An AES-GCM Authenticated Encryption Crypto-Core for IoT Security

Byung-Yoon Sung, Ki-Bbeum Kim, Kyung-Wook Shin
Kumoh National Institute of Technology
E-mail sungby0809@kumoh.ac.kr

Abstract

This paper describes a design of AES-GCM authenticated encryption (AE) crypto-core suitable for IoT security applications. The AES-GCM core provides confidentiality by Counter (CTR) mode of block cipher AES, and it also provides integrity and authenticity by GHASH. AES encryption supports two key lengths of supports key length of 128 and 256-bit. In order to optimize the overall performance, GHASH block was designed to perform Galois field multiplication in 11 clock cycles, resulting in the number of clock cycles between AES encryption and Galois field multiplication are matched. The AES-GCM core was verified by FPGA implementation, and it occupies 35,352 gate equivalents (GEs). The estimated throughput is 332 Mbps with maximum clock frequency of 140 MHz.

Keywords: AES, GCM, GHASH, mode of operation, authenticated encryption, IoT security

1. Introduction

With the rapid development of the wire and wireless communications including Internet of Things (IoT) and wireless sensor network (WSN), information security has become an increasingly important issue. The IoT security has multi-facet issues that include confidentiality of data, secure communication with integrity and authenticity. Since wireless and IoT devices have a limited hardware resource, it is important to design hardware-based lightweight cryptosystems.

NIST standardizes various block ciphers and mode of operations to provide confidentiality and integrity of information. Until recently, many block ciphers and mode of operations have been proposed including AES, ARIA, PRESENT, LEA, GCM, CCM, and so on [1, 2, 3].

This paper proposes a hardware design of AES-GCM core suitable for IoT device security. Section 2 briefly introduces the AES-GCM authenticated encryption and GHASH. Section 3 explains hardware design of AES-GCM core, and FPGA verification results are discussed in section 4.

2. AES-GCM Authenticated Encryption

Authenticated encryption (AE) scheme is a form of symmetric-key cryptography that provides integrity and authenticity as well as confidentiality. Six AE modes including Counter with CBC-MAC (CCM), Encrypt-then-MAC (EtM), Galois/Counter Mode (GCM), Key Wrap have been standardized in ISO/IEC 19772:2009 [4].

GCM developed by D. A. McGrew and J. Viegais [5] is a mode of operation for symmetric key block ciphers. It was designed originally as a way of supporting very high data rates, since it can take advantage of pipelining and parallel processing techniques to bypass the limits imposed by feedback MAC algorithms. Recently, GCM is being specified for use in lower rate applications due to its ease of use and scalability.

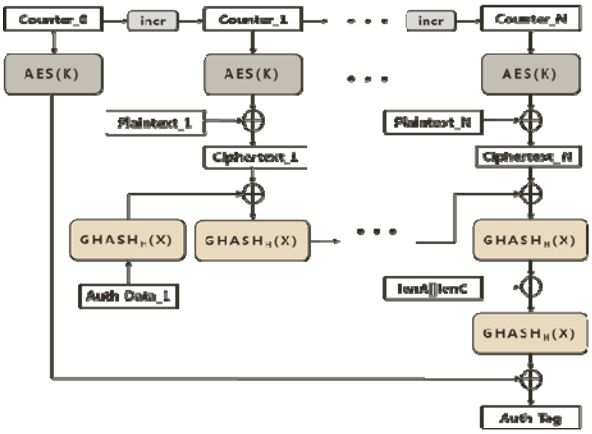


Figure 1: AES–GCM algorithm

Figure 1 depicts the AE encryption operation that shows a case with only a single block of AAD (labeled Auth Data 1) and N blocks of plaintext. AES(K) denotes the block cipher encryption using the secret key K, and $\mathrm{GHASH}_H(X)$ denotes Galois field multiplication in $GF(2^{128})$ by hash key H, and incr denotes the counter increment function.

AES-GCM has been specified for use in a number of recent standards including IEEE 802.11ae (MACsec), NSA Suite B Cryptography.

Confidentiality is obtained by CTR mode of operation of block cipher AES. GHASH function provides integrity through authentication tags generated by multiplying additional authentication data (AAD), ciphertext, plaintext, and data length information with GHASH key. GHASH function $GHASH_H(X)$ calculates multiplication in Galois field GF (2^{128}) defined in (1). $X = X_1 \| X_1 \| \ldots \| X_{m-1} \| X_m$ is obtained as the concatenation of ciphertext, AAD and the length of those two data, and H denotes the hash subkey generated by applying block cipher to the zero block.

$$X_1 \cdot H^m \oplus X_2 \cdot H^{m-1} \oplus \ldots \oplus X_{m-1} \cdot H^2 \oplus X_m \cdot H \qquad (1)$$

3. AES-GCM crypto-core design

Figure 2 shows the AES-GCM crypto-core designed in this paper, which has two crypto-blocks of AES block and GHASH block, four 128-bit registers (iAES, HKey, Text and iGHASH), two 16-bit registers (LenA and LenC), adders and XORs, and control block. The AES crypto-block performs encryption of 128-bit data block with 128-bit or 256-bit secret key. The round block and key scheduler was designed with 128-bit data-path, resulting that encryption/decryption of a data block takes 11 or 15 clock cycles depending on the key length.

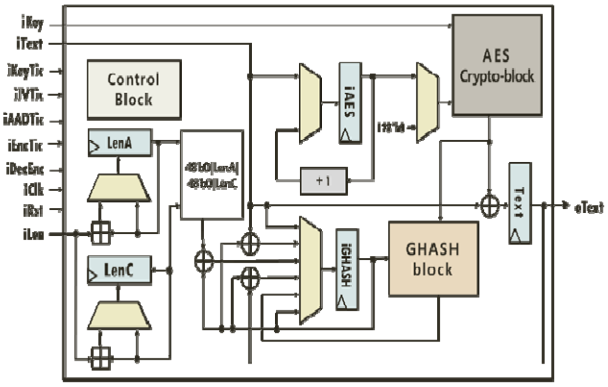


Figure 2: Architecture of AES–GCM core

Figure 3 shows GHASH block designed in this paper, which performs Galois field multiplication based on 'little endian' method that processes multiplication from left to right. It consists of GF_SubMul block, HKey_Reg, and HTag_Reg. The GF_SubMul block is composed of twelve PPGA blocks. PPGA is a combinational logic of AND gates for partial product generation and XOR gates for addition and reduction. Each PPGA block processes one partial product of 128-bit. HKey_Reg stores hash subkey of 128-bit to be used for multiplication, and HTag_reg stores internal result of hash tag value obtained from partial product addition.

As can be seen in Figure 1, the ciphertext blocks coming out from AES encryption enter into GHASH block for Galois field multiplication. If there is a mismatch in the number of clock cycles required for AES encryption and GHASH multiplication, overall performance will be degraded. Therefore, it is important to make those two blocks work simultaneously without any idle cycles in order to optimize overall performance. Considering AES encryption consumes 11, 15 clock cycles depending on secret key length, GHASH block was designed to use 11 clock cycles for Galois field multiplication. To this end, GHASH block was designed to have twelve PPGA blocks working concurrently. Each PPGA block has 128-bit data-path to process one partial product of 128-bit. With our design of GHASH, twelve partial products are processed in a clock cycle, thus 128-bit Galois field multiplication can be calculated in 11 clock cycles, which means that the number of clock cycles between AES encryption and Galois field multiplication are matched [6].

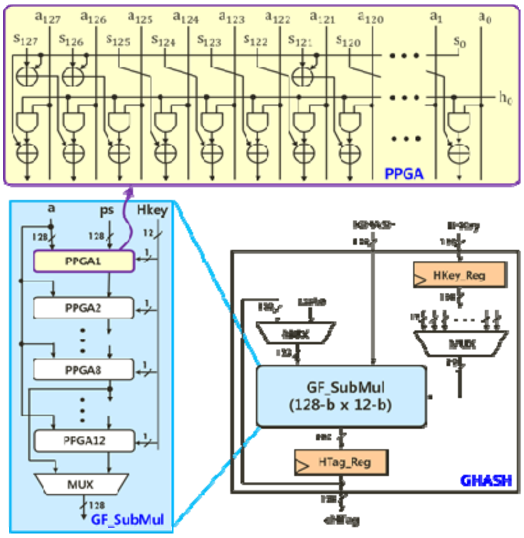


Figure 3: Architecture of GHASH Block

Figure 4 shows the timing diagram of the encryption mode of AES-GCM core. The AES block and HASH block operate simultaneously, and they consume 11 clock cycles to process one data block.

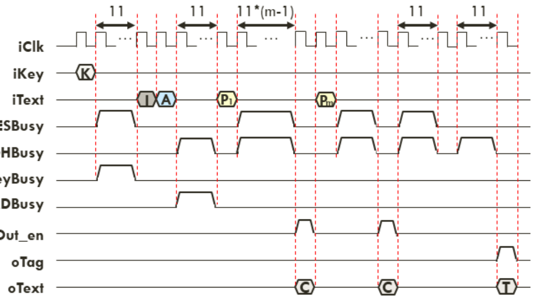


Figure 4: Timing diagram of AES-GCM core

4. FPGA verification

The AES-GCM core designed in Verilog HDL was verified by FPGA implementation. Verification setup consists of Virtex5 FPGA board (XC5VSX-95T), UART interface, and GUI software as shown in Figure 5. Table 1 lists the test vectors used. Secret key, IV, AAD, and plaintext blocks are loaded from PC to FPGA through RS232C port. The AES-GCM core implemented on FPGA encrypts them to make ciphertext obtained by AES encryption, and Tag data obtained by GCM mode of operation. The ciphertext and Tag data are sent back to PC to be displayed on screen. In addition, the AES-GCM core decrypts ciphertext to make decrypted (i.e., plaintext) obtained by AES decryption, and Tag data obtained by GCM mode of operation. Figure 6 shows the screenshot of FPGA verification results of AES-GCM core for 256-bit key length mode. As can be seen in Figure 6, the decrypted ciphertext is identical to the plaintext used for encryption. Two Tag data obtained by GCM encryption and decryption are matched. These FPGA verification results confirm that the AES-GCM core is working correctly.

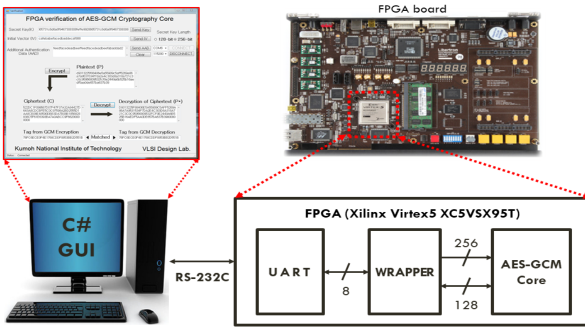
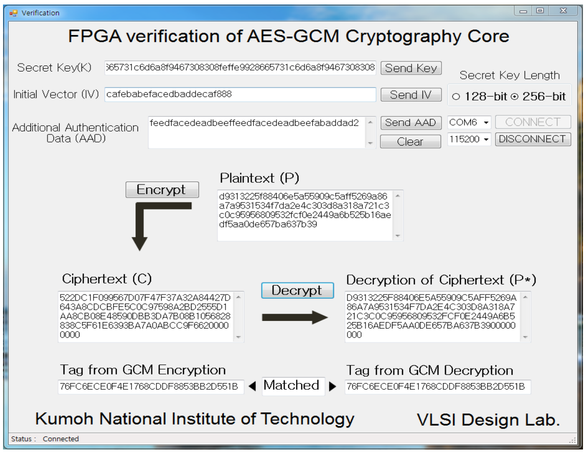


Figure 5: FPGA Verification setup

Table 1: Test vectors for AES-GCM [2]

Secret Key	feffe9928665731c6d6a8f9467308308 feffe9928665731c6d6a8f9467308308
IV	cafebabefacedbaddecaf888
AAD	Feedfacedeadbeeffeedfacedeadbeef abaddad2
Plaintext	d9313225f88406e5a55909c5aff5269a 86a7a9531534f7da2e4c303d8a318a72 1c3c0c95956809532fcf0e2449a6b525 b16aedf5aa0de657ba637b39
Ciphertext	522dc1f099567d07f47f37a32a84427d 643a8cdcbfe5c0c97598a2bd2555d1aa 8cb08e48590dbb3da7b08b1056828838 c5f61e6393ba7a0abcc9f662
Tag	76fc6ece0f4e1768cddf8853bb2d551b



FPGA verification of AES-GCM Cryptography Core

Secret Key(K) 665731c6d6a8f9467308308feffe9928665731c6d6a8f9467308308

Initial Vector (IV) cafebabefacedbaddecaf888

Secret Key Length ○ 128-bit ● 256-bit

Additional Authentication Data (AAD) feedfacedeadbeeffeedfacedeadbeefabaddad2

COM6
115200

Plaintext (P)
d9313225f88406e5a55909c5aff5269a86
a7a9531534f7da2e4c303d8a318a721c3
c0c95956809532fcf0e2449a6b525b16ae
df5aa0de657ba637b39

Ciphertext (C)
522DC1F099567D07F47F37A32A84427D
643A8CDCBFE5C0C97598A2BD2555D1
AA8CB08E48590DBB3DA7B08B1056828
838C5F61E6393BA7A0ABCC9F6620000
0000

Decryption of Ciphertext (P*)
D9313225F88406E5A55909C5AFF5269A
86A7A9531534F7DA2E4C303D8A318A7
21C3C0C95956809532FCF0E2449A6B5
25B16AEDF5AA0DE657BA637B3900000
000

Tag from GCM Encryption 76FC6ECE0F4E1768CDDF8853BB2D551B ◀ Matched ▶ Tag from GCM Decryption 76FC6ECE0F4E1768CDDF8853BB2D551B

Kumoh National Institute of Technology VLSI Design Lab.

Status : Connected

Figure 6: Screenshot of FPGA verification results of AES-GCM core for 256-bit key length mode

4. Conclusion

An AES-GCM crypto-core that provides authenticated encryption mode of operation was designed and verified by FPGA implementation. The AES-GCM core synthesized with a 0.18um CMOS cell library occupies 35,352 GE. The estimated maximum clock frequency is 140 MHz, and throughput is 332 Mbps.

Acknowledgement

•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 also are thankful to IDEC for EDA software support.

References

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

[2] 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.

[3] 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.

[4] ISO/IEC 19772:2009, “Information technology - Security techniques - Authenticated encryption”, *International Organization for Standardization (ISO)*, March 2013.

[5] D. McGrew, J. Viega, “The Galois/Counter Mode of Operation (GCM)”, NIST Modes Operation Symmetric Key Block Ciphers, pp. 1-44, May 2005.

[6] Y. Hori, A. Satoh, H. Sakane, K. Toda “Advances in Information and Computer Security” *International Workshop on Security (IWSEC),* pp. 261-278, 2008