ISSN:1226-7244 (Print)
ISSN:2288-243X (Online)
논문번호 18-02-02
j.inst.Korean.electr.electron.eng.Vol.22,No.2,233~241,June 2018
http://dx.doi.org/10.7471/ikeee.2018.22.2.233
7

ARIA/AES 기반 GCM 인증암호를 지원하는 암호 프로세서

A Cryptographic Processor Supporting ARIA/AES-based GCM Authenticated Encryption

성 병 윤*, 김 기 쁨**, 신 경 욱*★

Byung-Yoon Sung*, Ki-Bbeum Kim**, Kyung-Wook Shin*★

Abstract

This paper describes a lightweight implementation of a cryptographic processor supporting GCM (Galois/Counter Mode) authenticated encryption (AE) that is based on the two block cipher algorithms of ARIA and AES. It also provides five modes of operation (ECB, CBC, OFB, CFB, CTR) for confidentiality as well as the key lengths of 128-bit and 256-bit. The ARIA and AES are integrated into a single hardware structure, which is based on their algorithm characteristics, and a 128×12-b partially parallel GF (Galois field) multiplier is adopted to efficiently perform concurrent processing of CTR encryption and GHASH operation to achieve overall performance optimization. The hardware operation of the ARIA/AES-GCM AE processor was verified by FPGA implementation, and it occupied 60,800 gate equivalents (GEs) with a 180 nm CMOS cell library. The estimated throughput with the maximum clock frequency of 95 MHz are 1,105 Mbps and 810 Mbps in AES mode, 935 Mbps and 715 Mbps in ARIA mode, and 138~184 Mbps in GCM AE mode according to the key length.

요 약

블록암호 알고리듬 ARIA, AES를 기반으로 GCM (Galois/Counter Mode) 인증암호를 지원하는 암호 프로세서를 경량화 구현하였다. 설계된 암호 프로세서는 블록암호를 위한 128 비트, 256 비트의 두 가지 키 길이와 5가지의 기밀성 운영모드 (ECB, CBC, OFB, CFB, CTR)도 지원한다. 알고리듬 특성을 기반으로 ARIA와 AES를 단일 하드웨어로 통합하여 구현하였으며, CTR 암호연산과 GHASH 연산의 효율적인 동시 처리를 위해 128×12 비트의 부분 병렬 GF (Galois field) 곱셈기를 적용하여 전체적인 성능 최적화를 이루었다. ARIA/AES-GCM 인증암호 프로세서를 FPGA로 구현하여 하드웨어 동작을 확인하였으며, 180 nm CMOS 셀 라이브러리로 합성한 결과 60,800 GE로 구현되었다. 최대 동작 주파수 95 MHz에서 키 길이에 따라 AES 블록암호는 1,105 Mbps와 810 Mbps, ARIA 블록암호는 935 Mbps와 715 Mbps, 그리고 GCM 인증암호는 138~184 Mbps의 성능을 갖는 것으로 평가되었다.

Key words : Block cipher, authenticated encryption, AES, ARIA, GCM, GHASH

---

* School of Electronic Engineering, Kumoh National Institute of Technology, ** Pixelplus Incorporated
★ 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 Feb. 27, 2018; revised Mar. 24, 2018 ; accepted Mar. 27, 2018

Ⅰ. 서론

사용자 혹은 사물에서 수집되는 정보를 네트워크를 통해 전송, 공유, 저장하는 사물인터넷(Internet of Things)은 보안에 취약한 무선네트워크를 기반으로 하므로, 보안 위협에 대응하기 위한 정보보안의 필요성과 중요성이 증대되고 있다 [1]. 다양한 형태의 보안 위협으로부터 정보의 기밀성(confidentiality), 무결성 (integrity) 등을 보장하기 위해서는 대칭키 (symmetric key) 암호, 공개키 (public key) 암호, 해시 (hash) 함수 등 다양한 보안 알고리듬을 기반으로 하는 정보보안 시스템이 사용된다. 정보의 기밀성 보장을 위해 사용되는 대칭키 암호 알고리듬으로는 AES (Advanced Encryption Standard)[2], ARIA (Academy, Research Institute, Agency)[3], LEA [4] 등이 사용된다. 전자서명, 키 분배 등에 적용되는 공개키 암호 알고리듬으로는 RSA (Rivest, Shamir, Adleman), 타원곡선 암호 (elliptic curve cryptography; ECC)[5] 등이 널리 사용되고 있다. 해시 함수는 무결성 (integrity), 전자서명 (digital signature), 인증 (authentication) 등에 사용되며, 대표적으로 SHA (Secure Hash Algorithm)[6] 알고리듬이 있다.

대칭키 방식의 블록암호는 기밀성 향상, 무결성 검증 등을 위해 운영모드 (mode of operation)가 사용되며, 기밀성 운영모드, 인증 운영모드, 인증암호 (authenticated encryption) 운영모드로 구분된다. 기밀성 운영모드는 블록암호의 기본 모드인 ECB (Electronic Code Book)와 CBC (Cipher Block Chaining), OFB (Output FeedBack), CFB (Cipher FeedBack), CTR (Counter) 이 있다. 무결성 검증을 위한 인증 운영모드는 CMAC (Cipher -based Message Authentication Code)가 사용되고, 기밀성과 무결성을 동시에 제공하는 인증암호 운영모드로 CCM (CBC-MAC with Counter), GCM (Galois/Counter Mode) 등이 사용된다[7],[8].

AES를 기반으로 하는 AES-GCM 인증암호는 무선랜 보안 WLAN 802.1ae (MACSec) [9], 광대역 무선네트워크 WRAN 보안[10] 등에 사용되고 있으며, IoT 보안 등으로 적용이 확대되고 있다. AES-GCM의 하드웨어 구현에 관한 연구결과로 Gbps 이상의 고성능 하드웨어 구현 사례들이 발표되고 있으며[11]-[13], 최근에는 블록암호 ARIA 기반의 ARIA-GCM 인증암호의 하드웨어 구현사례가 발표되었다[14].

일반적으로, IoT 디바이스는 제한된 하드웨어/소프트웨어 자원을 가지므로, IoT 보안 시스템의 구현을 위해서는 경량화, 저전력이 중요한 요소가 된다. 본 논문에서는 우리나라 블록암호 표준인 ARIA 알고리듬과 국제 표준인 AES 알고리듬을 동시에 지원하며, 5가지 기밀성 운영모드와 GCM 인증암호 운영모드를 지원하는 ARIA/AES-GCM (AA-GCM) 인증암호 프로세서를 경량화에 초점을 맞추어 설계하고 FPGA 구현을 통해 하드웨어 동작을 확인하였다.

Ⅱ장에서는 AA-GCM 인증암호 프로세서에 사용된 블록암호 및 운영모드 알고리듬에 대해 간략히 설명하고, Ⅲ장에서는 AA-GCM 인증암호 프로세서의 하드웨어 설계에 대해 설명한다. 설계된 회로의 기능검증 및 FPGA 구현 결과를 Ⅳ장에 기술하고, Ⅴ장에서 결론을 맺는다.

Ⅱ. AA-GCM 및 운영모드 알고리듬

1. ARIA 블록암호[3]

ARIA는 우리나라 전자정부 안전성 강화를 목적으로 국가보안기술연구소에 의해 개발된 블록암호 알고리듬이며, 2004년에 국가 표준으로 채택되었다. 국제적으로 널리 사용되고 있는 블록암호 표준 AES와 동일한 인터페이스를 갖도록 설계되었으며, 128 비트의 평문(암호문) 블록을 암호(복호)화하여 128 비트의 암호문(평문)을 생성하며, 경량 하드웨어 구현을 위해 최적화된 Involutional SPN 구조를 갖는다. 128, 192, 256 비트의 세 가지 키 길이를 지원하며, 키 길이에 따라 각각 12, 14, 16 회의 반복 라운드 변환에 의해 암호·복호화가 수행된다. 라운드 변환은 홀수 라운드 함수 F_o, 짝수 라운드 함수 F_e 그리고 최종 라운드 함수 F_f로 구분되며, 라운드 함수는 라운드 키 가산, 치환 (substitution), 확산 (diffusion) 연산으로 구성된다. 홀수 라운드의 치환연산은 두 가지의 치환 함수 S_1 및 S_2와 그 역치환 함수인 S_1^{-1}, S_2^{-1}로 구현된다. 짝수 라운드의 치환연산은 홀수 라운드 치환의 역 (inverse) 연산 관계를 갖는다. 최종 라운드의

치환연산은 짝수 라운드와 동일하고, 확산이 라운드 키 가산으로 대체된다. 라운드 키는 매 라운드마다 키 확장을 통해 생성된다.

2. AES 블록암호[2]

DES (Data Encryption Standard)를 대체하기 위해 2001년 미국 기술표준국에 의해 표준으로 제정된 AES는 오늘날 가장 널리 사용되고 있는 대칭키 방식의 블록암호 알고리듬이다. 128 비트의 평문(암호문)을 암호화(복호화)하여 동일한 길이의 암호문(평문)을 만들며, 128, 192, 256 비트의 키 길이에 따라 10, 12, 14회의 라운드변환을 수행한다. 라운드변환은 초기 라운드키 가산, 키 길이에 따른 (Nr-1)회의 반복 라운드 및 최종 라운드의 순서로 처리된다. 암호화의 라운드변환은 대치 (SubByte), 치환 (ShiftRow), 뒤섞음 (MixColumn), 라운드키 가산 (KeyAdd) 순서로 연산되며, 최종 라운드는 대치, 치환, 라운드 키 가산 순으로 연산된다. 복호화의 라운드 변환은 역대치 (InvSubByte), 역치환 (InvShiftRow), 역뒤섞음 (InvMixColumn)이 사용되며, 라운드 키가 역순으로 사용된다.

3. 블록암호 운영모드

ECB 모드는 블록암호의 기본 운영모드이다. CBC 모드는 평문과 이전 블록의 암호문이 XOR 연산되어 암호화된다. 최초 평문에는 초기화 벡터 (initial vector)가 XOR 연산된다. CFB 모드는 이전 블록의 암호문이 블록암호에 입력되어 암호화된 값과 평문이 XOR 연산되어 암호문으로 출력되며, 최초 입력은 IV이다. OFB 모드는 이전 블록의 블록암호 결과가 다시 블록암호에 입력되어 암호화된 값과 평문이 XOR 연산되어 암호문으로 출력되며, 최초 입력은 IV이다. CTR 모드는 nonce 계수 값이 블록암호에 입력되어 암호화된 값과 평문이 XOR 연산되어 암호문으로 출력된다.

GCM 모드는 정보의 기밀성과 무결성을 동시에 제공하는 인증암호 운영모드이다. 기밀성은 CTR 모드를 통해 제공되며, 무결성은 GHASH 함수를 통해 제공된다. GCM 모드에서 Galois Field (GF) 곱셈연산과 블록암호 연산은 병렬로 처리되어 고성능 구현이 가능하다. 2개의 평문 블록과 하나의 추가인증 데이터 (additional authentication data; AAD) 블록을 입력으로 갖는 GCM 알고리듬은 그림 1과 같다.[8] 최초 마스터키가 입력되면 128 비트의 0 ($128'b0$)이 블록암호 알고리듬에 의해 암호화되며, 암호화된 결과는 해시 키 (hash key)로 사용된다. 해시 키 생성이 완료된 후 AAD가 GF 곱셈연산으로 입력되고, AAD 블록의 길이에 따라 GF 곱셈연산의 반복 횟수가 결정된다. AAD 블록에 대한 GF 곱셈연산이 완료되면, 블록암호 알고리듬에 의해 CTR 모드 암호화 연산이 수행된다. CTR 모드 암호화에서 출력되는 암호문과 이전 GF 곱셈연산 결과 값이 XOR 연산된 후, GF 곱셈연산이 수행된다. 무결성 증명을 위한 인증태그는 식 (1)의 GHASH 함수를 통해 생성된다. 식 (1)에서 X_j는 AAD, CTR 모드 암호문, 입력된 데이터의 총 길이 정보를 나타내며, 해시 키 H는 $128'b0$을 CTR 암호화하여 생성 된다. 식 (1)에서 GHASH 함수를 구성하는 덧셈, GF 곱셈연산은 모두 기약다항식 $P(x)=x^{128}+x^7+x^2+x+1$를 적용하여 $GF(2^{128})$상에서 이루어진다[8].

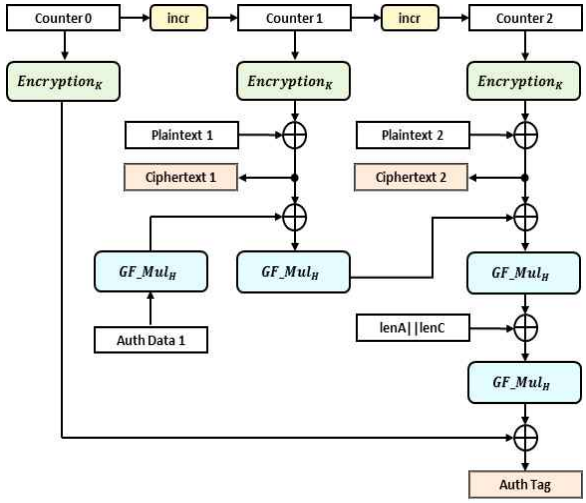

Fig. 1. GCM algorithm (for one AAD block and two plaintext blocks).
그림 1. GCM 알고리듬 (단일 AAD와 두개의 평문인 경우)

$$\sum_{j=1}^{m} X_j \cdot H^{m-j+1} = X_1 \cdot H^m \oplus X_2 \cdot H^{m-1} \oplus \cdots \oplus X_m \cdot H \quad (1)$$

III AA-GCM 인증암호 프로세서 설계

우리나라 블록암호 표준인 ARIA 알고리듬과 국제 표준인 AES 알고리듬의 5가지 기밀성 운영모드와 함께 GCM 인증암호 운영모드를 지원하는

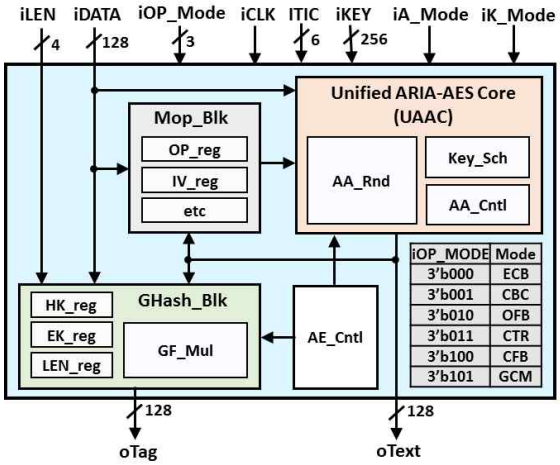

Fig. 2. Architecture of AA-GCM AE processor.
그림 2, AA-GCM AE 프로세서의 구조

ARIA/AES-GCM (AA-GCM) 인증암호 프로세서를 설계했다. AA-GCM 인증암호 프로세서는 128 비트와 256 비트의 두 가지 키 길이를 지원하며, 내부에 키 스케줄러를 포함하고 있어 평문/암호문 블록의 연속적인 암호·복호 및 GCM 운영모드 동작이 가능하다.

1. 전체구조

AA-GCM 크립토 프로세서의 구조는 그림 2와 같으며, ARIA-AES 통합 코어 (UAAC), GHASH 블록 (GHash_Blk), 운영모드 블록 (Mop_Blk), 제어 블록 등으로 구성된다. 키 값이 입력되는 256 비트의 iKEY와 평문·암호문, IV, AAD가 입력되는 128 비트의 iDATA 입력포트를 가지며, 암호문·평문이 출력되는 128 비트의 oText와 인증 태그 값이 출력되는 oTag 출력포트를 갖는다. iA_Mode 신호에 의해 블록암호 알고리듬 (ARIA, AES)이 선택되고, iK_Mode 신호에 의해 키 길이 (128, 256 비트)가 결정되며, iOP_Mode 신호에 의해 운영모드가 선택된다. UAAC는 ARIA와 AES의 암호·복호 기능을 단일 회로로 통합하여 구현되었으며, ARIA와 AES의 라운드변환을 처리하는 통합 라운드변환 블록 (AA_Rnd), 라운드키를 생성하는 통합 라운드키 생성 블록 (Key_Sch) 그리고 제어블록으로 구성된다.[15],[16] Mop_Blk는 GCM 인증암호 모드와 5가지 기밀성 운영모드에 사용되는 레지스터 (OP_reg, IV_reg)와 XOR 게이트 및 멀티플렉서를 포함한다. GHash_Blk는 $GF(2^{128})$ 상의 곱셈기 GF_Mul과 3개의 레지스터 (HK_reg, EK_reg, LEN_reg) 및 XOR 게이트로 구성되며, 제어블록은 AA-GCM 프로세서의 전체 동작을 제어한다.

2. 인증암호 운영모드의 동작

그림 3은 키 길이 128 비트인 경우에 대한 AA-GCM 프로세서의 동작 타이밍도를 보인 것이며, ARIA-GCM 운영모드는 그림 3-(a), AES-GCM 운영모드는 그림 3-(b)이다. 암호·복호에 사용될 키가 입력되면, UAAC에서 암호화 연산에 의해 128 비트의 해시 키가 생성된다. ARIA 모드에서는 키 초기화 후 해시 키가 생성되고, AES 모드에서는 복호화 키와 해시 키가 동시에 생성된다.

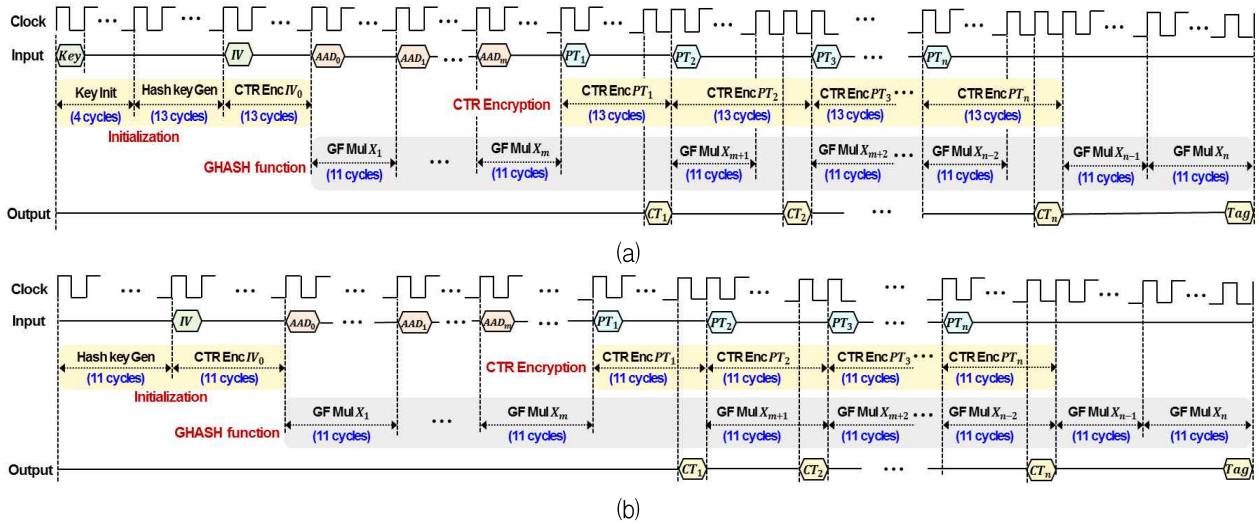

Fig. 3. Timing diagram of AA-GCM crypto-processor for 128-bit key length (a) ARIA-GCM (b) AES-GCM.
그림 3. 128-비트의 키 길이에 대한 AA-GCM 크립토 프로세서의 동작 타이밍도 (a) ARIA-GCM (b) AES-GCM

Table 1. Number of clock cycles for AE mode operation.
표 1. AE 운영모드의 소요 클록 사이클

Crypto mode	Key Init. (cycles)		CTR encryption (cycles)	GF multiplication (cycles)
ARIA-128	4	13	13	11
ARIA-256		17	17	11
AES-128	11		11	11
AES-256	15		15	11

생성된 해시 키는 GHash_Blk의 HK_reg에 저장된다. IV가 입력되면 Mop_Blk의 IV_reg에 저장되고, UAAC에서 암호화 연산된 후 GHash_Blk의 EK_reg에 저장된다. AAD가 입력되면, AAD의 데이터 길이 정보가 LEN_reg의 상위 64 비트 영역에 저장되고, 해시 키와 AAD가 GF_Mul에 입력되어 GF 곱셈연산이 수행된다. AAD 블록이 2개 이상인 경우에는 이전 블록의 GF 곱셈연산 결과 값과 XOR 연산되어 GF_Mul로 다시 입력된다. AAD에 대한 GF 곱셈연산이 끝나면, 평문(암호문)이 입력되며, Mop_Blk의 OP_reg에 저장된다. 평문의 블록길이 정보는 LEN_reg의 하위 64 비트 영역에 저장된다. IV_reg에 저장된 IV의 카운터 값을 이용하여 평문(암호문)에 대한 CTR 암호연산이 수행된다. 카운트된 IV가 UAAC에 입력되어 암호화된 후, OP_reg 저장된 평문과 XOR 연산되어 암호문으로 출력된다. 암호문은 이전 블록의 GF 곱셈연산 결과 값과 XOR 연산되어 GF_Mul에 다시 입력되어 다음 블록의 GF 곱셈연산에 사용된다. 모든 평문 블록에 대한 CTR 암호연산과 GF 곱셈연산이 끝나면, 마지막 GF 곱셈연산 결과 값과 LEN_reg에 저장된 길이 정보가 XOR 연산되어 GF_Mul에 입력된다. 마지막 GF 곱셈연산 결과 값은 EK_reg에 저장된 값과 XOR 연산되어 최종 인증 태그 값으로 출력된다.

표 1은 인증암호 운영모드의 하위 연산에 소요되는 클록 사이클 수를 보이고 있다. UAAC의 CTR 암호화는 블록암호 알고리듬과 키 길이에 따라 11~17 클록 사이클이 소요되는 점을 고려하여 GF 곱셈연산이 11 클록 사이클에 처리되도록 GF 곱셈기를 설계하였으며, 이를 통해 전체적인 동작 타이밍의 최적화를 이루었다.

3. $GF(2^{128})$ 곱셈기

GHASH 함수를 구현하는 핵심 연산블록인 GF 곱셈기는 128 비트 해시 키와 128 비트 데이터의 $GF(2^{128})$상의 곱셈을 연산한다. GF 곱셈기의 하드웨어 구현을 위한 다양한 방식들이 제안되고 있으며, 구현방식에 따라 곱셈연산에 소요되는 클록 사이클 수와 하드웨어 복잡도 사이에 교환조건이 존재한다.

그림 1의 GCM 알고리듬에서 보는 바와 같이, 평문을 암호화한 암호문이 GF 곱셈의 입력으로 사용되므로, 암호화 연산에 소요되는 클록 사이클 수를 고려해서 GF 곱셈기를 설계하는 것이 바람직하다. GF 곱셈을 단일 클록 사이클로 처리하는 병렬형 곱셈기는 CTR 모드 암호화 연산이 완료될 때까지 기다려야 하므로, 하드웨어 복잡도는 크면서도 동작 타이밍이 효율적이지 못하다. 반대로 $GF(2^{128})$ 곱셈을 128 클록 사이클에 처리하는 직렬형 GF 곱셈기는 적은 하드웨어가 사용되는 장점은 있으나 GCM 모드 전체의 성능을 저하시키는 요인이 되어 비효율적이다.

본 논문에서는 그림 3의 동작 타이밍도와 같이 AES, ARIA의 CTR 모드 암호화와 $GF(2^{128})$ 곱셈이 병렬로 수행되도록 설계하였다. 표 1에서 보듯이 본 논문의 AA-GCM 프로세서는 CTR 모드 암호화를 위해 키 길이에 따라 11~17 클록 사이클이 소요된다. 전체적인 동작 타이밍과 하드웨어 복잡도의 최적화를 고려하여 $GF(2^{128})$ 곱셈연산이 11 클록 사이클에 걸쳐 '리틀 앤디언(little endian)' 방식으로 연산되도록 GF 곱셈기를 설계하였다.

$GF(2^{128})$ 곱셈을 연산하는 GF_Mul의 내부 구조는 그림 4-(a)와 같으며, PP_AR 블록, GF 곱셈 연산의 중간 값을 저장하는 128 비트 레지스터 Gm_reg 및 멀티플렉서 등으로 구성된다. PP_AR 블록의 내부 구성은 그림 4-(b)와 같으며, 128×12 비트의 부분곱 생성과 가산 및 모듈러 연산을 위한 XOR 게이트로 구성된다. iGHASH로 입력되는 128 비트 데이터(AES, ARIA의 CTR 암호 결과)와 12 비트의 해시 키 곱셈이 단일 클록 사이클에 처리되며, 128×128 비트의 GF 곱셈에 총 11 클록 사이클이 소요된다.

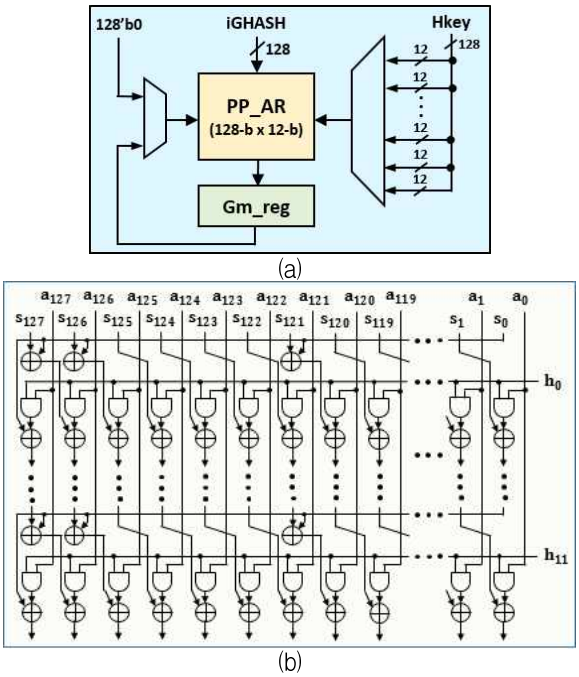

Fig. 4. $GF(2^{128})$ multiplier for GHASH (a) GF_Mul block (b) PP_AR block for partial product addition and reduction of 128×12-bit.
그림 4. GHASH 함수를 위한 $GF(2^{128})$ 상의 곱셈기 (a) GF_Mul 블록 (b) 부분곱 덧셈과 모듈로 연산을 위한 128×12-비트 PP_AR 블록

Ⅳ 기능검증 및 성능평가

AA-GCM 인증암호 프로세서는 FPGA 구현을 통해 하드웨어 동작을 검증하였다. FPGA 검증 시스템은 그림 5와 같이 FPGA 보드, UART 인터페이스, C# 기반 구동 소프트웨어로 구성되며, FPGA는 Xilinx Virtex5 XC5VSX-95T 디바이스가 사용되었다. FPGA에 구현된 AA-GCM 인증암호 프로세서로 테스트 벡터를 보내고, 암호·복호 동작 및 인증 결과는 GUI 프로그램에 의해 화면에 표시된다.

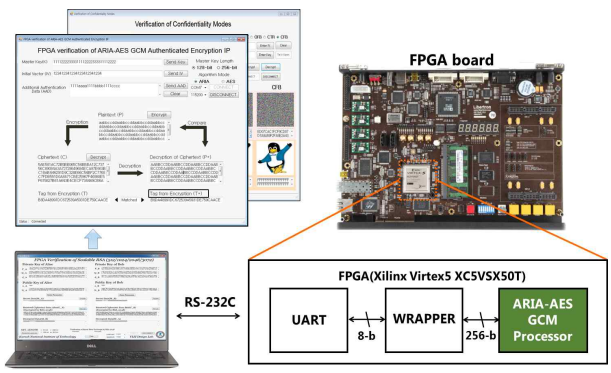

Fig. 5. FPGA Verification setup.
그림 5. FPGA 검증시스템 구성

1. 기밀성 운영모드 동작 검증

그림 6-(a)는 AA-GCM 인증암호 프로세서의 기밀성 운영모드에 대한 FPGA 검증 결과이며, 키 길이 128 비트로 동작하는 AES의 5가지 운영모드에 대한 암호·복호 동작의 FPGA 검증 결과를 보이고 있다. GUI 화면 좌측 위의 펭귄 원본 이미지 데이터가 FPGA로 전송되어 AA-GCM 프로세서에서 5가지 기밀성 운영모드로 암호화된 결과는 화면 중앙의 5개 이미지와 같다. 암호화 결과 중, ECB 모드의 암호화 결과는 원본 이미지의 윤곽이 희미하게 드러나는 것을 볼 수 있으며, 이는 동일한 평문을 암호화하면 동일한 암호문이 출력되는 ECB 운영모드의 특성 때문이다. CBC, OFB, CTR, CFB 운영모드의 암호화 결과는 원본 이미지가 무작위 값으로 암호화된 것을 확인할 수 있으며, 이들 운영모드는 동일한 평문을

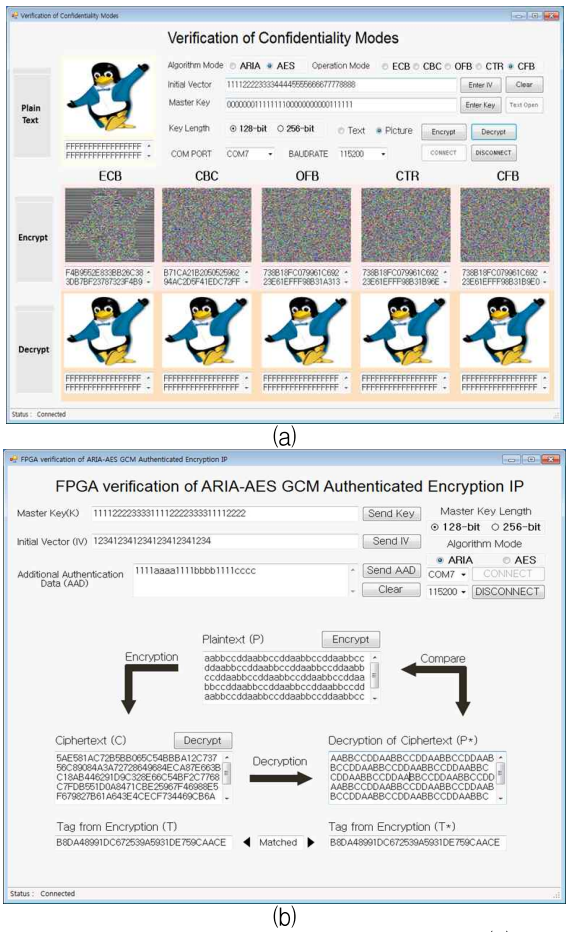

Fig. 6. Screenshots of FPGA verification results (a) AES encryption and decryption with 128-bit key, (b) ARIA-GCM with 128-bit key.
그림 6. FPGA 검증결과 화면 캡처 (a) 키 길이 128 비트의 AES 암호·복호 동작 (b) 키 길이 128 비트의 ARIA-GCM 및 암호·복호 동작

Table 2. Comparison of authenticated encryption cores.
표 2. 인증암호 코어의 비교

	This paper	[14]	[11]	[12]	[13]
Algorithm	ARIA, AES	ARIA	AES	AES	AES
Mode of operation	GCM, ECB, CTR, CBC, OFB, CFB	GCM	GCM	GCM	GCM
Key size [bits]	128, 256	128, 256	128	128	128
Datapath size [bits]	128	128	4-parallel of 128	unrolled & pipelined of 128	128
Technology / FPGA device	180 nm	180 nm	65 nm	Virtex7	Virtex5
Hardware complexity	60,800 GEs	44,986 GEs	625,000 GEs	38,241 slices	3,211 slices
Throughput [Mbps]	AES-128, 256: 1105, 810 ARIA-128, 256: 935, 715 AES-GCM-128, 256: 184, 155 ARIA-GCM-128, 256: 160, 138	160, 138	8,300	15,240	27,700
Max. frequency [MHz]	95	100	N/A	119	216.3

암호화하더라도 동일한 암호문이 출력되지 않는 특성 때문이다. 화면 아랫부분의 5개 이미지는 암호화된 이미지를 다시 복호화하여 얻어진 것이다. 최초 암호화에 사용된 원본 펭귄 이미지와 동일한 결과가 출력되었으며, 이와 같은 검증을 통해 설계된 AA-GCM 인증암호 프로세서의 하드웨어 동작이 정상임을 확인하였다.

2. 인증암호 운영모드 동작 검증

그림 6-(b)는 AA-GCM 인증암호 프로세서의 GCM 운영모드 검증결과 중 일부를 보인 것이며, 키 길이 128 비트로 동작하는 ARIA 인증암호 모드인 ARIA-GCM의 검증결과이다. 암호화의 경우 마스터키 K, 초기화 벡터 IV, 추가 인증 데이터 AAD, 그리고 평문 P의 순서로 입력된 후, 암호화 동작에 의해 암호문 C와 인증태그 T가 생성된다. 복호화 과정에서는 마스터키 K, 초기화 벡터 IV, 추가 인증 데이터 AAD, 그리고 암호문 C의 순서로 입력된 후, 복호화 동작에 의해 복호문 P*와 복호화 인증태그 T*가 생성된다. 그림 6-(b)로부터, 평문 P와 동일한 복호문 P*가 얻어졌으며, 또한 암호화에 의해 생성된 인증 태그 T와 복호화에 의해 생성된 인증 태그 T*가 일치함을 확인할 수 있다. 이와 같은 검증을 통해 FPGA에 구현된 AA-GCM 인증암호 프로세서의 GCM 운영모드가 올바로 동작함을 확인하였다

3. AA-GCM 코어의 성능평가

Verilog HDL로 설계된 AA-GCM 인증암호 프로세서를 0.18㎛ CMOS 표준 셀 라이브러리로 합성한 결과, 최대 95 MHz의 클록 주파수로 동작 가능한 것으로 평가되었다. 80 MHz의 동작 주파수로 합성한 결과, 128, 256 비트의 두 가지 키 길이를 지원하는 ARIA-AES 크립토 코어는 49,688 GE, 5가지 기밀성 운영모드를 지원하는 회로는 4,970 GE, $GF(2^{128})$의 유한체 곱셈을 연산하는 GF_Mul 블록은 6,111 GE로 구현되었으며, AA-GCM 인증암호 코어는 60,800 GE로 구현되었다.

설계된 AA-GCM 인증암호 코어의 연산 성능을 95 MHz 동작 주파수에 대해 평가하였다. 키 길이 128, 256 비트에 따라 AES의 기밀성 운영모드는 각각 1,105 Mbps, 810 Mbps이고, ARIA의 기밀성 운영모드는 각각 935 Mbps, 715 Mbps로 예측되었다. GCM 운영모드는 128, 256 비트 키 길이에 따라 AES의 경우 각각 184, 155 Mbps, ARIA의 경우 각각 160, 138 Mbps로 예측되었다.

ARIA와 AES를 동시에 지원하는 GCM 인증암호의 구현 사례가 없어 직접적인 비교는 어려우나, 본 논문의 AA-GCM 인증암호 프로세서와 문헌에 발표된 유사 사례를 표 2에 비교하였다. 문헌 [14]의 사례는 128, 256 비트의 키 길이 지원과 128 비트 데이터패스로 구현되어 본 논문의 경우와 유사하나, ARIA-GCM만 지원하고 블록암호의 5가지 운영모드를 지원하지 않아 유용성 측면에서 다소 떨어진다. 문헌 [11]~[13]의 사례는 AES 기반의 고성능 GCM 인증암호 구현 사례이다.

문헌 [11]의 사례는 128 비트 데이터패스 4개를 병렬로 동작시켜 8.3 Gbps의 성능을 구현하였으나, 625 kGE가 사용되어 본 논문의 AA-GCM 코어에 비해 10배 이상의 하드웨어를 필요로 한다. 문헌 [12]의 사례는 128 비트 데이터패스의 라운드 펼침(unrolled) 및 파이프라인 구조로 구현되어 15.24 Gbps의 높은 성능을 가지나 높은 하드웨어 복잡도를 갖는다. 문헌 [13]의 사례는 라운드키 스케줄링 대신에 하드웨어 내장 라운드키 방식과 서브 파이프라인을 도입하여 동작 주파수를 높였다. 표 2에서 볼 수 있듯이, 외국의 사례들은 AES 기반 GCM 인증암호의 고성능 구현에 초점이 맞추어져 있다. 본 논문의 설계는 국제표준 AES와 함께 국내 표준 ARIA를 동시에 지원하며, 인증암호뿐만 아니라 5가지 기밀성 운영모드를 지원하면서 60,000 GE의 적은 하드웨어, 130~180 Mbps의 AE 성능을 가져 유용성 측면에서 우수하며 경량 하드웨어 보안 모듈을 필요로 하는 IoT 보안 응용에 적합한 것으로 평가된다.

V 결론

블록암호의 CTR 운영모드와 GHASH 함수에 의해 정보의 기밀성과 인증을 동시에 제공하는 GCM 인증암호 프로세서를 설계하였다. AES 블록암호를 기반으로 하는 AES-GCM 인증암호의 하드웨어 구현사례들이 발표되고 있으나, 본 논문에서는 국내 블록암호 표준 ARIA와 국제 표준 AES를 동시에 지원하는 이중 표준 ARIA/AES- GCM 인증암호 프로세서를 설계하였다. AA-GCM 인증암호 프로세서는 60,800 GE로 구현되어 경량화를 특징으로 하며, 블록암호의 기밀성 운영모드는 715~1,105 Mbps, GCM 인증암호 운영모드는 138~184 Mbps의 성능을 갖는 것으로 평가되었다. 본 논문의 인증암호 프로세서는 GCM 운영모드 이외에 블록암호의 5가지 기밀성 운영모드를 지원하므로, 다양한 분야의 보안 하드웨어 구현에 적용될 수 있다. 또한 ARIA, AES의 통합 구현과 부분 병렬 GF 곱셈기를 통한 저면적 및 성능 최적화를 통해 경량 하드웨어가 필요한 IoT 보안 분야에 적합하다.

References

[1] C. Maple, "Security and Privacy in the Internet of Things," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 155-184, 2017. DOI:10.1080/23738871.2017.1366536

[2] Advanced Encryption Standard, NIST Standard FIPS 197, 2001.

[3] 128 bit Block Encryption Algorithm ARIA, KS X 1213:2004, 2004.

[4] 128-Bit Block Cipher LEA, TTA Standard TTAK.KO-12.0223, 2013.

[5] *Digital Signature Standard (DSS)*, NIST Standard FIPS PUB 186-4, 2013.DOI:10.6028/NIST.FIPS.186-4

[6] *Secure hash standard (SHS)*, NIST Standard FIPS PUB 180-4, 2012. DOI:10.6028/NIST.FIPS.180-4

[7] Morris Dworkin,"Recommendation for Block Cipher Modes of Operation-Methods and Techniques,"*NIST Special Publication* 800-38A, Dec, 2001. DOI:SP 800-38A

[8] D. McGrew and J. Viega, "*The Galois/ Counter Mode of Operation (GCM)*," Submission to NIST Modes of Operation Process, 2004.

[9] *IEEE Standard for Local and Metropolitan Area Networks, Media Access Control (MAC) Security*, 2006. DOI:10.1109/IEEESTD.2006.245590

[10] Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands, IEEE Standard 802.22-2011, pp. 1-672, 2011.

[11] V. P. Hoang, V. T. Nguyen, A. T. Nguyen, C. K. Pham, "A low power AES-GCM authenticated encryption core in 65nm SOTB CMOS process," *Proceedings of 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 112-115, Boston, 2017. DOI:10.1109/MWSCAS.2017.8052873

[12] J. Vliegen, O. Reparaz, and N. Mentens "Maximizing the Throughput of Threshold-protected AES-GCM Implementations on FPGA," *Proceedings of 2017 IEEE 2nd International Verification and Security Workshop (IVSW)*, pp. 140-145, Thessaloniki, Greece, 2017. DOI:10.1109/IVSW.2017.8031559

[13] K.M. Abdellatif, R. Chotin-Avot, and H. Mehrez, "Improved Method for Parallel AES-GCM Cores Using FPGAs," *Proceedings of 2013 International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, Cancun, 2013. DOI:10.1109/ReConFig.2013.6732299

[14] K.B. Kim, B.Y. Sung and K.W. Shin "An Implementation of GCM Authenticated Encryption based on ARIA Block Cipher," *in Proceeding of conference on korea information and communication engineering*, Pusan, pp.111, 2017.

[15] 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, 2008.

[16] 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

BIOGRAPHY

Byung-Yoon Sung (Member)

2015 : BS degree in Electronic Engineering, Kumoh National Institute of Technology.

2017~ : Graduate student of Kumoh National Institute of Technology

Ki-Bbeum Kim (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-Wook Shin (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)