블록암호와 해시함수의 통합 보안 프로세서 구현

김기쁨* · 신경욱*

*금오공과대학교

An Unified Security Processor Implementation of Block Ciphers and Hash Function

Ki-Bbeum Kim* · Kyung-Wook Shin*

Kumoh National Institute of Technology

E-mail : kkp@kumoh.ac.kr

요 약

블록암호 국제표준 AES(Advanced Encryption Standard), 국내표준 ARIA(Academy, Research Institute, Agency) 및 국제표준 해시함수 Whirlpool을 통합 하드웨어로 구현하였다. ARIA 블록암호와 Whirlpool 해시함수는 AES와 유사한 구조를 가지며, 본 논문에서는 저면적 구현을 위해서 하드웨어 자원을 공유하여 설계하였다. Verilog-HDL로 설계된 ARIA-AES-Whirlpool 통합 보안 프로세서를 Virtex5 FPGA로 구현하여 정상 동작함을 확인하였고, 0.18㎛ 공정의 CMOS 셀 라이브러리로 합성한 결과 20 MHz의 동작 주파수에서 71,872 GE로 구현되었다.

키워드

ARIA, AES, Whirlpool, Block Cipher, Hash Function, Hardware sharing

Ⅰ. 서 론

사물인터넷(Internet of Things) 시대를 맞아 스마트홈, 의료, 교통 등 실생활에 밀접한 분야로 IoT 기술이 적용되고 있다. 따라서 경량화된 플랫폼에 최적화된 암호화 및 인증 기술의 필요성 또한 강조되고 있다. IoT 디바이스는 주로 와이파이(Wi-Fi), 6LoWPAN, 지그비(ZigBee), LoRA 등의 규격에 의해 무선 네트워크로 연결되는데 이러한 프로토콜들은 기밀성(confidentiality), 무결성(integrity) 및 기기 간 인증(authentication)이 필수적으로 요구되며 ARIA[1], AES[2], SHA-2[3], RSA[4]와 같은 강도가 높은 암호들을 지원한다. 그러나 RFID와 같은 초소형 기기는 기존의 기기와는 달리 자원과 성능이 제약적이기 때문에 저전력/저면적 구현이 중요하다. 본 논문에서는 블록암호 ARIA, AES 알고리듬과 해시함수 Whirlpool[5]의 기능을 선택적으로 지원하는 ARIA-AES-Whirlpool 통합 보안 프로세서의 효율적인 하드웨어 공유 구조를 제안하고, 이를 Verilog-HDL로 모델링 하여 FPGA 구현을 통해 하드웨어 동작을 검증하였다.

Ⅱ. ARIA[1], AES[2] 및 Whirlpool[5]

ARIA와 AES는 128-비트의 평문(암호문) 블록을 암호(복호)화하여 동일한 길이의 암호문(평문)을 만드는 대칭키 방식의 블록암호로 128/192/256-비트의 세 가지 키 길이를 지원한다. ARIA와 AES 알고리듬의 치환계층에서 사용되는 S-box는 동일한 유한체 $GF(2^8)$상의 역원 연산을 이용하여 구현되며 서로 유사한 구조를 가진다.

해시함수는 가변 길이의 입력 메시지를 고정 길이의 해시 값으로 만드는 압축함수이다. 블록암호 알고리듬에 기반을 둔 Whirlpool 해시함수는 Miyaguchi-Preneel 구조로 가변 길이의 평문을 입력받아 블록마다 512-비트의 고정된 입력을 가지며, 평문, 암호문, 암호키를 모두 XOR 연산하여 메시지 다이제스트를 생성한다. Whirlpool 해시함수는 non-Feistel 구조로서 AES 블록암호 알고리듬과 유사한 구조를 가진다. ARIA, AES 블록암호 및 Whirlpool 해시함수의 구조 및 특징은 표 1과 같으며 세 가지 알고리듬을 하드웨어 구현할 경우 자원공유 될 수 있는 공통된 기능들이 있음을 알 수 있다.

Table. 1. Comparison of ARIA, AES and Whirlpool

	ARIA	AES	Whirlpool
Structure	ISPN	SPN	Miyaguchi-Prineel
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 ($x \to x^{-1}$, $x^{247} \to x^{-1}$)	SubBytes ($x \to x^{-1}$)	SubBytes (4×4 mini S-box)
	-	ShiftRows	ShiftColumns
	DiffLayer (16×16 binary matrix)	MixColumns (4×4 circulant matrix)	Mixrows (8×8 circulant matrix)

III. 블록암호와 해시함수의 통합 보안 프로세서 설계

설계된 ARIA-AES-Whirlpool(AAW) 통합 보안 프로세서는 블록암호 ARIA, AES 알고리듬과 해시함수 Whirlpool의 기능을 선택적으로 수행한다. AAW 통합 보안 프로세서의 전체구조는 그림 1과 같으며 가변 길이의 평문을 512-비트의 고정 길이로 분할하여 처리하기 위해 메시지를 패딩해주는 패딩블록(padder), 세 가지 알고리듬의 라운드 연산을 선택적으로 수행하는 통합 라운드 블록(round), 통합 라운드 키 생성 블록(key_gen) 및 제어블록(control) 등으로 구성된다.

통합 라운드 블록은 중간상태 레지스터(State_reg), 통합 치환계층(AAW-Sbox), 통합 확산계층(AAW-Diff), AES의 라운드 변환 과정에서 바이트 단위로 이동 연산을 수행하는 Shift-Row, 그리고 라운드 키 가산(AddKey)에서 사용되는 128-비트 XOR 게이트 등으로 구성된다. 통합 라운드 블록은 중간상태 레지스터를 공유하여 설계하였으며 Whirlpool 연산의 경우 평문 메시지가 입력되면 ShiftColumns 연산을 하여 데이터를 저장한다. 통합 치환계층은 ARIA와 AES의 S-box

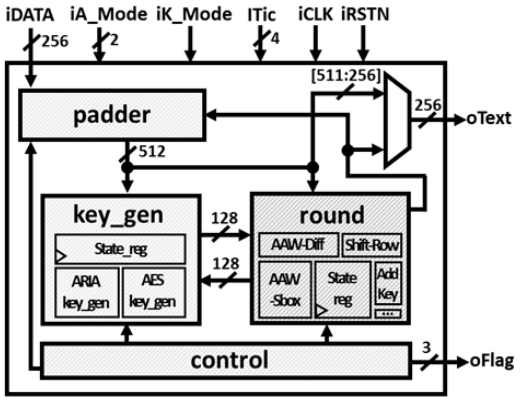


Fig. 1. Architecture of AAW processor

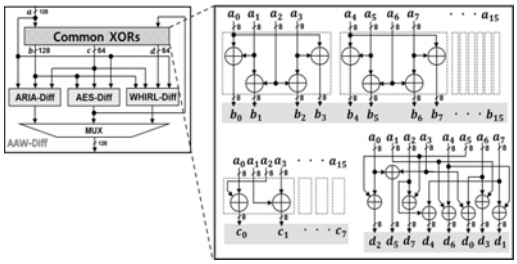


Fig. 2.Structure of AAW-Diff

연산을 통합 설계하였으며, 유한체 $GF(2^8)$상의 역원 연산인 x^{-1}을 ARIA와 AES의 S-box연산 수행 시 공유할 수 있도록 설계하였다. 통합 확산계층은 그림 2 와 같이 ARIA, AES 및 Whirlpool의 확산함수에 공통으로 사용되는 XOR 공유항을 이용하여, 효율적으로 구현하였다. 통합 라운드 키 생성 블록은 상태 레지스터를 공유하여 설계하였다. Whirlpool의 라운드 연산에는 128-비트 데이터패스로 설계되어 한 라운드 연산에 4 클록 사이클을 소모하여 라운드 연산에만 40 클록 사이클을 소요한다. Whirlpool 해시의 경우 키 확장 연산이 라운드함수와 동일하기 때문에 면적을 최소화하기 위해 라운드함수 재사용 구조를 채택하여 라운드 연산과 키 확장 연산에 총 80 클록 사이클을 소요한다. ARIA의 경우에는 키 초기화에 4 클록 사이클이 소요되며, 라운드 연산은 키 길이에 따라 13/17 클록 사이클이 소요된다. AES의 경우 복호화 키 생성에는 키 길이에 따라 10/14, 라운드 변환에는 11/15 클록 사이클이 소요된다.

IV. 기능검증 및 FPGA 검증

설계된 AAW 통합 보안 프로세서의 동작을 시뮬레이션으로 검증했으며, 기능검증이 완료된 AAW 통합 보안 프로세서는 FPGA 구현을 통해 하드웨어 동작을 검증하였다. FPGA 검증시스템은 그림 3과 같이 FPGA 보드, UART 인터페이스, C#GUI 소프트웨어로 구성된다. Virtex5

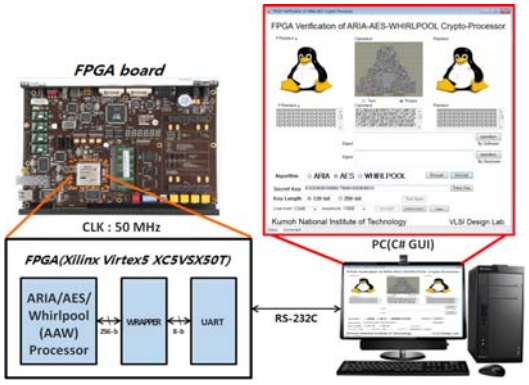
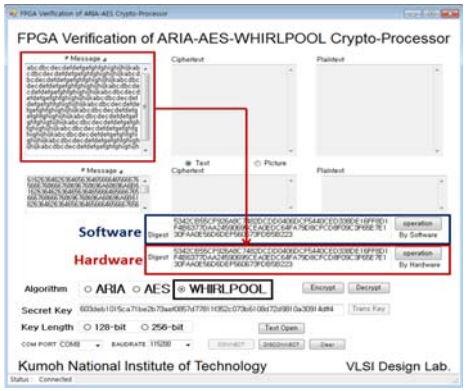


Fig. 3. FPGA verification setup

(a)



(b)

Fig. 4. FPGA verification of AAW processor
(a) AES-128 (b) Whirlpool

FPGA 디바이스가 사용되었으며, PC와 PFGA 사이에 데이터 송수신은 RS-232C를 통해 이루어진다. 그림 4는 FPGA 검증 결과를 보이고 있으며, 그림 4-(a)는 AES-128의 FPGA 검증 결과를 나타내고 있다. GUI 프로그램을 통해 AAW 통합 보안 프로세서의 암호화/복호화 결과가 화면에 표시되며 좌측 이미지를 암호화 한 후 복호화 하여 좌측의 원본 이미지가 복원되어 암호화/복호화 정상 동작을 확인하였다. 그림 4-(b)은 Whirlpool 해시암호의 FPGA 검증 결과로 메시지를 소프트웨어로 연산하여 출력된 다이제스트와 하드웨어로 연산된 다이제스트를 비교하여 AAW 통합 보안 프로세서의 정상 동작을 확인하였다.

V. 결 론

블록암호 알고리듬 ARIA, AES와 해시암호 Whirlpool 알고리듬을 선택적으로 수행하는 AAW 통합 보안 프로세서를 효율적으로 구현하였다. 치환계층과 확산계층의 하드웨어 자원공유를 통해 하드웨어 복잡도를 줄였다. 0.18㎛ 공정의 CMOS 셀 라이브러리로 합성한 결과, 20 MHz의 동작 주파수에서 71,872 GE로 구현이 되었으며, 패딩블록을 제외하면 45,023 GE이다. 최대 동작 주파수 80 MHz 클록 속도를 기준으로 ARIA는 602~787 Mbps 처리율로 수행되고, AES는 682~930, Whirlpool은 128 Mbps 처리율로 수행된다.

ACKNOWLEDGMENTS

· "This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(No. 2017R1D1A3B03031677)."
· 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] SHA-2 Standard, National Institute of Standards and Technology (NIST), Secure Hash Standard, FIPS PUB 180-2, www.itl.nist.gov/fipspubs/fip180-2.htm, 2002.
[4] RSA Laboratories, PKCS 1 v2.1 : RSA Cryptography Standard, 2002.
[5] Paulo S.L.M. Barreto and Vincent Rijmen,"The WHIRLPOOL Hashing Function," pp1-20, May. 2003.