LETTER *Special Section on Trust, Security and Privacy in Computing and Communication Systems*

Efficient Sequential Architecture of AES CCM for the IEEE 802.16e

Jae Deok JI[†], ***Nonmember***, **Seok Won JUNG**[††a)], ***Member***, ***and*** **Jongin LIM**[†††], ***Nonmember***

SUMMARY In this paper, we propose efficient sequential AES CCM architecture for the IEEE 802.16e. In the proposed architecture, only one AES encryption core is used and the operation of the CTR and the CBC-MAC is processed concurrently within one round. With this design approach, we can design sequential AES CCM architecture having 570 Mbps@102.4 MHz throughput and 1,397 slices at a Spartan3 3s5000 device.

key words: *cryptography, communication system security, integrated chip design, FPGA*

1. Introduction

The Counter with the Cipher Block Chaining-Message Authentication Code (CCM) mode proposed by Whiting et al. is a mode of operations for symmetric block ciphers [1]. This mode combines two block cipher modes: the counter (CTR) mode and the cipher block chaining-message authentication code (CBC-MAC) mode. In the IEEE 802.16e and IEEE 802.11i wireless network, the CCM mode is used for message encryption and authentication using advanced encryption standard (AES).

Depending on the architecture for hardware implementation of the AES CCM, CTR and CBC-MAC operations may be processed in a parallel mode [2], [3] or in a sequential mode [4]. In a parallel mode, encryption for the CTR and the CBC-MAC are performed concurrently using two AES encryption cores, so throughput can be enhanced but the hardware resource utilization is also increased.

To reduce the amount of hardware resources, the sequential AES CCM architecture is suggested [4]. In sequential mode, only one AES encryption core is used and the operation of the CTR and the CBC-MAC is processed serially. The hardware resource utilization in sequential mode is much less than in parallel mode but the throughput is much less than in parallel mode. Due to the CBC feedback nature of CCM mode, an iterative fashion has been adopted to implement the AES core. Since the AES core optimization used in sequential mode is difficult, the control logic of AES CCM was mainly optimized rather than AES core logic [4].

In this paper, we propose sequential AES CCM architecture which improves throughput to compare previous sequential architecture. The SubBytes logic of AES encryption core is generally implemented using composite field logic to reduce the resource requirements. But the delay of the critical path is increased due to the complexity of the composite field arithmetic logic. To optimize AES core used in sequential mode, we divide composite field logic of SubBytes into two sub-stages to shorten the critical path delay and to make CBC-MAC and CTR mode processed concurrently within one round operation.

In our previous related work [5], the location of SubBytes dividing point was not optimal point and SubBytes logic in the key scheduling block used the SBOX look-up table. In this paper, in order to improve sequential AES CCM architecture, we have searched the optimal point achieving maximal throughput per a slice for a targeting device. In our approach, the critical path delay of the AES CCM logic has varied according to the location of SubBytes dividing point. Candidates of a dividing point are chosen nearby the half path of the multiplicative inverse block. We compare throughput/area ratios for candidates. To reduce the hardware resource utilization, SubBytes logic in the key scheduling block is also implemented using SubBytes composite field logic divided into 2 parts. With this design approach, we can design sequential AES CCM architecture having 0.408 throughput/area ratio. The suggested architecture is targeted to Spartan FPGA devices.

2. Proposed Architectures

2.1 AES Encryption Core Architecture

In the sequential architecture suggested by Bae [4], it uses one round module iteratively which performs a round of AES every clock cycle. CTR and CBC-MAC mode are processed alternatively using this round module, so it takes two clock cycles for one round operation. To shorten critical path delay, we divide one round into two parts which are performed concurrently at each clock cycle. Due to the CBC feedback nature of CCM, it can't divide one round into more than 3 parts. In our architecture, CTR and CBC-MAC mode use each part at the same clock cycle. The total cycles of one round operation in our architecture are two clock cycles which are the same as the Bae's architecture but the critical path is reduced to near half. Thus we obtain double throughput compared with throughput of Bae's architecture.

There are two implementation types of SubBytes logic divided into two parts to make sub-stage structure. One has

Manuscript received March 16, 2011.
Manuscript revised June 29, 2011.
[†]The author is with KISA, Songpa-Gu, Seoul, 138–950 Korea.
[††]The author is with Mokpo National Univ., Jeonnam, 534–729 Korea.
[†††]The author is with Korea Univ., Seoul, 136–701 Korea.
a) E-mail: jsw@mokpo.ac.kr
DOI: 10.1587/transinf.E95.D.185

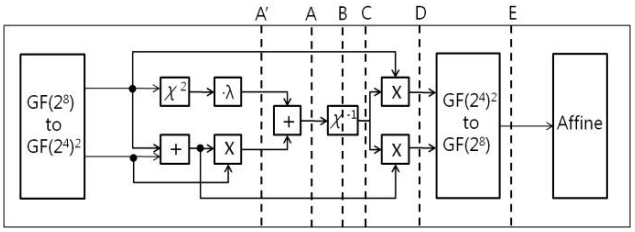

Fig. 1 Locations of dividing point for SubBytes.

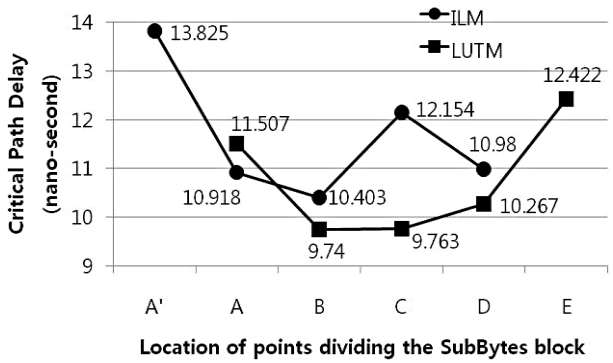

Fig. 2 Critical path delays according to dividing points.

the GF$(2^2)^2$ multiplicative inverse logic implemented by using composite field arithmetic logic (Inverse Logic Method, ILM) and another has the GF$(2^2)^2$ multiplicative inverse logic implemented by using a substitution table (Look-Up Table Method, LUTM). To find the optimal point achieving maximal throughput per a slice, we have synthesized the AES core logic as changing the location of SubBytes dividing point as shown in Fig. 1.

Figure 2 shows the critical path delay according to the SubBytes dividing points. The minimum critical path delay is obtained at B for LUTM implementation (9.74 ns). Figure 3 shows the hardware resource usage according to the dividing points. The minimum value is obtained at A for LUTM implementation (1275 slices). The throughput/area ratio is calculated for each point and the maximum ratio (0.408 Mbps/slices) is obtained at C for LUTM. From this result, the LUTM SubBytes logic divided at C point is the best logic to implement sequential AES Core. This SubBytes logic is used for the round transformation and key scheduler of the proposed AES core.

2.2 CCM Mode Implementation

Figure 4 shows the block diagram of the proposed CCM module. The AES CONTROL block and STATE MACHINE block perform management functions for packet encryption or decryption including communications with the external module and generation of CCM algorithm parameters. The AES CORE is the proposed AES encryption core.

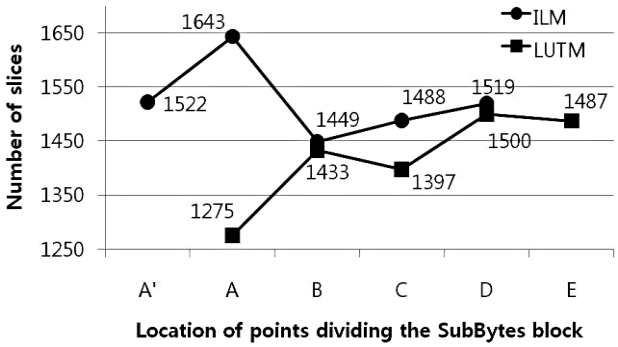

Fig. 3 Hardware resource usages according to dividing points.

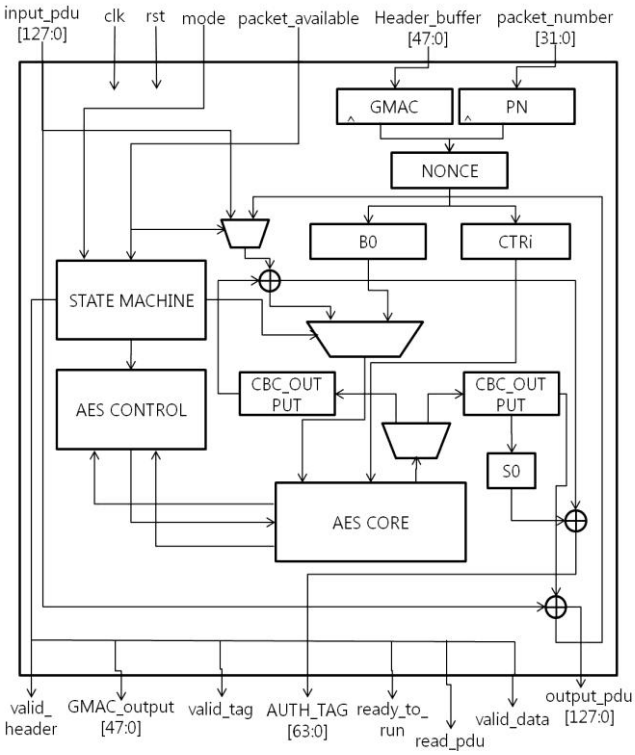

Fig. 4 Block diagram of the proposed CCM core.

Table 1 Comparison with other sequential implementation approach.

Author	Target Device	Device Utilization	Throughput	Throughput/ Area
D.H.Bae [4]	Altera Stratix	5605 (Logic Cell)	285Mbps @50Mhz	0.051
Our Design	Spartan3 3s5000	1397 (Slice)	570Mbps@ 102.4Mhz	0.408

3. Implementation Results

Table 1 summarizes the resource utilization and the timing constraint of our design and other work. As it can be seen, our design is more efficient in terms of device utilization and minimum period than previous sequential design [4].

Acknowledgments

This paper was supported by Research Funds of Mokpo National University in 2009.

References

[1] D. Whiting, R. Housley, and N. Ferguson, "Counter with CBC-MAC (CCM)," RFC 3610, 2003.
[2] A. Aziz and N. Ikram, "An FPGA-based AES-CCM crypto core for IEEE 802.11i architecture," Internal Journal of Network Security, vol.5, no.2, pp.224–232, 2007.
[3] I.A. Badillo, C.F. Uribe, R. Cumplido, and M.M. Sandoval, "Efficient hardware architecture for the AES-CCM protocol of the IEEE 802.11i standard," Computers and Electrical Engineering, Elsevier, 2010.
[4] D.H. Bae, "An efficient design of CCMP for robust security network," Information Security and Cryptology-ICISC 2005, LNCS 3935, pp.352–361, 2006.
[5] J.D. Ji, S.W. Jung, E.A. Jun, and J.I. Lim, "Efficient sequential architecture for the AES CCM mode in the 802.16e standard," 2009 Second International Conference on Intelligent Networks and Intelligent Systems, 2009.