ARIA 블록암호 기반의 GCM 인증암호 구현

김기쁨* · 성병윤* · 신경욱*

*금오공과대학교

An Implementation of GCM Authenticated Encryption based on ARIA Block Cipher

Ki-Bbeum Kim* · Byung-Yoon Sung* · Kyung-Wook Shin*

Kumoh National Institute of Technology

E-mail : kkp@kumoh.ac.kr

요 약

국제 표준화 기구인 ISO/IEC와 NIST(National Institute of Standards and Technology)에서는 정보 유출 방지 및 정보의 유효성 인증을 위해 다양한 암호 기법들을 표준으로 권고하고 있다. 그 중 NIST SP 800-38D에서 표준으로 권고된 GCM(Galois/Counter Mode) 인증 암호화 모드는 블록암호의 CTR 운영모드와 GHASH를 이용하여 메시지의 기밀성과 무결성을 동시에 제공하는 운영모드이다. 본 논문에서는 ARIA 블록암호 기반의 ARIA-GCM 프로세서를 Verilog HDL로 모델링 하고, Virtex5 FPGA로 구현하여 정상 동작함을 확인하였다. 0.18㎛ 공정의 CMOS 셀 라이브러리로 합성한 결과 20 MHz의 동작주파수에서 44,986 GE로 구현되었다.

키워드

ARIA, GCM, GHASH, AE

Ⅰ. 서 론

IoT(Internet of Things) 기술이 발전함과 동시에 IoT 보안에 관한 관심도 꾸준히 증가하고 있다. 각종 네트워크에 연결되어 정보가 수집, 전송, 공유되는 IoT 특성상 다양한 보안 위험에 노출될 수 있다. 특히, RFID와 센서노드와 같은 초절전/초경량 하드웨어의 경우 자체적인 접근 제어 기능이 없기 때문에 장치 간의 인증체계가 매우 중요하며 인증과 동시에 데이터 암호화가 이루어져야 한다[1].

NIST(National Institute of Standards and Technology)는 CCM(Counter with CBC-MAC), GCM(Galois/Counter Mode)[2]와 같은 인증암호(AE; Authenticated Encryption) 모드를 표준으로 권고하고 있다. 인증암호 모드는 블록암호를 기반으로 메시지에 대한 기밀성과 무결성을 동시에 보장할 수 있는 암호화 기법으로 본 논문에서는 국내 표준인 ARIA 블록암호 알고리듬 기반의 GCM 인증암호를 수행하는 ARIA-GCM 프로세서를 Verilog-HDL로 모델링 하여, FPGA 구현을 통해 하드웨어 동작을 검증하였다.

Ⅱ. ARIA[3] 알고리듬, GCM[4] 모드

블록 암호 ARIA 알고리듬은 대칭키 블록암호로 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.

GCM 인증암호 모드는 대칭키 기반으로 수행되며 개인키를 사용한 암호화 과정과 인증과정을 통해 메시지의 기밀성과 무결성 동시에 보장할 수 있다. GCM 인증암호는 기존의 해쉬를 이용한 MAC 생성과 함께 사용되는 블록암호의 CTR 모드와 같이 암호화 모듈과 인증모듈이 따로 생성되는 방법보다 자원과 속도 측면에서 효율적으로 구현될 수 있다. GCM 모드의 동작은 각각의 블록을 암호화하기 위해 CTR 모드를 사용하여

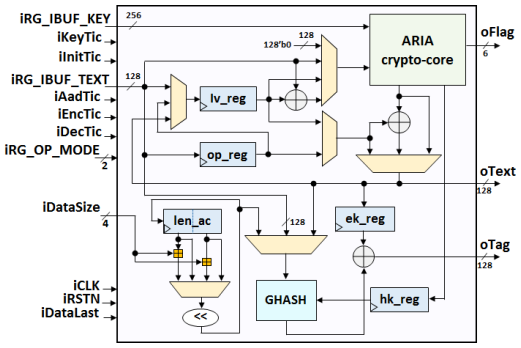


Fig. 1. Architecture of ARIA-GCM processor

블록을 암호화하고, 암호화된 데이터는 GHASH 함수 연산에 사용된다. GHASH 함수는 유한체 $GF(2^{128})$상의 곱셈 연산으로, 유한체 상의 곱셈을 수행하여 인증태그를 생성한다.[5]

III. ARIA-GCM 프로세서 설계

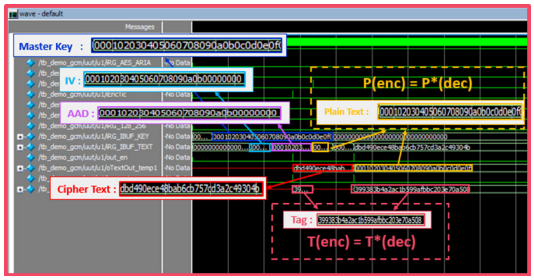
설계된 ARIA-GCM 프로세서는 128/256-비트 마스터키 길이를 지원하고, ARIA 블록암호를 이용한 기본적인 운영모드 ECB, CBC, OFB, CTR, CFB의 5가지 운영모드와 인증 암호화 운영모드인 GCM 운영모드를 지원한다.

그림 1은 ARIA-GCM 프로세서의 전체블록도로 ARIA crypto-core, 기본 운영모드와 GCM 모드에 사용되는 128-비트 레지스터(iv_reg, op_reg, ek_reg, hk_reg, len_ac), GHASH, 제어블록 등으로 구성된다.

ARIA-GCM 프로세서의 동작은 외부에서 마스터키가 입력되면 4 클록 사이클을 소모하는 키 초기화 과정을 거친 뒤 해쉬키 값을 생성하여 hk_reg에 저장한다. 초기화벡터, 추가인증데이터가 입력되면 초기화벡터를 암호화하여 ek_reg에 저장하고, 추가인증데이터에 대한 GHASH 연산을 한다. 추가인증데이터에 대한 처리가 모두 끝나면 평문이 입력되어 초기화벡터의 카운터 값을 암호화하여 평문과 XOR 연산된 값이 이전의 GHASH 연산된 값과 XOR 연산 후 GHASH 연산이 수행된다. 입력된 평문의 대한 암호화 연산이 끝나면 이에 대한 GHASH 값과 입력 데이터(추가인증데이터, 평문)의 길이 정보를 XOR 연산한 뒤 GHASH 연산을 수행한 값과 ek_reg에 저장된 값을 XOR 연산하여 인증태그 값을 출력한다.

IV. 기능검증 및 FPGA검증

설계된 ARIA-GCM 프로세서의 동작을 시뮬레이션으로 검증했으며, 검증결과는 그림 2와 같다. 그림 2는 ARIA-GCM 프로세서의 기능검증 결과



(a)

Alen = 128-b, Plen = 128-b

K	000102030405060708090A0B0C0D0E0F
IV	000102030405060708090A0B0C0D0E0F
A	000102030405060708090A0B0C0D0E0F
P	000102030405060708090A0B0C0D0E0F
C	DBD490ECE48BAB6CB757CD3A2C49304B
T	399383B4A2AC1B599AFBBC203E70A508

(b)

Fig. 2. Simulation results of ARIA-GCM processor (a) results of ARIA-GCM (b) Reference data

와 문헌[5]의 참조구현 값으로 그림 5-(b)의 참조구현 값인 마스터키(K), 초기화벡터(IV), 추가인증데이터(A), 평문(P)를 이용하여 암호화한 결과 암호문 "DBD4 90EC E48B AB6C B757 CD3A 2C49 304B"과 태그 "3993 83B4 A2AC 1B59 9AFB BC20 3E70 A508"이 출력되었고, 이를 복호화 하여 복호된 암호문(P*)이 출력되어 암호화 기능이 정상적으로 동작함을 확인하고, 복호화 후 출력된 태그값(T*)과 암호화 후 출력된 태그값(T)을 비교하여 일치함을 확인하였다. 기능검증이 완료된 ARIA-GCM 프로세서는 FPGA 구현을 통해 하드웨어 동작을 검증하였다. FPGA 검증시스템은 그림 3과 같이 FPGA 보드, UART 인터페이스, C#GUI 소프트웨어로 구성된다. Virtex5 FPGA 디바이스가 사용되었으며, PC와 PFGA 사이에 데이터 송수신은 RS232C를 통해 이루어진다.

그림 4는 ARIA-GCM 프로세서의 FPGA 검증결과를 보이고 있으며 암호화의 경우 마스터키

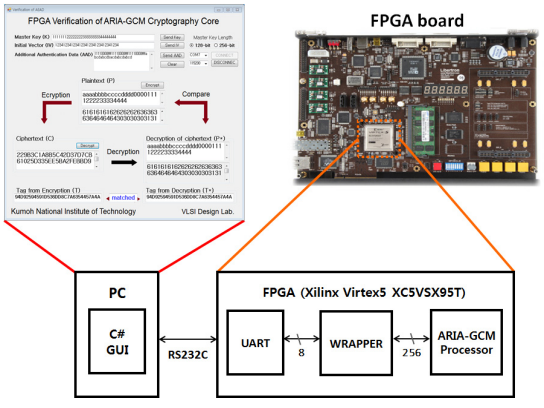


Fig. 3. FPGA verification setup

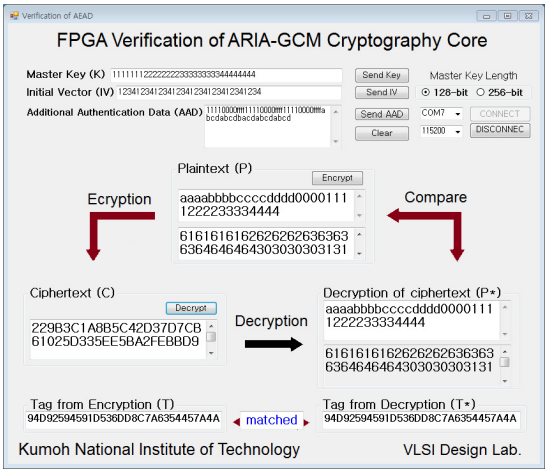


Fig. 4. FPGA verification of ARIA-GCM processor

(K), 초기화벡터(IV), 추가인증데이터(AAD)를 입력 후 평문(P)을 암호화하면 암호문(C)과 태그값(T)이 생성된다. 복호화의 경우 암호화와 동일한 마스터키(K), 초기화벡터(IV), 추가인증데이터(AAD)를 입력하여 암호문을 복호화 하면 복호된 암호문(P*)과 태그값(T*)이 생성된다. 평문(P)과 복호화 된 암호문(P*)을 비교하고, 암호화 후 생성된 태그값(T)과 복호화 후 생성된 태그값(T*)을 비교해서 일치함을 확인하여 FPGA에 구현된 ARIA-GCM 프로세서가 올바르게 동작함을 확인하였다.

V. 결 론

블록암호 ARIA 기반의 ARIA-GCM 프로세서를 Verilog HDL로 모델링 하고, Virtex5 FPGA로 구현하여 정상 동작함을 확인하였다. 0.18㎛ 공정의 CMOS 셀 라이브러리로 합성한 결과 최대 동작주파는 100 MHz이며, 20 MHz의 동작주파수에서는 44,986 GE로 구현되었다.

ACKNOWLEDGMENTS

· The authors are thankful to IDEC for EDA software support.

참고문헌

[1] BABAR, Sachin D., et al. Proposed on device capability based authentication using AES-GCM for internet of things (IoT). In: 3rd Springer International ICST Conference on Security and Privacy in Mobile Information and Communication Systems. 2011.

[2] Szalachowski, P., Ksiezopolski, B., & Kotulski, Z. (2010). CMAC, CCM and GCM/GMAC: Advanced modes of operation of symmetric block ciphers in wireless sensor networks. Information Processing Letters, 110(7), 247-251.

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

[4] McGrew, David, and John Viega. "The Galois/counter mode of operation (GCM)." NIST Modes Operation Symmetric Key Block Ciphers, 2005.

[5] KS X 1213-2:2014, 128 bit Block Encryption Algorithm ARIA, Part2: Modes of operation, Korean Agency for Technology and Standards (KATS), 2014.