IoT 디바이스의 인증암호를 위한 AES-GCM 암호코어

성병윤* · 김기쁨* · 신경욱*

*국립금오공과대학교

An AES-GCM Crypto-core for Authenticated Encryption of IoT devices

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

*Kumoh National Institute of Technology

E-mail : sungby0809@kumoh.ac.kr

요 약

본 논문에서는 IoT 디바이스의 인증암호를 위한 AES-GCM 암호코어를 설계하였다. AES-GCM 코어는 블록암호 AES와 GHASH 연산으로 기밀성과 무결성을 동시에 제공한다. 기밀성 제공을 위한 블록암호 AES는 운영모드 CTR과 비밀키 길이 128/256-bit를 지원한다. GHASH 연산과 AES 암호화(복호화)의 병렬 동작을 위해 소요 클록 사이클을 일치시켜 GCM 동작을 최적화 하였다. 본 논문에서는 AES-GCM 코어를 Verilog HDL로 모델링 하였고 ModelSim을 이용한 시뮬레이션 검증 결과 정상 동작함을 확인하였으며 Xilinx Virtex5 XC5VSX95T FPGA 디바이스 합성결과 4,567 슬라이스로 구현되었다.

키워드

AES, GCM, GHASH, Block Cipher, Authenticated Encryption

Ⅰ. 서 론

가전, 스마트 카 및 스마트 헬스에 이르기까지 사물인터넷(Internet of Things)은 사회 전반적인 분야에 보급이 확산 되고 있다. 효율적인 사물의 쓰임을 위해 네트워크를 통하여 정보를 수집, 저장 및 전송하는 IoT의 특성상 보안 위협에 노출될 수 있다. Hewlett Packard 사의 2015년 자료에 따르면 약 70%이상의 IoT가 인터넷 및 로컬네트워크에 암호화 없이 통신이 이루어짐을 발표하였다.[1] 통신환경의 취약점은 침입자의 목표가 되므로 일정수준 이상의 보안성을 갖춰야 한다.

정보의 기밀성과 무결성을 제공하기 위해 블록암호 AES, ARIA, LEA와 인증암호 운영모드 GCM, CCM 등의 여러 가지 블록암호와 운영모드 사용이 권장되고 있다.[2, 3, 4]

본 논문에서는 IoT 디바이스에 적합하며 기밀성과 무결성을 동시에 제공하는 AES-GCM 암호코어를 Verilog HDL로 모델링하였으며 ModelSim을 통하여 시뮬레이션 검증을 완료하였다. Ⅱ장에서는 AES 및 운영모드 GCM의 알고리즘에 대해 간략하게 설명하고, Ⅲ장에서는 AES-GCM 코어의 하드웨어 구성을 설명한다. 시뮬레이션 결과를 Ⅳ에서 기술하고, Ⅴ장에서 결론을 맺는다.

Ⅱ. AES 알고리즘 및 GCM 모드

AES는 Joan Deamen과 Vincent Rijnmen이 개발한 대칭키 암호 알고리즘으로 2001년 12월 NIST에서 DES를 대체할 암호 알고리즘의 공모전에서 최종적으로 선정되었다. AES는 128-bit 평문을 128-bit 암호문으로 출력하는 non-Feistel 알고리즘이다. 비밀키 길이는 128/192/256-bit를 사용하며, 각 비밀키 길이에 대응하는 라운드 수는 프리라운드를 포함하여 11/13/15 라운드이다. 각 라운드는 안정성 제공을 위해 대치(substitution), 치환(permutation), 뒤섞음(mixing), 키 덧셈(key adding)과 같은 4 가지 형태변환을 사용한다.[2]

GCM은 대칭키 블록암호 운영모드로 D. A. McGrew와 J. Viegais에 의해 개발되었다.[5] GCM은 블록암호와 GHASH 연산으로 기밀성과 무결성을 동시에 제공한다. GHASH 연산은 블록암호의 암호화(복호화)와 동시에 동작하는 병렬 동작 및 파이프라인 기법으로 고속 데이터 처리가 가능하다. GHASH 연산은 추가 인증 데이터(AAD), 암호문, 평문 및 데이터 길이정보와 GHASH 키를 유한체 $GF(2^{128})$상에서의 곱으로 인증태그를 생성하여 암호문 및 평문의 무결성을 제공한다.[3]

III. AES-GCM 코어 설계

설계된 AES-GCM 코어는 AES의 운영모드 CTR과 128/256-bit의 비밀키 길이를 지원한다. 그림 1은 AES-GCM 코어의 하드웨어 구성을 블록도로 나타낸 것으로 AES 블록, GCM 블록 및 제어블록으로 구성된다. AES 블록은 라운드 블록, 키스케줄러 및 제어블록으로 구성되며 데이터 패스는 128-bit이다. 128-bit의 평문(암호문)블록이 입력되면 128/256-bit의 비밀키를 사용하여 운영모드 CTR에서 암호화(복호화)된다. 비밀키 길이 128/256-bit에 따라 각각 11, 15 클록 사이클을 소요한다. GCM 블록은 세 개의 128-bit 레지스터(iAES, Text 및 iGHASH), 두 개의 16-bit 레지스터(LenA와 LenC), GHASH 및 덧셈기로 구성된다. GCM에 데이터가 입력되면 추가 인증 데이터일 경우 GHASH 연산을 하며, 평문(암호문)일 경우 초기벡터(IV)를 카운트하여 AES 블록으로 전송한다. 또한 AES 블록으로부터 암호문(평문)이 입력되면 GHASH 연산 한다.

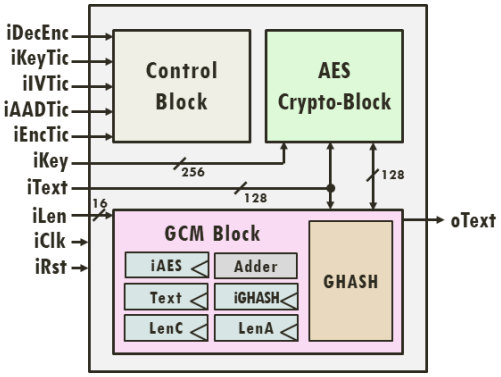

Fig. 1. Architecture of AES‐GCM core

GHASH는 'little endian' 수 체계를 기반으로 한 유한체 GF(2^{128})상의 곱셈기이다. 그림 2는 GHASH의 하드웨어 구성을 블록도로 나타낸 것으로 두 개의 레지스터(HKey_Reg, HTag_Reg), MUX 및 GF_SubMul로 구성된다. 데이터가 입력되면 한 클록 사이클 당 128-bit×12-bit의 데이터가 GF_SubMul에 의해 연산된다. 총 11 클록 사이클이 소요되어 GHASH 연산이 완료된다. GF_SubMul은 128-bit×12-bit 곱을 12개의 PPG로 구현된다. 128-bit×1-bit 곱의 PPG를 하드웨어로 구현하였으며, PPG는 곱 연산 구현을 위한 AND와 모듈러 연산 구현을 위한 XOR로 구성된다.

GHASH 연산은 AES 암호화(복호화) 클록 사이클과 동일한 11 클록 사이클을 소요한다. 클록 사이클 일치는 AES 암호화(복호화)와 GHASH 연산의 병렬 동작에 적합하여 GCM 동작에 효율적이다.

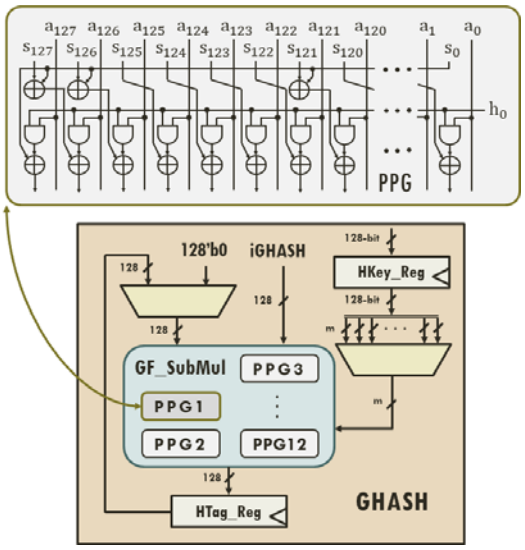

Fig. 2. Architecture of GHASH

IV. 시뮬레이션 기능검증

설계된 AES-GCM 코어는 시뮬레이션을 통한 기능검증을 하였다. 개발자의 기술 보고서에서 제공하는 표 1의[5] 참조 구현 값을 시뮬레이션에 사용하였다. 그림 3은 AES-GCM 코어의 시뮬레이션 결과 값이다. 시뮬레이션 입력은 비밀키, IV, AAD 및 Plaintext 순으로 입력되고 출력은 Ciphertext와 Tag 순으로 출력된다. 출력된 결과 값은 참조 구현 값 표1과 비교하여 정확히 일치함을 확인할 수 있다. 설계된 AES-GCM의 정상 동작을 확인하였다.

Table. 1. Test vectors for AES-GCM[5]

Secret Key	feffe9928665731c6d6a8f9467308308
IV	cafebabefacedbaddecaf88800000000
AAD	feedfacedeadbeeffeedfacedeadbeef abaddad2000000000000000000000000
Plaintext	d9313225f88406e5a55909c5aff5269a 86a7a9531534f7da2e4c303d8a318a72 1c3c0c95956809532fcf0e2449a6b525 b16aedf5aa0de657ba637b3900000000
Ciphertext	42831ec2217774244b7221b784d0d49c e3aa212f2c02a4e035c17e2329aca12e 21d514b25466931c7d8f6a5aac84aa05 1ba30b396a0aac973d58e09100000000
Tag	5bc94fbc3221a5db94fae95ae7121a47

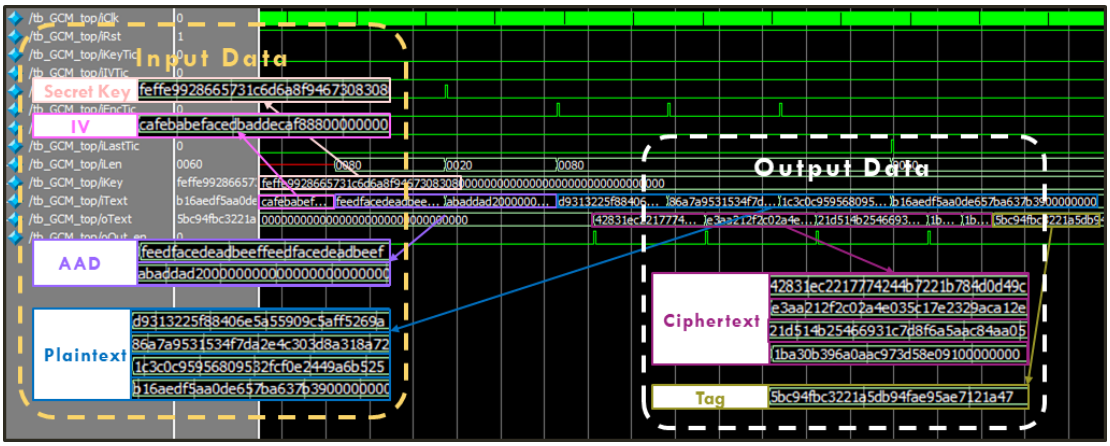

Fig. 3. Screenshot of Simulation results of AES-GCM core for 128-bit key length mode

Ⅴ. 결 론

NIST SP800-38D에서 권고하는 인증 암호화 운영모드 AES-GCM 코어를 설계하였다. Xilinx Virtex5 XC5VSX95T FPGA 디바이스로 합성한 결과 4,567 슬라이스로 구현되었으며, 최대동작 주파수는 140 MHz로 평가되었다.

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).

참고문헌

[1] H. P. “Internet of things research study”, pp. 1-6, 2015

[2] NIST Std. FIPS-197, “Advanced Encryption Standard”, *National Institute of Standard and Technology (NIST)*, pp. 1-51,November 2001.

[3] NIST SP800-38D, “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC”, *National Institute of Standard and Technology (NIST)*, pp. 1-39,November 2007.

[4] K. Kim, W. Cho, Y. Jang, K. Shin “An Efficient Implementation of ARIA and AES Block Cipher Algorithms Supporting Four Modes of Operation” *The Institute of Electronics Engineers of Korea*, pp.1-3, January 2017.

[5] D. McGrew, J. Viega, “The Galois/Counter Mode of Operation (GCM)”, *Updated submission to NIST, Modes of Operation Process,* pp. 1-44, May 2005.

[6] A Satoh, T Sugawara, T Aoki “High Performance Hardware Architectures for Galois Counter Mode”, *IEEE Transactions of computers*, pp. 1-14, July 2009.