ISSN:1226-7244 (Print)
ISSN:2288-243X (Online)
논문번호 18-01-06
38
j.inst.Korean.electr.electron.eng.Vol.22,No.1,38~45,March 2018
http://dx.doi.org/10.7471/ikeee.2018.22.1.38

ARIA/AES 블록암호와 Whirlpool 해시함수를 지원하는 통합 크립토 프로세서 설계

An Integrated Cryptographic Processor Supporting ARIA/AES Block Ciphers and Whirlpool Hash Function

김 기 쁨* , 신 경 욱**★

Ki-Bbeum Kim* , Kyung-Wook Shin**★

Abstract

An integrated cryptographic processor that efficiently integrates ARIA, AES block ciphers and Whirlpool hash function into a single hardware architecture is described. Based on the algorithm characteristics of ARIA, AES, and Whirlpool, we optimized the design so that the hardware resources of the substitution layer and the diffusion layer were shared. The round block was designed to operate in a time-division manner for the round transformation and the round key expansion of the Whirlpool hash, resulting in a lightweight hardware implementation. The hardware operation of the integrated ARIA-AES-Whirlpool crypto-processor was verified by Virtex5 FPGA implementation, and it occupied 68,531 gate equivalents (GEs) with a 0.18um CMOS cell library. When operating at 80 MHz clock frequency, it was estimated that the throughputs of ARIA, AES block ciphers, and Whirlpool hash were 602~787 Mbps, 682~930 Mbps, and 512 Mbps, respectively.

요 약

ARIA, AES 블록암호와 Whirlpool 해시함수를 단일 하드웨어 구조로 통합하여 효율적으로 구현한 크립토 프로세서에 대해 기술한다. ARIA, AES, Whirlpool의 알고리듬 특성을 기반으로 치환계층과 확산계층의 하드웨어 자원이 공유되도록 설계를 최적화하였다. Whirlpool 해시의 라운드 변환과 라운드 키 확장을 위해 라운드 블록이 시분할 방식으로 동작하도록 설계하였으며, 이를 통해 하드웨어 경량화를 이루었다. ARIA-AES-Whirlpool 통합 크립토 프로세서는 Virtex5 FPGA에 구현하여 하드웨어 동작을 검증하였으며, 0.18㎛ CMOS 셀 라이브러리로 합성한 결과 68,531 GE로 구현되었다. 80 MHz 클록 주파수로 동작하는 경우에, ARIA, AES 블록암호는 각각 602~787 Mbps, 682~930 Mbps, 그리고 Whirpool 해시는 512 Mbps의 성능을 갖는 것으로 예측되었다.

Key words : ARIA, AES, Whirlpool, block cipher, hash function, cryptographic processor

---

* Pixelplus Inc.,
** School of Electronic Engineering, Kumoh National Institute of Technology
★ Corresponding author
E-mail:kwshin@kumoh.ac.kr, Tel:+82-54-478-7427

※ Acknowledgment
・This work was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(No. 2017R1D1A3B03031677)
・This work was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korean government (Ministry of Trade, Industry & Energy, HRD Program for Software-SoC convergence) (No. N0001883)
・Authors are thankful to IDEC for supporting EDA software.
Manuscript received Mar. 8, 2018; revised Mar. 13, 2018 ; accepted Mar. 14, 2018
This is an Open-Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Ⅰ. 서론

사물인터넷 (Internet of Things) 기술을 기반으로 하는 다양한 융합 서비스들이 활성화됨에 따라 보안 위협에 대응할 수 있는 정보보안 기술의 중요성이 부각되고 있다. 특히, RFID, 무선 센서 네트워크 (WSN)와 같이 제한된 가용 자원을 갖는 응용분야의 정보보안을 위해서는 대칭키 (symmetric key) 암호와 해시 (hash) 함수 기반의 경량 하드웨어 보안 솔루션이 필요하다.[1,2]

IoT 디바이스는 주로 Wi-Fi, 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), 지그비 (ZigBee), LoRa 등의 규격에 의해 무선 네트워크로 연결되며, 이러한 프로토콜에서 기밀성 (confidentiality), 무결성 (integrity), 디바이스 간 인증 (authentication)이 필수적으로 요구된다. 연산 성능, 메모리 크기, 소비전력 등의 제약을 갖는 IoT 단말이나 WSN 노드에서는 암호 모듈의 경량화 및 저전력이 핵심요소가 되며, 이들 플랫폼에 최적화된 크립토 코어가 필요하다.

정보보안의 가장 기본적인 요소는 인가된 (비밀키를 가지고 있는) 사용자만 내용을 확인할 수 있도록 정보를 암호화하는 기밀성이며, 이를 위해 대칭키 방식의 블록암호가 사용된다. 널리 사용되는 대칭키 암호로는 AES (Advanced Encryption Standard)[3], ARIA (Academy, Research Institute, Agency)[4], LEA (Lightweight Encryption Algorithm)[5] 등이 있다. 정보보안의 또 다른 핵심 요소는 제3자에 의해 정보가 변경, 조작되지 않았음을 확인할 수 있도록 정보의 무결성을 검증하거나, 디바이스 간 인증을 통해 정당한 사용자만 접근할 수 있도록 하는 것이다. 이와 같은 무결성, 인증을 위해 해시함수가 사용되며, 대표적인 해시 알고리듬은 미국 국립표준기술연구소 (NIST)에 의해 개발된 SHA-2[6], 블록암호를 압축함수로 사용하는 Whirlpool[7] 등이 있다.

본 논문에서는 IoT, WSN을 비롯한 다양한 분야의 정보보안 시스템의 하드웨어 구현에 핵심 IP (Intellectual Property)로 사용될 수 있도록 대표적인 블록암호 표준 AES와 ARIA 알고리듬, 그리고 해시함수 Whirlpool을 통합하여 경량 하드웨어로 구현하였다. AES는 국제 표준으로 채택되어 정보보안 분야에서 널리 사용되고 있으며, ARIA는 국내 표준으로 정부기관 등 국내에서 상용화되는 제품에 인증이 요구된다. Whirlpool 해시함수는 국내 해시함수 표준으로 채택된 SHA-256에 준한 보안 성능을 갖는 것으로 평가되며, 우리나라 해시함수 이용지침[8]에는 Whirlpool을 SHA-2와 더불어 메시지의 무결성 검증을 위한 전자서명에 이용하도록 명시하고 있다.

본 논문에서는 블록암호 ARIA, AES와 해시함수 Whirlpool의 알고리듬 특성을 토대로 단일 하드웨어로 통합하여 구현한 ARIA-AES-Whirlpool (AAW) 크립토 프로세서를 설계하였으며, 자원공유 기법을 적용하여 하드웨어 최적화를 이루었다. 정보의 기밀성을 제공하는 ARIA, AES 블록암호와 무결성, 인증을 제공하는 Whirlpool 해시함수를 동시에 지원하므로 다양한 분야에 응용이 가능하다. Ⅱ장에서는 블록암호 및 해시함수 알고리듬에 대해 간략히 소개하고, Ⅲ장에서는 AAW 통합 크립토 프로세서 설계에 대해 설명한다. 설계된 회로의 FPGA 검증 및 성능평가 결과를 Ⅳ장에서 기술하고, Ⅴ장에서 결론을 맺는다.

Ⅱ. ARIA, AES 블록암호 및 Whirlpool 해시

ARIA [4] 는 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.

AES [3]는 2001년도 NIST에 의해 표준으로 제정된 대칭키 방식의 블록암호 알고리듬이며, non-Feistel SPN 구조를 갖는다. AES는 128-비트의 평문(암호문)을 암호(복호)하여 동일한 길이의 암호문(평문)을 만들며, 128, 192, 256비트의 세 가지 키 길이에 따라 10, 12, 14회의 라운드 변환을 수행한다.

Whirlpool [7] 해시함수는 AES를 고안한 Vincent Rijmen과 Paulo Barreto에 의해 제안되었으며, ISO/IEC 10118-3 표준으로 채택되었다. Whirlpool 해시함수는 Miyaguchi-Preneel 구조를 특징으로 하여 2^{256} 비트 미만 길이의 평문을 입력받아 512 비트의 메시지 다이제스트를 생성한다. 압축함수로는 AES와 유사한 Non-Feistel SPN 구조의 블록암호가 사용된다.

표 1은 블록암호 ARIA, AES와 Whirlpool 해시 함수의 알고리듬 특성을 비교한 것이며, 알고리듬 측면에서 여러 가지 유사성이 있음을 알 수 있다. 블록암호 ARIA와 AES 그리고 Whirlpool 해시의 압축 함수로 사용되는 블록암호는 모두 Non-Feistel SPN 구조를 기반으로 하는 공통점을 갖는다. ARIA와 AES는 동일한 블록 길이와 키 길이를 지원하며, Whirlpool의 압축 함수는 블록 길이와 키 길이가 모두 512 비트이다.

ARIA와 AES의 차이점으로는, ARIA는 ISPN 구조를 기반으로 하여 암호화와 복호화 과정이 동일하며, 라운드 변환에 동일한 변환함수가 사용된다. 반면에, AES는 SPN 구조 기반이므로 암호화와 복호화 과정이 역순이며, 또한 라운드 변환에 역변환 함수가 사용된다. Whirlpool 해시 함수의 경우, 전체 구조는 Miyaguchi-Prineel 구조를 기반으로 하지만 압축함수로 사용되는 블록암호는 SPN 구조를 기반으로 한다.

ARIA와 AES의 가장 큰 공통점으로는 S-box를 정의하는 유한체가 동일하며, 또한 동일한 기약다항식(irreducible polynomial)을 사용한다는 점이다. ARIA에 사용되는 S-box S_1은 AES의 S-box와 동일하며, 또한 S-box S_1과 S_2는 유한체 $GF(2^8)$ 상의 역원 연산과 아핀 (affine) 변환으로 구현될 수 있다. ARIA의 확산계층은 암호화 연산과 복호화 연산에 동일하게 하나의 이진 행렬곱셈이 적용되고, AES의 확산계층은 암호화와 복호화에 서로 다른 4×4 행렬곱셈이 사용되며, Whirlpool에서는 8×8 행렬 곱셈으로 구성된다. ARIA, AES, Whirlpool의 확산 행렬 수식에 공통으로 존재하는 항들을 분리해 내는 방법을 통해 일부 하드웨어 자원을 공유시킬 수 있다.

Table. 1. Comparison of ARIA, AES and Whirlpool.
표 1. ARIA, AES 및 Whirlpool 비교

	ARIA	AES	Whirlpool
Structure	ISPN	SPN	Miyaguchi-Prineel (SPN)
Block lengths(bit)	128		512
Key lengths(bit)	128/192/256		512
Number of rounds	12/14/16	10/12/14	10
Irreducible polynomial	$x^8+x^4+x^3+x+1$		$x^8+x^4+x^3+x^2+1$
Key extension	Key extension algorithm		Round function
Round functions	AddRoundKey		
	SubstLayer ($x\rightarrow x^{-1}$, $x^{247}\rightarrow x^{-1}$)	SubBytes ($x\rightarrow x^{-1}$)	SubBytes (4 x 4 mini S-box)
	-	ShiftRow	ShiftColumn
	DiffLayer (16 x 16 binary matrix)	MixColumn (4×4 circulant matrix)	Mixrow (8×8 circulant matrix)

III ARIA-AES-Whirlpool 통합 크립토 프로세서 설계

블록암호 국내 표준인 ARIA와 국제 표준인 AES 그리고 해시함수 국제 표준인 Whirlpool의 알고리듬 특성을 토대로 블록암호와 해시함수를 단일 하드웨어로 통합한 ARIA-AES-Whirlpool (AAW) 크립토 프로세서를 구현하였다. AAW 크립토 프로세서는 128 비트와 256 비트의 두 가지 키 길이를 지원하며, 192 비트 키 길이는 잘 사용되지 않으므로, 키 스케줄러의 간소화를 위해 지원하지 않도록 하였다. 내부에 키 스케줄러를 포함하고 있어 평문/암호문 블록의 연속적인 암호·복호 및 해시함수 동작이 가능하다.

1. AAW 크립토 프로세서의 구조

AAW 크립토 프로세서의 전체 구조는 그림 1과 같으며, 가변 길이의 입력 메시지를 512-비트의 고정 길이로 분할하여 처리하기 위해 메시지를 패딩 (padding) 처리하는 메시지 패더 블록 (Mpad), 통합 키 생성 블록 (Key_gen), 세 가지 알고리듬의 라운드 연산을 수행하는 통합 라운드 블록 (Rnd_AAW) 및 제어블록으로 구성된다.

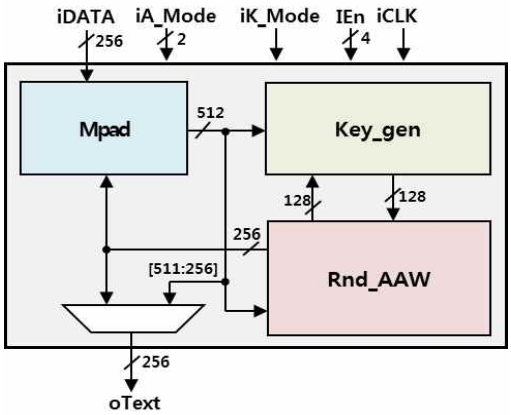


Fig. 1. Architecture of integrated ARIA-AES-Whirlpool (AAW) crypto-processor.
그림 1. ARIA-AES-Whirlpool (AAW) 통합 크립토 프로세서의 구조

AAW 크립토 프로세서는 제어신호에 따라 블록암호 ARIA, AES의 두 가지 마스터키 길이(128 비트, 256 비트)와 암호·복호, 그리고 Whirlpool 해시함수를 선택적으로 수행한다. 256 비트의 입력포트 iDATA를 통해 ARIA, AES의 마스터 키, 평문(암호문) 및 Whirlpool의 메시지 길이, 메시지 데이터가 입력된다. 256 비트의 출력포트 oText를 통해 ARIA, AES의 암호문(평문) 및 Whirlpool 해시의 메시지 다이제스트가 출력된다. 내부 데이터패스는 128 비트로 설계되어 ARIA와 AES의 한 라운드 연산이 단일 클록 사이클로 처리되며, Whirlpool 해시의 한 라운드 연산은 4 클록 사이클로 처리된다.

설계된 AAW 크립토 프로세서의 알고리듬과 키 길이에 따른 소요 클록 사이클 수는 표 2와 같다. ARIA-128, ARIA-256 모드의 경우에는 키 초기화 연산에 4 클록 사이클이 소요되고, 키 길이에 따라 라운드 연산에 13, 17 클록 사이클이 소요된다. AES-128, AES-256 모드의 경우에는 키 길이에 따라서 키 생성에 각각 10, 14 클록 사이클이 소요되고, 라운드 변환에는 각각 11, 15 클록 사이클이 소요된다. Whirlpool 모드는 키 생성과 라운드 연산에 각각 40 클록 씩 총 80 클록 사이클이 소요된다. Whirlpool의 경우 키 생성 연산이 라운드 연산과 동일하므로, 본 설계에서는 라운드 함수 재사용 방식을 적용하여 라운드 연산과 키 생성이 시분할 방식으로 처리되도록 설계하였으며, 이를 통해 하드웨어를 간소화하였다.

2. 통합 라운드 블록

통합 라운드 블록은 ARIA와 AES의 라운드 변환, ARIA의 키 초기화 연산, Whirlpool의 라운드 변환 및 키 생성 연산을 수행한다. 내부 구조는 그림 2와 같으며, 128 비트의 데이터패스로 설계하였다. 매 라운드 연산의 중간 결과를 저장하는 512 비트의 상태 레지스터 (State_Reg), 치환계층 연산을 선택적으로 수행하는 통합 치환계층 블록 (AAW-Sbox), 확산계층 연산을 선택적으로 수행하는 통합 확산계층 블록 (AAW-Diff)들은 3가지 알고리듬의 특성을 기반으로 하드웨어 자원이 공유되도록 최적화하여 설계되었다. 이 외에 AES와 Whirlpool의 라운드 변환 과정에서 바이트 단위로 순환이동 연산을 수행하는 Shift-Row, Shift-Col 및 라운드 키 가산에서 사용되는 XOR 게이트, 멀티플렉서 등으로 구성된다.

Table. 2. Number of clock cycles of AAW operation mode.
표 2. AAW 동작모드의 소요 클록 사이클 수

Algorithm	Key size (bit)	Operation mode	Key generation (cycles)	Round operation (cycles)
ARIA	128	ARIA-128	4	13
	256	ARIA-256		17
AES	128	AES-128	10	11
	256	AES-256	14	15
Whirlpool	512	Whirlpool	40	40

가. 통합 치환계층 블록

통합 치환계층은 ARIA, AES의 치환 연산과 Whirlpool의 치환 연산을 선택적으로 수행한다. ARIA와 AES의 치환계층을 구성하는 S-box는 동일한 유한체 $GF(2^8)$을 기반으로 한다. ARIA에 사용되는 S-box S_1은 AES의 S-box와 동일하며, ARIA의 S-box S_1과 S_2는 유한체 $GF(2^8)$ 상의 역원 (inverse) 연산과 아핀 변환으로 구현될 수 있다. 이와 같은 두 알고리듬의 치환계층의 유사성을 이용하면, 하드웨어 공유를 통해 저면적의 효율적인 하드웨어 구현이 가능하다[9, 13].

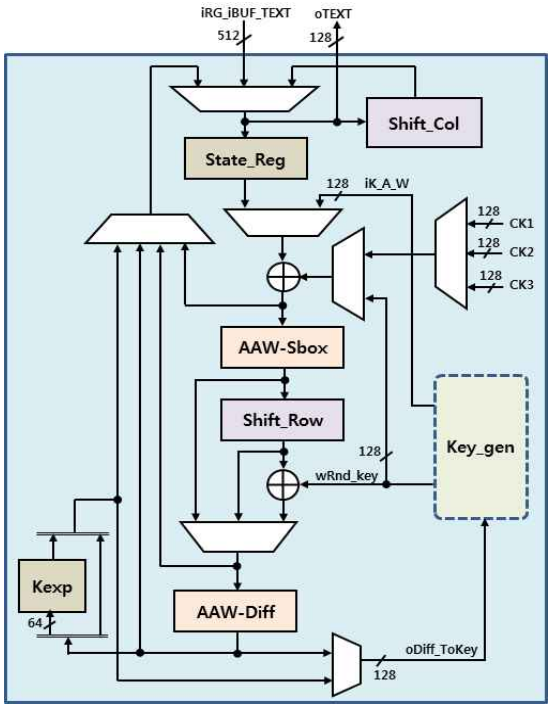
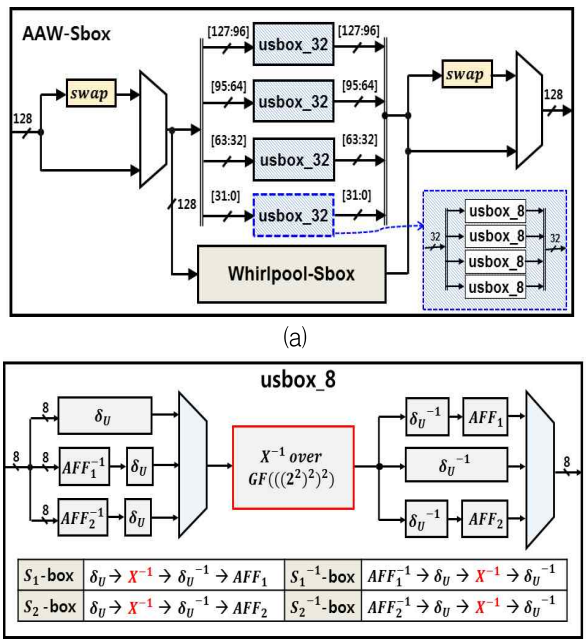


Fig. 2. Unified round block(round).
그림 2 통합 라운드 블록 (round)

본 설계에서는 ARIA와 AES의 치환계층 연산을 단일 회로로 통합하여 설계하였으며, LUT 구현 대신에 $GF(2^8)$ 상의 곱의 역원 (multiplicative inverse) 연산회로를 이용하여 구현하였다. Whirlpool의 치환계층 연산은 LUT로 구현되었다. 세 알고리듬의 치환계층을 선택적으로 수행하는 통합 치환계층 블록 (AAW-Sbox)은 그림 3-(a)의 구조를 갖는다. ARIA의 홀수 라운드와 AES의 암호·복호화 연산의 경우에는 128 비트 데이터가 32 비트 씩 나뉘어 4개의 usbox_32 블록에 입력되어 연산된다. ARIA 알고리듬의 짝수 라운드 경우에는 128 비트 입력이 32 비트씩 나뉘어 swap 블록을 거친 후, 4개의 usbox_32 블록에 입력되어 연산되고, 그 결과가 다시 swap 블록을 거쳐 출력된다. Whirlpool 연산의 경우에는 128 비트 데이터가 Whirl-Sbox로 입력되어 연산된다. ARIA와 AES에서 사용되는 두 종류의 S-box S_1, S_2와 그 역원인 S_1^{-1}, S_2^{-1}를 선택적으로 수행하는 usbox_8 블록의 구조는 그림 3-(b)와 같으며, $GF(2^8)$ 상의 역원 연산과 아핀 변환으로 구현되었다. usbox_8 블록은 $GF(2^8)$ 상의 역원 연산 기능을 공유하면서 S_1, S_1^{-1}, S_2, S_2^{-1}의 기능을 선택적으로 수행하도록 설계되었다.



(a)

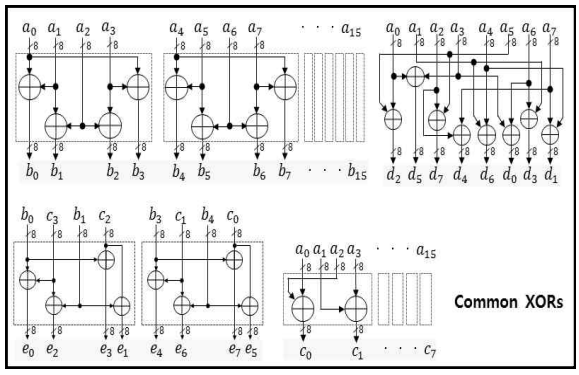
(b)

Fig. 3. Unified substitution layer (a) Unified substitution block (AAW-Sbox) (b) usbox_8 block.

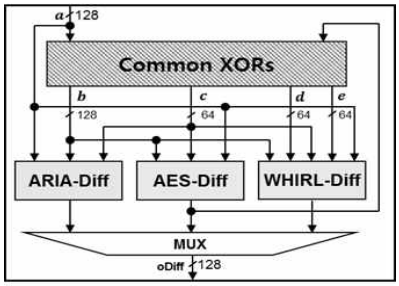
그림 3. 통합 치환계층 (a) 통합 치환 블록 (AAW-Sbox), (b) usbox_8b 블록

나. 통합 확산계층 블록

AES의 확산계층에는 암호화에 MixColumn 연산이 사용되고, 복호화에 역변환 InvMixColumn 연산이 사용된다. InvMixColumn 연산의 행렬은 MixColumn 연산의 행렬을 포함한다. AES의 MixColumn 연산과 InvMixColumn 연산은 바이트의 4×4 행렬 곱셈으로 표현되며, $GF(2^8)$ 상의 덧셈과 곱셈을 수반한다. Whirlpool의 확산계층의 연산은 8×8 행렬곱셈으로 표현되며, $GF(2^8)$상에서 기약다항식 $x^8+x^4+x^3+x^2+1$로 모듈로 곱셈연산을 수행한다. ARIA 블록암호의 확산계층에는 16×16 involution 이진 행렬이 사용된다. ARIA, AES, Whirlpool 확산계층의 회로 구현에 있어서 세 알고리듬의 확산행렬에 포함되어 있는 공통항을 찾아 하드웨어를 공유시킴으로써 효율적인 통합 확산연산 회로를 구현할 수 있다. 그림 4-(a)는 세 알고리듬의 확산행렬에 포함되어 있는 공통항의 일부를 보인 것이며, 통합 확산계층의 구조는 그림 4-(b)와 같다. 통합 확산 블록은 세 알고리듬에 공통으로 사용되는 XOR 블록, ARIA 확산 연산회로, AES 확산 연산회로, Whirlpool 확산 연산회로 등으로 구성된다.



(a)



(b)

Fig. 4. Unified diffusion layer (a) Common XORs (b) Unified diffusion block (AAW-Diff).

그림 4. 통합 확산계층 (a) 공통 XOR 항, (b) 통합 확산 블록 (AAW-Diff)

Ⅳ. FPGA 구현 검증 및 성능평가

설계된 AAW 크립토 프로세서는 그림 5와 같이 FPGA 보드, UART 인터페이스, PC, 구동 소프트웨어로 구성되는 검증 시스템을 통해 하드웨어 동작을 검증하였으며, Virtex5 XC5VSX-95T FPGA 디바이스가 사용되었다. AAW 크립토 프로세서의 FPGA 검증결과는 그림 6과 같다. 그림 6-(a)는 키 길이 128-비트의 ARIA 블록암호의 검증결과 화면이며, 좌측의 원본 이미지를 FPGA로 전송하여 AAW 크립토 프로세서에서 암호화한 결과는 중앙의 이미지와 같으며, 원본 이미지가 랜덤 값으로 암호화되었음을 확인할 수 있다. 중앙의 암호화된 이미지를 다시 FPGA로 전송하여 AAW 크립토 프로세서에서 복호화한 결과는 우측의 이미지와 같으며, 원본 이미지가 정확하게 복원되었다. 그림 6-(b)는 Whirlpool 해시함수 동작 모드의 검증결과를 보이고 있다. AAW 크립토 프로세서의 Whirlpool 함수를 통해 얻어진 메시지 다이제스트와 소프트웨어로 연산된 결과를 비교해서 일치함을 확인하였다. 이와 같은 FPGA 검증을 통해 설계된 AAW 크립토 프로세서가 하드웨어 상에서 올바르게 동작함을 확인하였다.

설계된 AAW 크립토 프로세서는 0.18㎛ CMOS 표준 셀 라이브러리로 합성한 결과, 최대 80 MHz의 클록 주파수로 동작 가능한 것으로 평가되었다. 80 MHz의 클록 주파수로 합성한 결과, 68,531 GE로 구현되었으며, Whirlpool 해시함수의 패더 블록을 제외하면 43,335 GE이다. 80 MHz 클록 주파수로 동작하는 경우에, 키 길이에 따라 ARIA 암호·복호는 787 Mbps, 602 Mbps, AES 암호·복호는 930, Mbps, 682 Mbps의 처리율을 가지며, Whirlpool 해시함수는 512 Mbps의 처리율을 갖는 것으로 평가되었다.

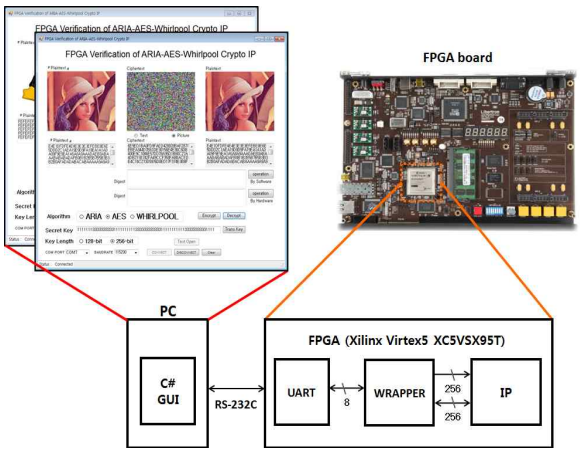


Fig. 5. FPGA Verification setup.
그림 5. FPGA 검증 시스템 구성

본 논문과 동일하게 블록암호와 해시함수를 통합하여 구현한 크립토 프로세서 사례가 없으며, 키 길이, 데이터패스 비트 수, 내부 마스터키 레지스터 포함 여부 등의 조건이 달라서 직접적인 비교는 어려우나, 본 논문의 AAW 크립토 프로세서와 문헌에 발표된 ARIA, AES, Whirlpool 프로세서 사례를 표 3에 비교하였다.

문헌 [10]의 사례는 Whirlpool 해시함수를 256 비트 데이터패스로 구현하여 약 4.9 Gbps의 높은 처리율을 가지나, 본 논문의 AAW 통합 프로세서보다 약 30% 더 많은 게이트를 필요로 하므로,

(a)

(b)

Fig. 6. FPGA verification results of integrated AAW crypto processor (a) ARIA-128 mode (b) WHIRLPOOL mode.
그림 6. AAW 통합 크립토 프로세서의 FPGA 검증 결과 (a) ARIA-128 모드 (b) WHIRLPOOL 모드

Table. 3. Comparison of ARIA-AES-Whirlpool cryptographic processors.
표 3. ARIA-AES-Whirlpool 크립토 프로세서 비교

	This paper	[10]	[11]	[12]	[13]
Algorithms supported	ARIA, AES, Whirlpool	Whirlpool	AES	ARIA	ARIA, AES
Key length supported [bits]	128, 256	512	128, 192, 256	128	128
Bit width of datapath [bits]	128	256	32	32	128
Cycles for processing a block [cycles]	AES(128/256): 11/15 ARIA(128/256): 13/17 Whirlpool: 80	21	50/60/70	356	AES-Enc/Dec: 11/21 ARIA: 16
Area [GE]	68,531 (43,335)* * Excluding padder	90,809	25,000	13,893	19,056
Max. frequency [MHz]	80	200	220	71	90
Throughput [Mbps] (@ Max.freq)	ARIA(128/256): 787/602 AES(128/256): 930/682 Whirlpool: 512	4,886	520	25	1,047/546/720
Technology [um]	0.18	0.18	0.35	0.35	0.25

경량 하드웨어 구현이 필요한 분야에 적합하지 않은 것으로 평가된다. 문헌 [11]의 AES 블록암호 프로세서 사례는 220 MHz의 클록 주파수로 동작하지만 라운드 블록이 32 비트 데이터패스로 구현되어 128 비트 데이터패스로 구현된 본 논문의 AAW 통합 프로세서 보다 처리율이 낮다.

ARIA 블록암호의 경량화 구현 사례인 문헌 [12]는 하드웨어 최소화를 위해 32 비트 데이터패스로 설계한 경우이다. 본 논문에서 설계된 AAW 크립토 프로세서의 페더 블록을 제외한 면적과 ARIA 블록암호 성능을 적용해서 게이트당 처리율을 계산하면 18.1 Kbps/gate이며, 문헌 [12]의 경우는 1.8 Kbps/gate로 본 논문의 설계에 비해 약 1/10 정도로 낮다. 문헌 [12]의 사례는 ARIA 알고리듬의 128 비트 단일 키 길이를 지원하는 반면에 본 논문의 AAW 프로세서는 세 가지 알고리듬과 두 가지 키 길이를 지원하면서도 게이트당 처리율 측면에서 우수한 것으로 평가된다. 문헌 [13]의 사례는 ARIA와 AES의 통합 구현이지만 128 비트의 키 길이만 지원하므로, 128 비트와 256 비트의 두 가지 키 길이와 Whirlpool 해시함수를 지원하는 본 논문의 설계에 비해 적은 게이트 수로 구현되었다.

본 논문의 설계는 국제표준 블록암호 AES와 국내표준 블록암호 ARIA 그리고 경량 해시함수 Whirlpool를 동시에 지원하면서 약 68,000 GE의 적은 하드웨어와 510~930 Mbps의 성능을 가져 유용성 측면에서 우수하며, 경량 하드웨어 보안 모듈을 필요로 하는 IoT 보안 응용에 적합한 것으로 평가된다.

V. 결 론

블록암호 표준인 ARIA, AES와 Whirlpool 해시함수를 단일 하드웨어 구조로 통합하여 설계하고, FPGA 구현을 통해 하드웨어 동작을 검증하였다. 세 알고리듬의 공통 특성을 기반으로 자원공유 기법을 적용하여 설계하였으며, 이를 통해 저면적, 저전력을 실현했다. 기밀성 및 무결성을 제공하는 AAW 크립토 프로세서는 0.18㎛ CMOS 공정에서 68,531 GE로 구현되었으며, 패더블록을 제외하면 43,335 GE로 구현되었다. 최대 80 MHz의 클록 주파수로 동작하는 경우에, ARIA는 602~787 Mbps의 처리율, AES는 682~930 Mbps의 처리율, 그리고 Whirlpool은 512 Mbps 처리율을 갖는 것으로 평가되었다. 본 논문의 AAW 크립토 프로세서는 하드웨어 경량화와 저전력을 특징으로 하므로, 제한된 자원을 가져 경량 하드웨어가 필요한 IoT, RFID, WSN 등 다양한 응용분야의 정보보호 SoC 설계에 IP로 활용이 가능하다.

References

[1] A. Whitmore, A. Anurag, and L.D. Xu, “The Internet of Things - A Survey of Topics and Trends,” *Information Systems Frontiers*, vol. 17, no. 2, pp. 261-274, 2015. DOI: 10.1007/s10796-014-9489-2

[2] C. Maple, "Lightweight Cryptography Applicable to Various IoT Devices," *NEC Technical Journal*, vol. 12, no. 1, pp. 67-71, 2017.
[3] *Advanced Encryption Standard*, NIST Standard FIPS 197, Nov. 2001.
[4] *128 bit Block Encryption Algorithm ARIA*, KS X 1213:2004, 2004.
[5] *128-Bit Block Cipher LEA*, TTA Standard TTAK.KO-12.0223, 2013.
[6] *Secure hash standard (SHS)*, NIST Standard FIPS PUB 180-4, Mar. 2012.
[7] P. Kitsos and O. Koufopavlou., "Whirlpool Hash Function: Architecture and VLSI Implementation," *Proc. of International Symp. on Circuits and Systems*, pp. 893-896, 2004. DOI: 10.1109/ISCAS.2004.1329416
[8] *Guideline on Usage for Hash Function*, TTA Standard. TTAK.KO-12.0109, 2009.
[9] K.B. Kim and K.W. Shin, "A Unified ARIA-AES Cryptographic Processor Supporting Four Modes of Operation and 128/256-bit Key Lengths," *Journal of The Korea Institute of Information and Communication Engineering*, vol. 21, no. 4, pp. 795-803, 2017. DOI: 10.6109/jkiice.2017.21.4.795
[10] A. Satoh, "ASIC Hardware Implementations for 512-bit Hash Function Whirlpool," *Proc. of International Symposium on Circuits and Systems*, pp. 2917-2920, 2008. DOI: 10.1109/ISCAS.2008.4542068
[11] H.K. Ahn and K.W. Shin, "AES-128/192/256 Rijndael Cryptoprocessor with On-the-fly Key Scheduler," *Journal of The Institute of Electronics Engineers of Korea*, vol. 39-SD, no. 11, pp. 961-971, 2002.
[12] J. Park, Y.D. Kim, S. Yang and Y. You, "Low Power Compact Design of ARIA Block Cipher," *Proc. of International Symposium on Circuits and Systems*, pp. 313-316, 2006. DOI: 10.1109/ISCAS.2006.1692585
[13] B.S. Koo, G.H. Ryu, T.J. Chang and S. Lee, "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.

BIOGRAPHY

Ki-BbeumKim(Member)

2016 : BS degree in Electronic Engineering, Kumoh National Institute of Technology
2018 : MS degree in Electronic Engineering, Kumoh National Institute of Technology
2018~Present : Research Engineer, Pixelplus Incorporated.

Kyung-WookShin(Member)

1984 : BS degree in Electronic Engineering, Korea Aerospace University
1986 : MS degree in Electronic Engineering, Yonsei University
1990 : PhD degree in Electronic Engineering, Yonsei University
1990~1991 : Senior Researcher in Semiconductor Research Center, Electronics and Telecommunication Research Institute (ETRI)
1991~Present : Professor in School of Electronic Engineering, Kumoh National Institute of Technology
1995~1996 : University of Illinois at Urbana-Champaign (Visiting Professor)
2003~2004 : University of California at San Diego (Visiting Professor)
2013~2014 : Georgia Institute of Technology (Visiting Professor)