A Compact, Ultra-Low Power AES-CCM IP Core for Wireless Body Area Networks

Van-Phuc Hoang[1], Thi-Thanh-Dung Phan and
Van-Lan Dao
Le Quy Don Technical University
236 Hoang Quoc Viet Str., Hanoi, Vietnam
Email: [1]phuchv@mta.edu.vn

Cong-Kha Pham
Department of Engineering Science,
The University of Electro-Communications
1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585, Japan
Email: pham@ee.uec.ac.jp

***Abstract*—This paper presents a compact, ultra-low power AES-CCM authenticated encryption IP core for WBANs by combining a low area 8-bit AES encryption core, iterative structure and other optimized circuits. The proposed AES-CCM IP core can be used for the message security at the MAC level, e.g. message encryption and authentication, based on AES forward cipher function with a 128-bit key for counter and cipher block chaining modes of operations. The implementation results show that the proposed AES-CCM IP core achieves a very high resource efficiency and ultra-low power consumption while meeting the requirement of operation speed in WBANs.**

Keywords*— low power; AES-CCM; authenticated encryption; ASIC

I. INTRODUCTION

IEEE 802.15.6 is a new standard for wireless body area networks (WBANs) which tend to provide short range, wireless communications in a variety of medical and non-medical applications as depicted in Fig.1. IEEE 802.15.6 standard constrains the devices to operate with very low transmit power for the safety reasons. Moreover, WBANs supports a high quality of service such as the emergency messaging. Hence, it requires a strong security level for some transactions with essential information [1].

Advanced Encryption Standard (AES) is a highly recommended security standard for data encryption [2]. In [3], the authors also summarized some main security requirements and introduced some techniques to protect the system from possible attacks by several modes of operation such as encryption only (AES-CTR), authentication only (AES-CBC-MAC) and encrypted authentication (AES-CCM).

In IEEE 802.15.6 standard for WBANs, AES-CCM is recommended for authenticated encryption purpose [1]. However, it may lead to the high hardware complexity in the context of area and power constrained wearable and implant devices in WBANs. Hence, compact and ultra-low power AE hardware cores are highly desired. Moreover, due to the increasing demand on mobile and wearable electronic devices, the requirement of low area and power efficient circuits and modules is becoming essential. In literature, there is not any paper presenting the hardware inplementation of ultra-low power AES-CCM core for IEEE 802.15.6 WBAN standard.

Therefore, this work focuses on the implementation of a low area, ultra-low power AES-CCM core for WBANs to provide both message encryption and message authentication. Especially, this paper aims to propose a new efficient architecture and improved ultra-low power AES-CCM implementation using an advanced 65nm CMOS technology for this emerging network standard. The main contribution of this paper is a compact, ultra-low power AES-CCM IP core for WBANs by combining a low area 8-bit AES encryption core, iterative structure and other optimized circuits.

The rest of this paper is organized as follows. Section II reviews AES-CCM mode and propose an iterative AES hardware architecture. Section III presents the iteration structure of AES-CCM AE core. Section IV shows the implementation results and discussions. Finally, section V concludes the paper.

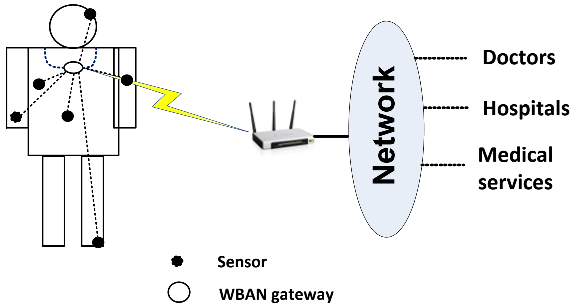


Fig. 1. An application of WBAN in medical system.

II. AES ENCRYPTION CORE ARCHITECTURE FOR AES-CCM IP CORE DESIGN

AES-CCM was specified in NIST Special Publication 800-38C [2] in which AES block cipher core is used for the purpose of authenticated encryption. The bit order of each input block is formatted as [1]-[2]. The AES-CCM operation consists of two related processes which are generation/ encryption and decryption/verification. Firstly, in the generation/encryption process, an initial block B_0, and Payload blocks ($B_1 \div B_n$) are used in CBC mode, as shown in Fig. 2, to generate a message authentication code (MAC). Then, CTR mode whose inputs are Counter Blocks CTR_i, as shown in Fig.3, is applied to generate the cipher-text. The size of received cipher-text is equal to sum of the length of payload and the length of MAC. In decryption/verification process, counter mode decryption is applied to cipher-text to recover

978-1-5090-3561-8/16/$31.00 ©2016 IEEE

the MAC and the corresponding payload; then, CBC mode is applied to the payload, the associated data, and the nonce to verify the correctness of the received MAC. A successful verification indicates that the payload and its associated data come from the same source with access to the key so that a MAC provides a high level of authentication [2].

Since AES encryption block is the essential part in the AES-CCM core, the choice for its architecture is very important. Previous papers [4]-[5] implemented low area AES encryption cores by using the 8-bit AES core architecture and an optimized S-box structure. For FPGA implementation, using block RAMs to implement the 8-bit AES core is also a promising solution to reduce AES core area, as shown in [6]. The penalty of this solution is that it may lead to the lower throughput due to its iterative manner. Then, using a pipeline AES structure is a promising approach to improve the throughput, such as the AES core in [7], although this core area is 3.6 times larger than the iterative looping structure. Some other papers [8]-[12] also mentioned some improved implementations of AES-CCM core for different applications.

On the other hand, it is important to note that a typical data rate in WBANs of up to 10Mbps can meet the speed requirement for most of entertainment and healthcare services [1]. Since throughput is not the most important issue in WBANs, in this work, iteration structure is used to minimize the hardware resource and to meet the requirement of low power consumption as well. The above mentioned 8-bit AES architecture is used to process 128-bit AES encryption blocks, as shown in Fig.5 in which the parallel to serial converter and other additional components are also used.

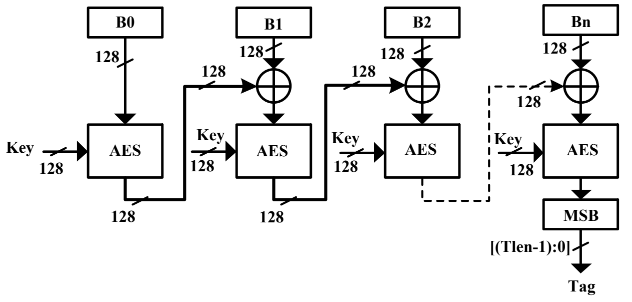


Fig. 2. Block diagram of the CBC mode.

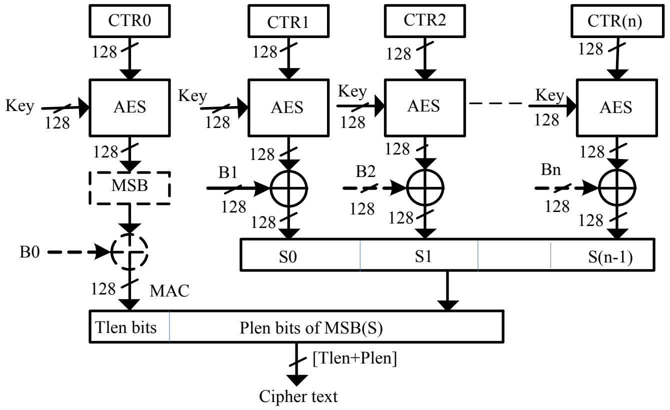


Fig. 3. Block diagram of the CTR mode.

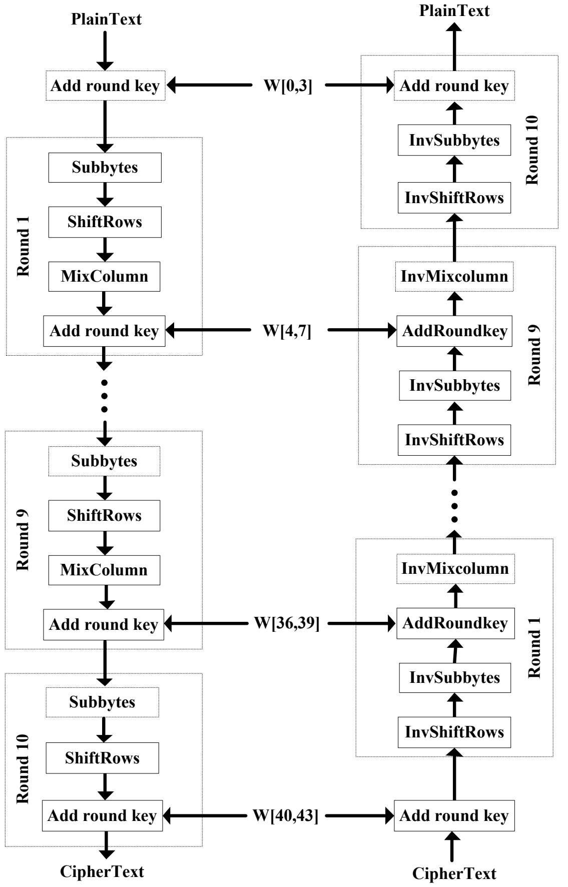


Fig. 4. Standardized AES encryption and decryption algorithms.

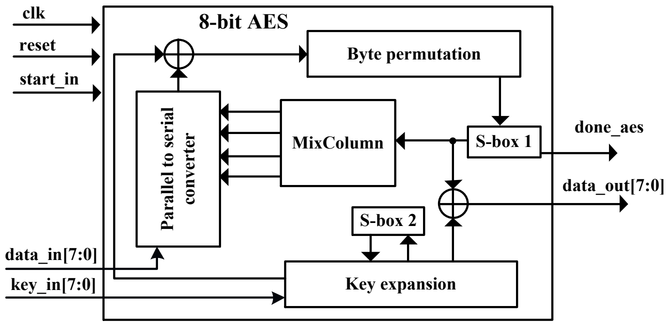
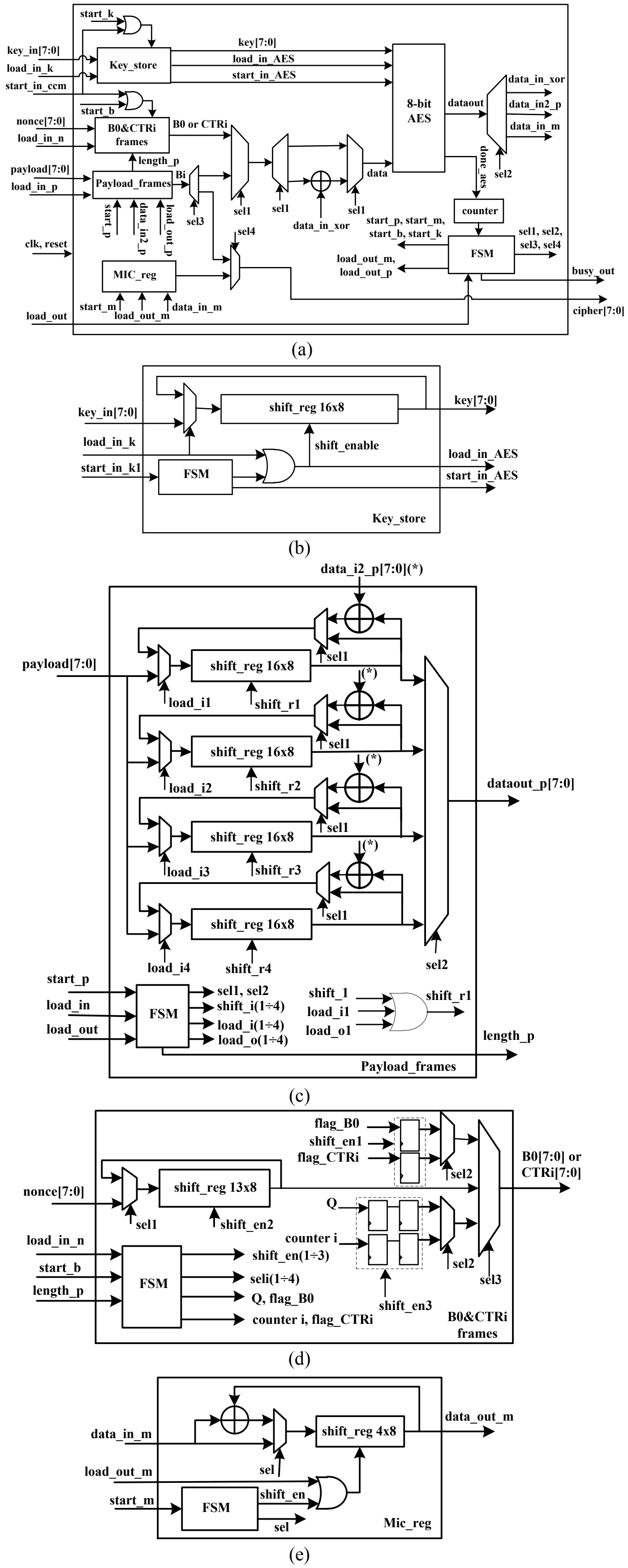


Fig. 5. The 8-bit AES encryption core architecture [5].

III. AES-CCM CORE DESIGN

From the above discussions, to reduce the area as well as the power consumption of AES-CCM core, the iteration structure is employed with only one AES block to implement AES-CCM operation. The AES-CCM core architecture is shown as Fig.6. The general block diagram is depicted in Fig.6a and its building blocks are shown more detail in other figures such as key_store (Fig.6b), payload_frame (Fig.6c), shift registers, multiplexers and other blocks. Fig. 6d is the block to generate B0 and CTRi frames. The tag result is stored as shown in Fig.6e. All operations in this core are controlled by a finite state machine (FSM) as shown in Table I.



(a)

(b)

(c)

(d)

(e)

Fig. 6. Proposed 8-bit AES-CCM IP core architecture.

TABLE I. GENERATED SIGNALS BY FSM FOR PROPOSED AES-CCM IP CORE.

Round	start_b	start_p	start_k	start_m	sel1	sel2
0	0	0	0	0	0	00
$1 \div x$	0	1	1	0	1	00
$x+1$	0	1	1	1	1	10
$x+2$	1	0	1	1	0	10
$(x+3) \div 2x-1$	1	1	1	0	0	01
$2x$	0	1	0	0	-	-

x=[Plen/128]

TABLE II. SIGNALS IN PROPOSED AES-CCM IP CORE.

Signal	Direction	Function
clk, reset	Input	System clock and reset
load_in_k	Input	Control signal to load Key
load_in_p	Input	Control signal to load Payload
load_in_n	Input	Control signal to load Nonce
load_out	Input	To get data output
start_in_ccm	Input	Control signal to start the processing of encrypted authentication
key_in	Input	Key input
nonce	Input	Nonce input
payload	Input	Payload input
cipher	Output	Data output consists of MAC and encrypted payload
busy_out	Output	To indicate that the output is ready to read

IV. IMPLEMENTATION RESULTS

The AES-CCM encryption core was implemented with VHDL code, simulated with ModelSim-Altera 10.1d and synthesized with Xilinx FPGA devices. Then, the proposed AES-CCM core was implemented with the ultra-low power 65nm CMOS standard library using Synopsys Design Complier tool as well. RTL simulation and post-synthesis simulation were also done with Synopsys VCS tool. The function of each signal in the proposed AES-CCM core is described in Table II. An example of a test vector for AES-CCM core is shown in Table III in which Klen is the length of *key_in*. In our simulation test case, the following parameters are chosen as: Klen=128, Nlen=104, Tlen=32 and Plen=256. The cipher output includes 288 bits. With the input data as shown in this table, the proposed AES-CCM core requires 6 AES encryption loops (i.e. 960 clock cycles) to complete one authenticated encryption operation.The simulation results have confirmed the correct operation of proposed AES-CCM core.

The FPGA implemented results of AES-CCM core designs are shown in Table IV in which all the designs were synthesized and targeted on different Xilinx FPGA devices. As pointed out in this table, when compared with other designs, our proposed AES-CCM core is more area efficient but the maximum clock frequency is little lower in some cases. Also, the ASIC implementation results in Table V show that with the low area of 8.1kgates and the ultra-low power consumption of 3.98µW/MHz, the proposed AES-CCM core can be employed for energy and resource constraint applications such as WBANs. The speed of proposed AES-CCM core (149MHz) is also sufficient for IEEE 802.15.6 WBANs [1].

TABLE III. AN EXAMPLE OF A TEST VECTOR FOR PROPOSED AES-CCM IP CORE.

Key_in (128-bit)	0x40, 0x41, 0x42, 0x43, 0x44, 0x45, 0x46, 0x47, 0x48, 0x49, 0x4a, 0x4b, 0x4c, 0x4d, 0x4e, 0x4f
Nonce (104-bit)	0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19, 0x1a, 0x1b, 0x00
Payload (256-bit)	0x20, 0x21, 0x22, 0x23, 0x24, 0x25, 0x26, 0x27 0x28, 0x29, 0x2a, 0x2b, 0x2c, 0x2d, 0x2e, 0x2f, 0x30, 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
Cipher_text (288-bit)	0xd5, 0x2a, 0x25, 0x43, 0xb9, 0x0d, 0x01, 0xf7, 0x6e, 0x0f, 0xd8, 0xb1, 0x3c, 0x97, 0x13, 0x3f, 0x9c, 0x46, 0x15, 0x9a, 0x9a, 0xaa, 0x73, 0x2e, 0xea, 0x26, 0x04, 0x58, 0x24, 0x30, 0x48, 0xd0, 0x8f, 0x1d, 0x92, 0x4e

TABLE IV. FPGA IMPLEMENTATION RESULTS OF PROPOSED AES-CCM IP CORE COMPARED WITH OTHERS.

Design	FPGA Device	Number of Slices	BRAM/ ROM	Speed (MHz)
[7]	3S4000FG900	2154	2048 bit	-
Our	**3S4000FG900**	**507**	**3320 bit**	**51.1**
[8]	XC5VLX50F676	3942	10 blocks	114
Our	**XC5VLX50-2F676**	**563**	**3320 bit**	**139**
[9]	XC3S700AFG484	3435	10 BRAMs	63.1
Our	**XC3S700AFG484**	**507**	**3320 bit**	**70.8**
[10]	XC3S700A	1803	4 ROMS	105
Our	**XC3S700A**	**507**	**3320 bit**	**70.8**
[12]	XC7A200TL	80	11 BRAMs	91.5
Our	**XC7A200TL**	**554**	**76 bit**	**177.4**

TABLE V. ASIC IMPLEMENTATION RESULTS OF PROPOSED AES-CCM IP CORE COMPARED WITH OTHERS.

Design	In [11]	This work
Technology	250nm CMOS	65nm CMOS
Area (kgates)	14.9	8.1
Speed (MHz)	-	149
Throughput (Mbps)	54	119.2
Power (µW/MHz)	440	3.98

V. CONCLUSIONS

In this paper, we have presented a compact, ultra-low power AES-CCM authenticated encryption IP core for IEEE 802.15.6 WBANs with an efficient iterative architecture employing optimized components and design techniques. The implementation results in both FPGA and ASIC hardware platforms shown that with the merit of low area and ultra-low power consumption, the proposed AES-CCM IP core can be employed for the emerging WBANs and other applications. In the future, we will apply the proposed AES-CCM IP core for a WBAN application.

ACKNOWLEDGEMENT

This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.02-2015.20.

REFERENCES

[1] "IEEE standard for local and metropolitan area networks - Part 15.6: Wireless Body Area Networks," *IEEE Std 802.15.6*, 2012.

[2] "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality," *NIST Special Publication 800-38C,* May 2004.

[3] S. Saleem, S. Ullah and K. S. Kwak, "Towards security issues and solutions in wireless body area networks," *Proc. 2010 6th International Conference on Networked Computing (INC)*, pp. 1-4, May 2010.

[4] P. Hamalainen, T. Alho, M. Hannikainen, T.D. Hamalainen, "Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core," *Proc. 9th EUROMICRO Conference on Digital System Design: Architectures, Methods and Tools (DSD2006)*, pp.577-583, 2006.

[5] Van-Lan Dao, Anh-Thai Nguyen, Van-Phuc Hoang and Tuan-Anh Tran "An ASIC Implementation of Low Area AES Encryption Core for Wireless Networks," *Proc. 2015 International Conference on Communications, Management and Telecommunications (ComManTel)*, pp. 99-102, Dec. 2015.

[6] Hi-Jeng Chang, Chi-Wu Huang, Hung-Yun Tai, Mao-Yuan Lin and Teng-Kuei Hu, "8-bit AES FPGA Implementation using Block RAM," *Proc. 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON)*, pp.2654-2659, Nov. 2007.

[7] R. V. Kshirsagar, M. V. Vyawahare, "FPGA Implementation of High speed VLSI Architectures for AES Algorithm," *2012 Fifth International Conference on Emerging Trends in Engineering and Technology,* pp.239-242, Nov. 2012.

[8] Emmanuel Lopez-Trejo, Francisco Rodriguez-Henriquez, and Arturo Diaz-Pierez, "An FPGA Implementation of CCM Mode Using AES," *Information Security and Cryptology - ICISC 2005*, *Lecture Notes in Computer Science*, *Springer*, vol.3935, pp.322-334, Dec. 2005.

[9] Ignacio Algredo-Badillo, Claudia Feregrino-Uribe, Rene Cumplido, Miguel Morales-Sandoval, "FPGA Implementation Cost and Performance Evaluation of the IEEE 802.16e and IEEE 802.11i Security Architectures Based on AES-CCM," *Proc. 5th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE 2008*), pp.304-309, Nov. 2008.

[10] Jae Deok Ji, Seok Won Jung, "Efficient Sequential Architecture for the AES CCM Mode in the 802.16e Standard," *Proc. 2009 Second International Conference on Intelligent Networks and Intelligent Systems,* pp.253-256, Nov. 2009.

[11] Lian Huai, Xuecheng Zou, Zhenglin Liu, Yu Han, "An Energy-Efficient AES-CCM Implementation for IEEE802.15.4 Wireless Sensor Networks," *Proc. 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, pp.394-397, Apr. 2009.

[12] Antonio de la Piedra, Abdellah Touhafi and An Braeken, "Compact implementation of CCM and GCM modes of AES using DSP blocks," *Proc. 23rd International Conference on Field programmable Logic and Applications*, pp.1-4, Sep. 2013.