동일한 키가 사용되는 대칭키 암호는 기밀성을 제공하는 기본적인 암호방식이며, AES(Advanced Encryption Standard) [2], ARIA(Academy, Research Institute, Agency) [3], LEA(Lightweight Encryption Algorithm) [4] 등 매우 다양한 알고리듬이 사용되고 있다. 공개키 암호는 정보 송신자와 수신자가 공개된 키와 자신의 비밀키를 사용하여 암호화와 복호화를 하는 방식으로 전자서명, 키 분배 등을 위해 사용되며, RSA(Rivest, Shamir, Adleman) [5], ECC(Elliptic Curve Cryptography) [6] 등이 대표적이다.

블록암호는 정보를 일정한 크기(블록)로 분할하여 블록단위로 암호화하는 대칭키 암호방식이며, 정보의 기밀성을 필요로 하는 다양한 정보보안 시스템에 기본적으로 사용되고 있다. 널리 사용되고 있는 대칭키 블록암호는 미국에서 표준으로 제정된 AES가 있으며, 우리나라는 AES에 대응되는 블록암호로 ARIA를 국가표준으로 제정하여 민간분야와 국가기관의 보안시스템에 사용하도록 적극 권장하고 있다. AES와 ARIA는 알고리듬 특성상 여러 가지 공통점을 갖는다. 두 알고리듬은 Non-Feistel 방식의 SPN(Substitution-Permutation Network) 구조를 기반으로 하며, 블록길이와 키 길이가 동일하고, S-box를 정의하는 유한체와 기약다항식(irreducible polynomial)이 동일하다는 특징을 갖는다.

따라서 두 블록암호 알고리듬을 통합하여 다중표준지원 암호 프로세서를 구현하면, 스마트카드, 전자여권 등 기밀성과 인증이 요구되는 다양한 정보보호 분야의 보안 SoC 설계에 효율적으로 사용될 수 있다.

본 논문에서는 블록암호 ARIA와 AES를 단일 하드웨어 구조로 통합하여 구현한 이중표준지원 암호 프로세서에 대해 기술한다. ARIA와 AES의 라운드변환 연산의 공통적 특성을 이용한 자원공유 기법을 적용함으로써 최적화된 구현결과가 얻어졌다. 블록암호의 기밀성 향상을 위해 OFB(Output Feed-Back), CBC(Cipher Block Chaining), CTR(Counter) 운영모드와 128-비트, 256-비트의 두 가지 키 길이를 지원하도록 설계하였으며, FPGA 구현을 통해 하드웨어 동작을 검증하였다. Ⅱ장에서는 ARIA와 AES 블록암호에 대해 설명하고, Ⅲ장에서는 ARIA- AES 통합 암호 프로세서 설계에 대해 설명한다. 설계된 회로의 기능 검증 및 FPGA 구현 결과를 Ⅳ장에서 기술하고, Ⅴ장에서 결론을 맺는다.

Ⅱ. ARIA, AES 블록암호

2.1. ARIA 블록암호 [3]

ARIA는 128-비트의 평문(암호문) 블록을 암호(복호)화하여 동일한 길이의 암호문(평문)을 만드는 대칭키 방식의 블록암호 알고리듬이다. 128/192/256-비트의 세 가지 키 길이를 지원하며, 키 길이에 따라 12/14/16회의 라운드 변환을 수행하는 ISPN(Involution SPN) 구조를 갖는다. involution 이란 암호화 과정과 복호화 과정이 동일한 구조를 일컬으며, SPN 구조는 S-box와 확산함수가 반복적으로 적용되는 구조이다.

ARIA의 암호화·복호화 과정은 그림 1과 같으며, 홀수 라운드변환 함수(F_o)와 짝수 라운드변환 함수(F_e)로 구분되어 각기 다른 치환(substitution) 계층이 사용되며, 마지막 라운드변환 함수(F_f)에는 확산(diffusion) 계층이 라운드키 덧셈으로 대체된다. 암호화 과정에서는 암호화 라운드키 ek_i가 사용되고, 복호화 과정에서는 복호화 라운드키 dk_i가 사용되며, 라운드키는 키 확장을 통해 생성된다. 라운드 변환 함수 F_o와 F_e 그리고 F_f는 그림 2와 같이 라운드키 가산, 치환계층, 확산계층으로 구성된다. 홀수 라운드 변환 함수 F_o와 짝수 라운드 변환 함수 F_e에 각기 다른 치환 연산이 사용된다.

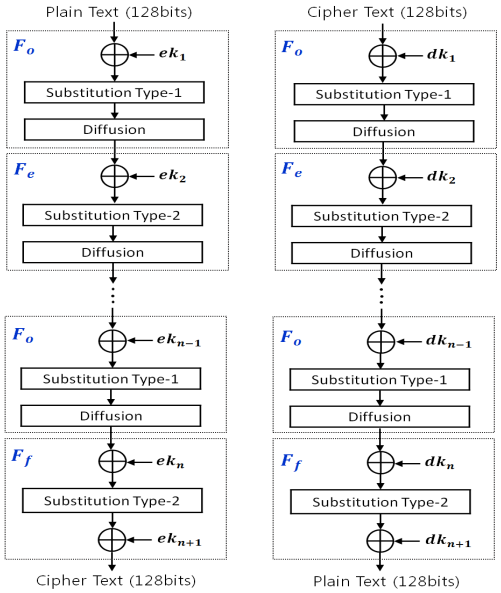


Fig. 1 Encryption and decryption of ARIA block cipher (a) encryption, (b) decryption

치환계층은 그림 3과 같이 두 가지 유형으로 구성되며, 유형-1은 홀수 라운드 변환 함수 F_o에 사용되고 유형-2는 짝수 라운드 변환 함수 F_e에 사용된다. 각 유형은 8-비트 입출력을 갖는 두 가지 S-box S_1, S_2와 이들의 역원인 S_1^{-1}, S_2^{-1}로 구성된다. 짝수 라운드 함수의 치환 LT^{-1}는 홀수 라운드 함수 치환 LT의 역치환으로 구성된다. 라운드키 가산은 이전 라운드의 중간 결과값과 128-비트 라운드키의 XOR 연산으로 구현된다.

확산계층은 16x16 involution 이진 행렬을 이용한 바이트 단위의 확산함수로 구성되며, 여기서 involution 이진 행렬은 $A^{-1}=A$의 성질을 갖는 행렬을 의미한다. 확산함수는 입력 16-바이트에 대해 바이트 단위의 행렬

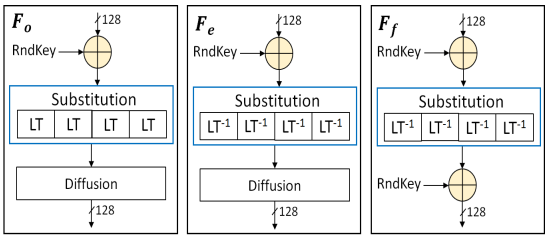


Fig. 2 Round functions of ARIA block cipher

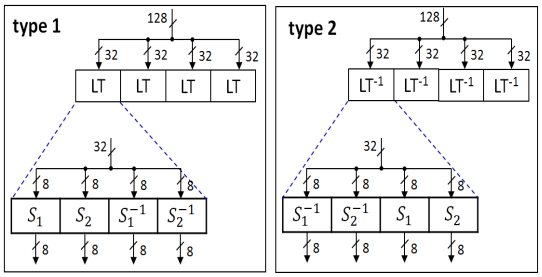


Fig. 3 Substitution layer of ARIA block cipher

곱셈을 수행하여 16-바이트의 결과를 출력한다.

ARIA 블록암호의 키 확장은 키 초기화와 라운드키 생성의 두 단계로 구성된다. 암호키로부터 4개의 128-비트 초기화 키 값 w0, w1, w2, w3가 생성된다. 라운드키 생성과정에서는 초기화 키 값 w0, w1, w2, w3를 조합하여 암호화 라운드키 ek_i와 복호화 라운드키 dk_i가 생성된다. 키 길이에 따라 12/14/16회의 라운드로 구성되고 마지막 라운드에는 키 가산이 두 번 이루어지므로, 13/15/17개의 라운드키가 생성된다.

2.2. AES 블록암호 [2]

AES는 DES(Data Encryption Standard)를 대체하기 위해 2001년도 미국 기술표준국에 의해 표준으로 제정된 블록암호 알고리듬이며, non-Feistel 방식의 SPN 구조를 갖는다. 128-비트의 평문(암호문)을 암호(복호)하여 동일한 길이의 암호문(평문)을 만들며, 128/192/256-비트의 키 길이에 따라 10/12/14회의 라운드변환을 수행한다. AES의 암호화 과정은 그림 4-(a)와 같으며, 초기 라운드키 가산, (N_r-1)회의 반복 라운드 및 최종 라운드로 처리된다. 각 라운드 변환은 SubByte, ShiftRow, MixColumn, AddroundKey의 변환으로 구성된다. 복호화 과정은 그림 4-(b)와 같으며, 암호화 라운드 연산에 사용되는 SubByte의 역변환인 InvSubByte, ShiftRow의 역변환인 InvShiftRow, MixColumn의 역변환인 InvMixColumn이 사용된다. 복호화에서는 라운드키가 역순으로 사용된다.

라운드키 가산(AddRoundKey)은 128-비트의 중간 연산 결과인 state와 라운드키의 XOR로 구현된다. SubByte 변환은 state를 구성하는 바이트에 대해 독립적인 비선형 치환을 수행한다. 비선형 치환에 사용되는 S-box는 유한체 $GF(2^8)$상에서 곱의 역원(multiplicative

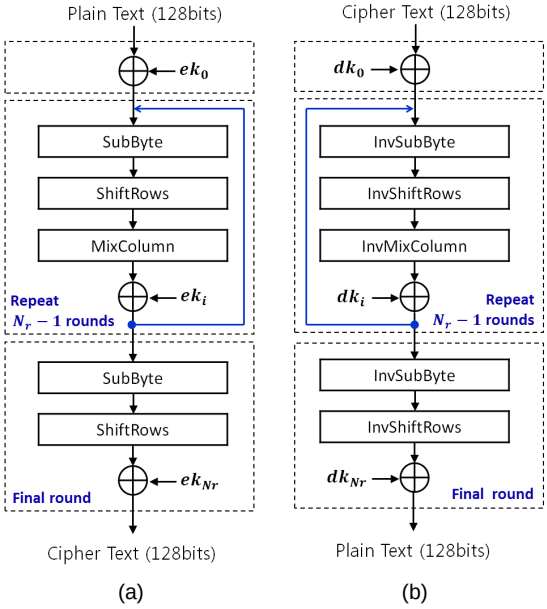


Fig. 4 Encryption and decryption of AES block cipher (a) encryption, (b) decryption

inverse)을 구하는 $x \rightarrow x^{-1}$ 매핑과 $GF(2^8)$ 상에서 어파인(affine) 변환으로 구현될 수 있다. ShiftRow 변환은 state의 행 위치에 따라 0~3까지의 오프셋으로 바이트 순환이동으로 구현된다. MixColumn 변환은 state의 행을 $GF(2^8)$ 상의 다항식으로 취급하여 상수 행렬과의 곱셈 연산으로 구현된다.

2.3. ARIA와 AES 블록암호의 비교

ARIA와 AES 블록암호는 블록 길이와 키 길이가 동일하고, non-Feistel SPN 구조를 기반으로 하여 알고리듬 측면에서 여러 가지 유사성을 갖는다. 따라서 두 알고리듬을 통합하여 단일 회로로 구현할 수 있으며, 자원공유를 통해 저면적, 저전력 구현이 가능하다.

두 알고리듬의 차이점으로는, ARIA는 ISPN 구조를 기반으로 하여 암호화와 복호화 과정이 동일하며, 라운드 변환에 동일한 변환함수가 사용된다. 반면에, SPN 구조 기반으로 하는 AES는 암호화와 복호화 과정이 역순이며, 라운드 변환에 역변환 함수가 사용된다. 또한, 두 알고리듬은 키 길이에 따른 라운드 회수가 다르고, AES의 라운드 변환에는 ShiftRow와 InvShiftRow 연산이 포함되어 있는 차이점이 있다.

두 알고리듬의 공통점으로는, 블록길이와 키길이가 동일하며, 또한 S-box를 정의하는 유한체와 기약다항식(irreducible polynomial)이 동일하다. ARIA에 사용되는 S-box S_1은 AES에 사용되는 S-box와 동일하며, S-box S_1, S_2는 유한체 $GF(2^8)$ 상의 역원 연산과 affine 변환으로 구현될 수 있다. AES의 확산계층은 암호화와 복호화에 서로 다른 4×4 행렬 곱셈으로 구성되며, 이를 위해 $GF(2^8)$ 상의 덧셈과 곱셈이 사용된다. 반면에 ARIA의 확산계층은 암호화와 복호화에 동일하게 하나의 이진 행렬 곱셈이 사용된다. ARIA와 AES의 확산 행렬 수식에 공통으로 존재하는 항을 분리해 내는 방법을 통해 하드웨어 자원을 공유시킬 수 있다.

Ⅲ. ARIA-AES 통합 프로세서 설계

3.1. 전체 구조

ARIA와 AES 블록암호를 선택적으로 지원하는 통합 ARIA-AES 프로세서(UAAP)를 설계하였다. UAAP는 ARIA와 AES의 암호(복호) 기본 기능과 함께 4가지 운영모드(ECB, CBC, OFB, CTR)와 2가지 마스터키 길이(128-비트, 256-비트)를 지원하도록 설계되었다. 전체 구조는 그림 5와 같으며, 통합 ARIA-AES crypto-core (UAACC)와 운영모드 동작에 사용되는 두 개의 128-비트 레지스터(IV_reg , op_reg) 및 XOR 게이트 등으로 구성된다. 256-비트의 암호키 입력포트, 128-비트의 평문(암호문) 및 초기화 벡터(initial vector) 입력포트, 그리고 128-비트의 평문(암호문) 출력포트를 갖는다.

UAACC는 ARIA와 AES의 암호・복호 기능을 단일 회로로 통합하여 그림 6의 구조로 구현되었다. ARIA와 AES의 라운드 변환을 처리하는 통합 라운드 변환 블록(URnd), 라운드키를 생성하는 통합 라운드키 생성 블록(KeyGen) 그리고 제어 블록으로 구성된다.

ARIA-128, 256 모드의 라운드 변환에는 각각 13, 17

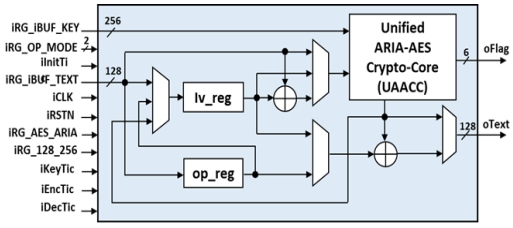


Fig. 5 Architecture of unified ARIA-AES processor(UAAP)

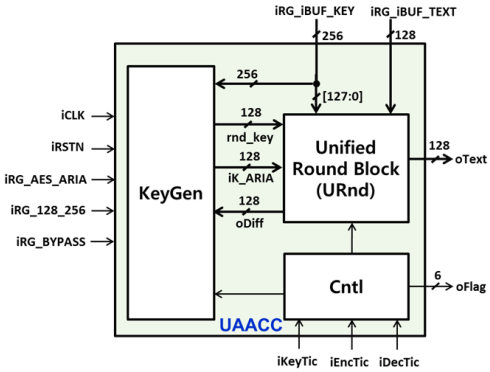


Fig. 6 Unified ARIA-AES crypto-core(UAACC)

클록 사이클이 소요된다. ARIA 블록암호의 라운드키 스케줄링은 키 초기화 과정과 키 확장의 두 단계로 이루어지며, 키 초기화 과정에는 라운드 변환 함수가 사용된다. 본 설계에서는 그림 7의 통합 라운드 변환 블록을 사용하여 키 초기화 연산이 이루어지도록 하였다. AES-128, 256 모드의 경우에는 키 초기화에 각각 10, 14 클록 사이클이 소요된다. AES 복호화 라운드키는 암호화 연산의 역순으로 사용되므로, 암호화 연산의 마지막 라운드키를 생성하여 내부에 저장하기 위한 과정이다. AES-128, 256 모드의 라운드 변환에는 각각 11, 15 클록 사이클이 소요된다.

3.2.통합 라운드 변환 블록

통합 라운드 변환 블록(URnd)은 ARIA와 AES의 라운드 변환과 ARIA의 키 초기화 연산을 수행한다. 두 블록암호의 라운드 변환을 구성하는 치환계층과 확산계층에 자원공유 기법을 적용하여 그림 7과 같이 설계하였다. 라운드 연산의 중간 결과를 저장하는 128-비트 상태 레지스터(rState), ARIA와 AES의 치환계층 연산을 선택적으로 수행하는 통합 치환연산 블록(USbox_128), 두 블록암호의 확산계층 연산을 선택적으로 수행하는 통합 확산연산 블록(Udl_mc), AES 라운드 변환에서 바이트 단위의 순환이동을 수행하는 순환시프트 블록(shift_ row), 그리고 라운드키 가산과 ARIA의 키 초기화 과정에서 사용되는 XOR 게이트 등으로 구성된다.

ARIA 모드에서는 중간결과 레지스터 rState에 저장된 평문(암호문)이 라운드키와 가산되고 USbox_128 블록과 Udl_mc 블록을 통해 치환계층과 확산계층 연산이 이루어지고, 그 결과가 다시 rState에 저장된다. ARIA

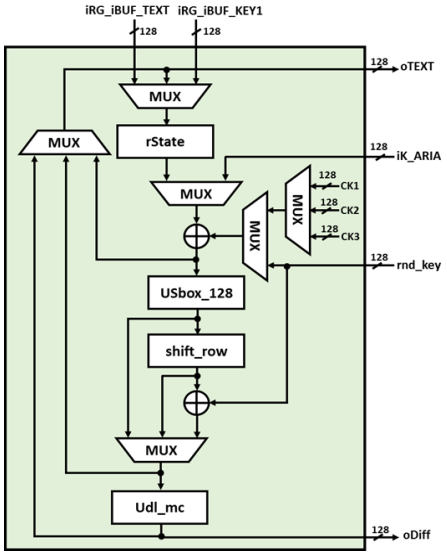


Fig. 7 Unified round block(URnd)

블록암호는 ISPN 구조를 기반으로 하므로, 암호화와 복호화의 연산이 동일한 과정으로 이루어진다. AES 암호화 모드의 경우, 레지스터 rState에 저장된 평문이 라운드키와 가산되고, USbox_128, shift_row, Udl_mc를 순차적으로 거쳐 그 결과가 다시 rState에 저장된다. 복호화에서는 rState에 저장된 암호문이 USbox_128, shift_row, Udl_ mc를 순차적으로 거친 후, 라운드키와 가산되어 그 결과가 다시 rState에 저장된다.

3.2.1.통합 치환연산 블록

ARIA와 AES의 치환계층을 구성하는 S-box는 동일한 유한체 $GF(2^8)$를 사용한다. ARIA에서 사용되는 S-box S_1은 AES의 S-box와 동일하며, ARIA의 S-box S_1과 S_2는 유한체 $GF(2^8)$상의 역원 연산과 affine 변환으로 구현될 수 있다. 이와 같은 두 알고리듬의 치환계층의 유사성을 이용하면, 하드웨어 공유를 통해 저면적의 효율적인 하드웨어 구현이 가능하다. 본 설계에서는 두 블록암호의 치환계층 연산을 단일 회로로 통합하여 설계하였으며, LUT 구현 대신에 $GF(2^8)$상의 곱의 역원 연산 회로를 이용하여 구현하였다.

ARIA-AES 통합 치환연산 블록(USbox_128)은 그림 8의 구조로 구현되었다. ARIA의 홀수 라운드와 AES의 암호·복호 연산의 경우에는 128-비트 데이터가 32-비트씩 나뉘어 4개의 USbox_32 블록에 입력되어 연산된다.

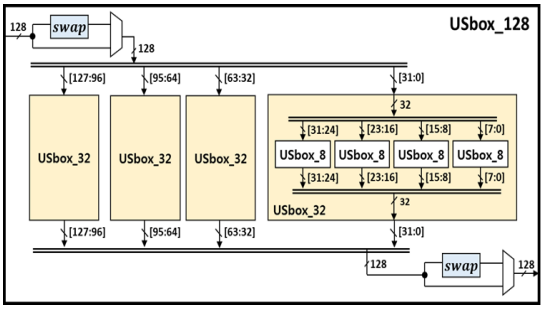


Fig. 8 Unified substitution block(USbox_128)

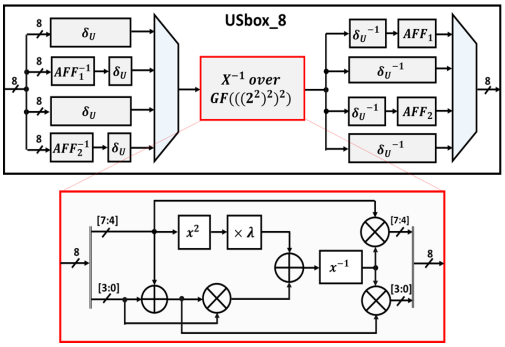


Fig. 9 Unified S-box(USbox_8) using multiplicative inverse over composite field $GF(((2^2)^2)^2)$

ARIA의 짝수 라운드에서는 128-비트 입력이 32-비트씩 나뉘어 swap 블록을 거친 후, 4개의 USbox_32 블록에 입력되어 연산되고, 그 결과가 다시 swap 블록을 거쳐 출력된다. swap 블록 블록은 128-비트의 입력을 4개의 32-비트 워드로 분할하고, 각각의 32-비트 워드에 대해 상위 2-바이트와 하위 2-바이트의 위치를 교환하는 기능을 수행한다. 이와 같이 swap 블록을 사용하면 ARIA 블록암호의 홀수 라운드에 사용되는 치환계층 유형-1과 짝수 라운드에 사용되는 치환계층 유형-2를 단일 회로로 구현할 수 있다. USbox_32 블록은 4개의 USbox_8 블록으로 구성된다.

ARIA와 AES에서 사용되는 두 종류의 S-box S_1, S_2와 그 역원 S_1^{-1}, S_2^{-1}는 $GF(2^8)$ 상의 역원 연산과 affine 변환으로 구현될 수 있다. 본 논문에서는 $GF(2^8)$ 상의 역원 연산 기능을 공유하면서 S_1, S_1^{-1}, S_2, S_2^{-1}의 기능을 선택적으로 수행하도록 USbox_8 블록을 그림 9와 같이 설계하였다. AFF_1과 AFF_2는 각각 S-box S_1과 S_2의 affine 변환을 나타내고, AFF_1^{-1}과 AFF_2^{-1}는 각각 S_1^{-1}과 S_2^{-1}의 affine 변환을 나타낸다.

$GF(2^8)$ 상의 곱의 역원은 다항식 기저(polynomial basis)를 사용하여 복합체(composite field) $GF(((2^2)^2)^2)$ 상의 곱의 역원 연산회로로 구현하였다. $GF(((2^2)^2)^2)$ 상의 곱의 역원은 그림 9와 같이 유한체 곱셈기($\otimes$) 3개와 $GF(2^4)$상의 곱의 역원회로(x^{-1}), 제곱(x^2) 및 XOR 연산으로 구현된다. $GF(2^4)$ 상의 곱의 역원인 x^{-1} 연산은 LUT 방식으로 구현하였다.

3.2.2.통합 확산연산 블록

AES의 확산 계층에는 암호화에 MixColumn 연산이 사용되고, 복호화에는 역변환인 InvMixColumn 연산이 사용된다. AES의 MixColumn 연산과 InvMixColumn 연산은 바이트의 4×4 행렬 곱셈으로 표현되며, $GF(2^8)$ 상의 덧셈과 곱셈을 수반한다. ARIA 블록암호의 확산 계층에는 involution 이진 행렬이 사용된다. AES와 ARIA의 확산 행렬에 포함되어 있는 공통항을 찾아 하드웨어를 공유시킴으로써 효율적인 통합 확산연산 회로를 구현할 수 있다.

통합 확산연산 회로(Udl_mc)는 그림 10의 구조로 설계되었으며, ARIA와 AES의 확산함수에 공통으로 사용되는 XOR 블록, ARIA 확산연산 회로(ARIA-Diff) 그리고 AES 확산연산 회로(AES-Diff)로 구성된다. AES의 복호화 확산함수 InvMixColumn는 암호화 확산함수인 MixColumn를 포함하므로, 자원공유를 이용하여 효율적으로 구현될 수 있다[7].

3.2.3. 순환시프트 블록

AES 블록암호의 라운드 변환에 사용되는 순환시프트 연산은 state의 값을 변경시키지 않으면서 state 행의 위치에 따라 0~3까지의 오프셋으로 바이트들을 순환

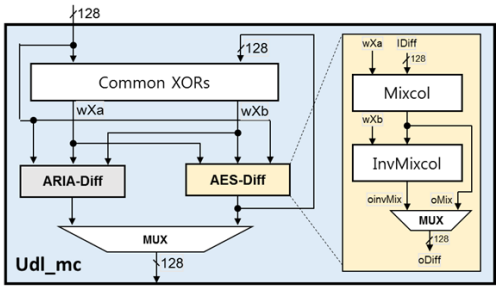


Fig. 10 Unified diffusion block(Udl_mc)

이동시킨다. 순환시프트 블록은 암호화 연산에서는 바이트 단위의 왼쪽 순환이동 동작하고, 복호화 연산에서는 오른쪽 순환이동 동작을 수행하도록 설계되었다.

Ⅳ. FPGA 구현 검증

설계된 ARIA-AES 통합 암호 프로세서 UAAP는 그림 11과 같이 FPGA 보드, UART 인터페이스, PC, 구동 소프트웨어로 구성되는 검증 시스템을 통해 하드웨어 동작을 검증하였으며, Virtex5 XC5VSX-95T FPGA 디바이스가 사용되었다. PC와 FPGA 사이의 데이터 송수신은 RS232C를 통해 이루어진다. PC에서 FPGA로 전송된 평문(암호문) 데이터는 설계된 UAAP로 입력되어 128-비트 블록 단위로 암호 및 복호화가 이루어진다. UAAP에서 출력되는 암호문(평문)은 PC로 전송되어 화면에 표시된다.

그림 12는 FPGA 검증 결과를 보이고 있다. 그림 12-(a),(b)에서 좌측의 원본 이미지를 FPGA로 전송하여 UAAP에서 암호화한 결과는 중앙의 이미지와 같다. 그림 12-(a)의 중앙의 이미지는 ECB 모드로 암호화한 결과이며, 원본 이미지가 암호화 되었지만 윤곽이 드러나는 것을 볼 수 있다. 이는 ECB 모드의 경우 동일한 평문을 암호화하면 동일한 암호문이 출력되는 특성 때문이다. 그림 12-(b)의 중앙의 이미지는 동일한 원본 이미지를 CBC 모드로 암호화한 결과이다. 원본 이미지가 랜덤 값으로 암호화되었음을 확인할 수 있다. CBC 모드에서는 이전 블록의 암호화 결과가 다음 블록의 암호화에 사용되므로, 동일한 평문을 암호화 하더라도 동일한 암호문이 출력되지 않기 때문이다.

그림 12의 중앙에 암호화된 이미지를 다시 FPGA로 전송하여 복호화한 결과는 우측의 이미지와 같으며, 암호화에 사용된 원본 이미지가 복원되었음을 확인할 수 있다. FPGA 검증결과에서 볼 수 있듯이, 이미지를 암호화하고 암호화된 이미지를 복호하여 원래 이미지와 일치하는 결과가 출력되었으므로, 설계된 ARIA-AES 통합 암호 프로세서가 정상 동작함을 확인하였다.

설계된 UAAP의 특성을 요약하면 표 1과 같다. 0.18 ㎛ CMOS 표준 셀 라이브러리로 합성한 결과, 최대 95 MHz의 클록 주파수로 동작 가능한 것으로 평가되었다. 80 MHz의 주파수로 합성한 결과, 두 가지 키길이를 지원하며 암호/복호를 수행하는 UAACC는 49,688 GE로

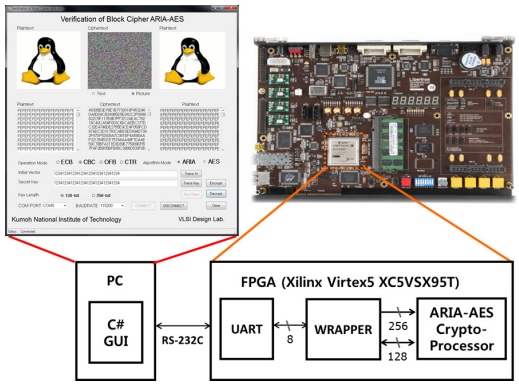
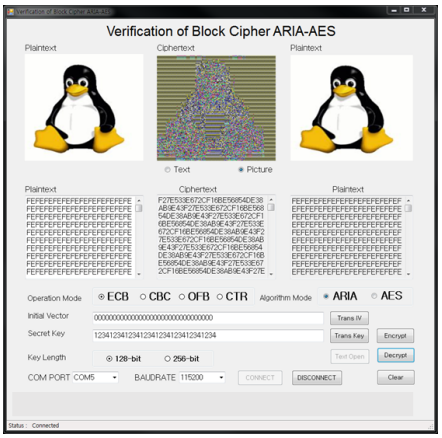
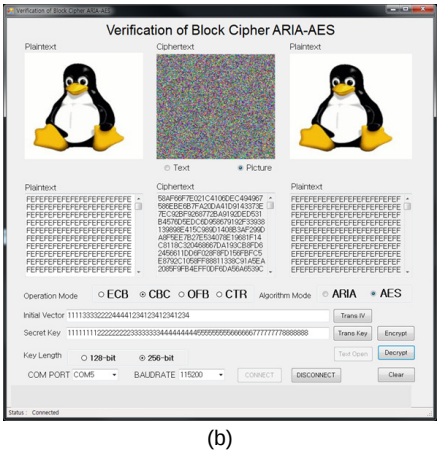


Fig. 11 FPGA Verification setup



(a)



(b)

Fig. 12 FPGA verification results of unified ARIA-AES processor (a) ARIA-ECB mode (b) AES-CBC mode

Table. 1 Summary of unified ARIA-AES processor(UAAP)

Key length [bits]	128-b, 256-b	
Modes of operation	ECB, CBC, OFB, CTR	
Cycles per block [cycles]	ARIA	128-b key: 13
		256-b key: 17
	AES	128-b key: 11
		256-b key: 15
Area @80 MHz [GE]	UAACC	49,688
	Mode operation	4,970
	UAAP (Total)	54,658
Throughput @80 MHz [Mbps]	ARIA	128-b key: 787
		256-b key: 602
	AES	128-b key: 930
		256-b key: 682
Max. clock freq. [MHz]	95 MHz	

구현되었고, 네 가지 운영모드를 지원하는 회로는 약 4,970 GE로 구현되었다. 전체 UAAP는 54,658 GE로 구현되었다. 설계된 UAAP의 연산 성능은 80 MHz 동작 주파수에서 키 길이(128-비트, 256-비트)에 따라 ARIA 모드에서는 787 Mbps, 602 Mbps, 그리고 AES 모드에서는 930 Mbps, 682 Mbps로 평가되었다.

표 2는 본 논문의 ARIA-AES 통합 암호 프로세서와 문헌에 발표된 ARIA 및 AES 프로세서 사례를 비교한 것이다. 지원되는 블록암호 표준, 키 길이, 운영모드, 데이터 패스 그리고 키 레지스터 포함 여부 등의 세부조건이 상이하여 직접적인 비교는 어렵다. 문헌 [10]의 사례는 ARIA와 AES의 통합 구현이라는 점에서 유사하지만, 128-비트 키 길이와 기본 ECB 운영모드만 지원한다. 본 논문의 UAAP는 128-비트와 256-비트의 두 가지 키 길이를 지원하며, 기본 ECB 운영모드 외에 CBC, CTR, OFB 운영모드를 추가적으로 지원하여 블록암호의 기밀성을 향상시켜 실용성을 높인 점이 장점이다.

표 2에 제시된 AES, ARIA의 독립적인 구현한 사례 [7, 8]을 참조하면, 하드웨어 공유를 통해 감소된 게이트 수를 간접적으로 평가할 수 있다. 문헌 [7]의 AES 프로세서는 32 비트 데이터 패스로 설계되었으므로, 128 비트 데이터 패스로 환산하면 대략 50,000 GE 정도가 소요될 것으로 예측되며, 128 비트 데이터 패스와 4가지 운영모드를 구현한 문헌 [8]의 ARIA 프로세서는 46,100 GE 이므로, 본 논문의 ARIA-AES 통합 프로세서는 하드웨어 공유로 대략 45,000 GE (50%)의 게이트 수가 절약된 것으로 평가된다.

Ⅴ. 결 론

우리나라 블록암호 표준인 ARIA와 미국 표준인 AES를 단일 하드웨어 구조로 통합하여 설계하고, FPGA 구현을 통해 하드웨어 동작을 검증하였다. 두 알고리듬의 공통 특성을 기반으로 자원공유 기법을 적용하여 저면적, 저전력으로 구현했다. 4가지 운영모드와 2가지 키길이를 지원하도록 설계된 ARIA-AES 통합 암호 프로세서는 0.18㎛ CMOS 공정에서 54,658 GE로 구현되었으며, 최대 95 MHz의 클록 주파수로 동작 가능하다. 80 MHz 클록 주파수로 동작하는 경우에, ARIA 모드에서 128-비트, 256-비트의 키길이에 따라 787 Mbps, 602 Mbps의 처리율을 갖는다. AES 모드에서는 128-비트, 256-비트의 키길이에 따라 930 Mbps, 682 Mbps의 처리율을 갖는다. ARIA-AES 이중표준 지원

Table. 2 Comparison of ARIA-AES cryptographic processors

	This paper	[7]	[8]	[9]	[10]
Algorithms supported	ARIA, AES	AES	ARIA	ARIA	ARIA, AES
Key length supported [bits]	128, 256	128, 192, 256	128, 192, 256	128	128
Modes of operation	ECB, CBC, OFB, CTR	ECB	ECB, CBC, OFB, CTR	ECB	ECB
Bit width of datapath [bits]	128	32	128	32	128
Cycles for processing a block [cycles]	AES(128/256): 11/15 ARIA(128/256): 13/17	50/60/70	16	356	AES-Enc, Dec: 11, 21 ARIA: 16
Max. frequency [MHz]	95	220	200	71	90
Area [GE]	54,658	25,000	46,100	13,893	19,056
Throughput [Mbps]	AES(128/256): 930/682 ARIA(128/256): 787/602	520	1,280	25	1,047/548/720
Technology [um]	0.18	0.35	0.13	0.35	0.25

암호 프로세서는 하드웨어 경량화와 저전력을 특징으로 가져 IoT, RFID 환경과 같이 제한된 자원을 갖는 응용분야의 정보보호 SoC 설계에 활용될 수 있다.

ACKNOWLEDGMENTS

- This paper was supported by Kumoh National Institute of Technology.
- Authors are thankful to IDEC for EDA software support.

REFERENCES

[1] J.S. Kumar and D.R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20-26, Mar. 2014.

[2] FIPS PUB 197, *Advanced Encryption Standard (AES)*, National Institute of Standard and Technology (NIST), Nov. 2001.

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

[4] TTA std. TTAK.KO-12.0223, *128-Bit Block Cipher LEA*, Telecommunications Technology Association, 2013.

[5] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[6] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, Jan. 1987.

[7] H.K. Ahn and K.W. Shin, "AES-128/192/256 Rijndael Cryptoprocessor with On-the-fly Key Scheduler," *Journal of The Korea Institute of Information and Communication Engineering*, vol. 39-SD, no. 11, pp. 961-971, Nov. 2002.

[8] D.H. Kim and K.W. Shin, "An Efficient Hardware Implementation of ARIA Block Cipher Algorithm Supporting Four Modes of Operation and Three Master Key Lengths," *Journal of The Korea Institute of Information and Communication Engineering*, vol. 16, no. 11, pp. 2517- 2524, Nov. 2012.

[9] J. Park et al., "Low Power Compact Design of ARIA Block Cipher," *Proceedings of International Symposium on Circuits and Systems*, pp. 313-316, May 2006.

[10] B. Koo et al., "Design of an Efficient AES-ARIA Processor using Resource Sharing Technique," *Journal of The Korea Institute of Information Security and Cryptology*, vol.18, no. 6A, pp. 39-49, Dec. 2008.

김기쁨(Ki-Bbeum Kim)

2016년 2월 금오공과대학교 전자공학부(공학사)
2016년 3월~현재 금오공과대학교 전자공학과 석사과정 재학 중
※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