An Efficient FPGA Implementation of AES-CCM Authenticated Encryption IP Core

Thi-Thanh-Dung Phan, Van-Phuc Hoang and Van-Lan Dao
Le Quy Don Technical University, 236 Hoang Quoc Viet Str., Hanoi, Vietnam
Email: dungphansqtt@gmail.com; phuchv@mta.edu.vn; kqha1025@gmail.com

***Abstract*— This paper presents an efficient AES-CCM IP core by combining a compact 8-bit AES encryption core and iterative structure. The AES-CCM core is used for message security at the MAC level, e.g. message authentication and encryption, based on AES forward cipher function for 128-bit keys operating with counter mode and cipher block chaining mode. The implementation results on FPGA show that the proposed AES-CCM core has higher resource usage efficiency compared with other designs.**

Keywords*— *AES-CCM; authenticated encryption; FPGA

I. INTRODUCTION

Recently, wireless networks are developed more and more so that they provide a wide range of applications and connectivity. The emerging IEEE 802.15.6 wireless body area networks (WBANs) tend to provide short range, wireless communications in a variety of medical and non-medical applications such as shown in Fig. 1. WBANs require the devices to operate with very low transmit power for safety reasons. Moreover, WBANs supports high quality services such as emergency messaging for some transactions which carry essential information [1].

On the other hand, Advanced Encryption Standard (AES) is a highly recommended security standard for the data encryption operations [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 operations such as encryption only (AES-CTR), authentication only (AES-CBC-MAC), and encrypted authentication (AES-CCM). In previous works, some optimized implementation methods for either AES encryption core or AES-CCM core have been presented [4]-[9]. However, more improvements are desired since emerging WBANs require low area, ultra-low power consumption encrypted authentication cores.

Therefore, this work focuses on the FPGA implementation of a low area AES-CCM IP core to provide both message encryption and authentication requirements. With the merit of low area impelementation, the proposed AES-CCM core can be further optimized and implemented in ASIC for WBAN and other emerging applications.

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

II. AES-CCM MODE OF OPERATION

AES-CCM is an authenticated encryption mode which was specified in NIST Special Publication 800-38C [2] in which AES block cipher core is used and the bit order of each input block is presented in [1]-[2]. The AES-CCM operation consists of two related processes which are generation/ encryption and decryption/verification. In the process of generation/encryption, an initial block B0, associated data blocks ($B_1 \div B_{k-1}$) and Pay-load blocks ($B_k \div B_n$) 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, the counter mode decryption is applied to cipher-text to recover the MAC and the corresponding payload; then, CBC mode is applied to the payload and the nonce to verify the correctness of the MAC. A successful verification means that the payload and its associated data are from the same source with access to the key so that a MAC provides a high level of authentication [2].

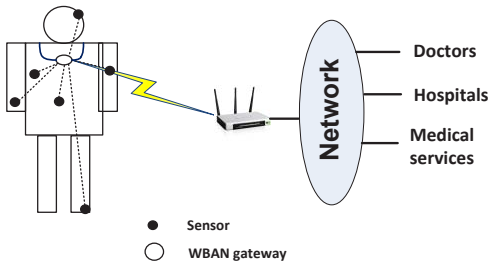

Fig. 1. An application of WBAN in tele-medicine systems.

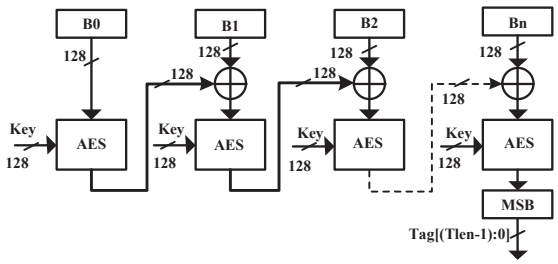

Fig. 2. Block diagram of the CBC mode.

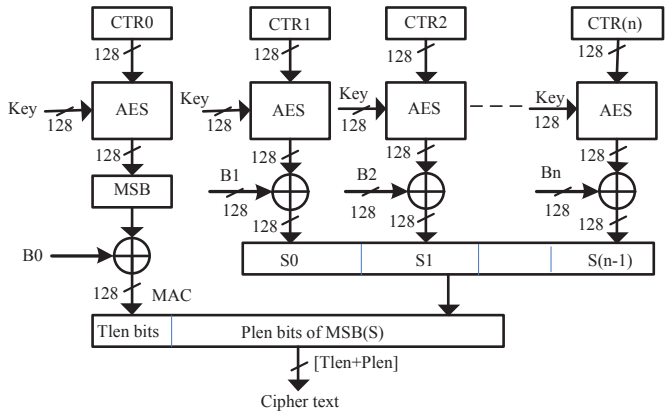

Fig. 3. Block diagram of the CTR mode.

III. AES-CCM CORE ARCHITECTURE

Since AES encryption is the essential part of the AES-CCM, the choice of its architecture is very important. Previous papers [4]-[5] implemented a low area AES encryption core by using 8-bit AES core architecture and optimizing S-box structure. Using Block RAM to implement 8-bit AES is also a solution to reduce AES core area, as shown in [6]. However, using 8-bit AES core architecture may lead to low throughput due to its iterative manner. Using an AES pipeline structure [7] is a promising solution to improve the throughput, such as an AES core in [7]. However, this core area is 3.6 times larger than the iterative looping structure. On the other hand, it is important to note that a typical data rate is up to 10Mbps in WBANs, which meet the requirements for most of entertainment and healthcare services [1]. In this paper, an iteration structure is used to optimize the hardware resource and also to meet the requirement of low power consumption [5] since throughput is not the most important issue in WBANs.

To process 128-bit AES encryption with the 8-bit architecture, we use several additional shift registers, as shown as Fig. 4. The compact S-box architecture is presented in Fig. 5 in which S-box is transformed from $GF(2^8)$ architecture to $GF(2^8)/GF(2^4)/GF(2^2)$ architecture [10]. The linear mapping block (*lin. map*) in Fig. 5 converts the basis from $GF(2^8)$ to $GF(2^8)/GF(2^4)/GF(2^2)$. After some processing steps [6], the result from $GF(2^8)/GF(2^4)/GF(2^2)$ is mapped to $GF(2^8)$.

As discussed previously, to reduce the area and power consumption of AES-CCM core, the iteration structure is employed with only one AES block to implement AES-CCM. The AES-CCM core architecture is shown as Fig. 6. In this figure, the AES core is used as presented in Fig. 4 in which 128-bit AES operation is processed in 8-bit data block in each clock cycle. As a result, it requires 160 clock cycles for each AES 128-bit data frame. Therefore, the framing format block, shift registers and multiplexers are used to implement 128-bit AES-CCM authenticated encryption. All operations in this core are controlled by a finite state machine (FSM). In Fig. 6, the counter is used to generate the loop index number for FSM to select the input data in each loop. Moreover, the CTR block provides CTRi frames for its counter mode.

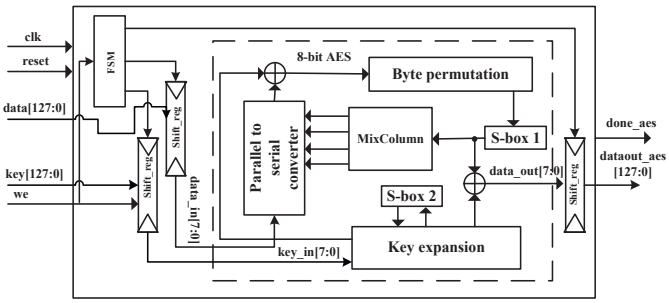

Fig. 4. The AES encryption core using 8-bit architecture.

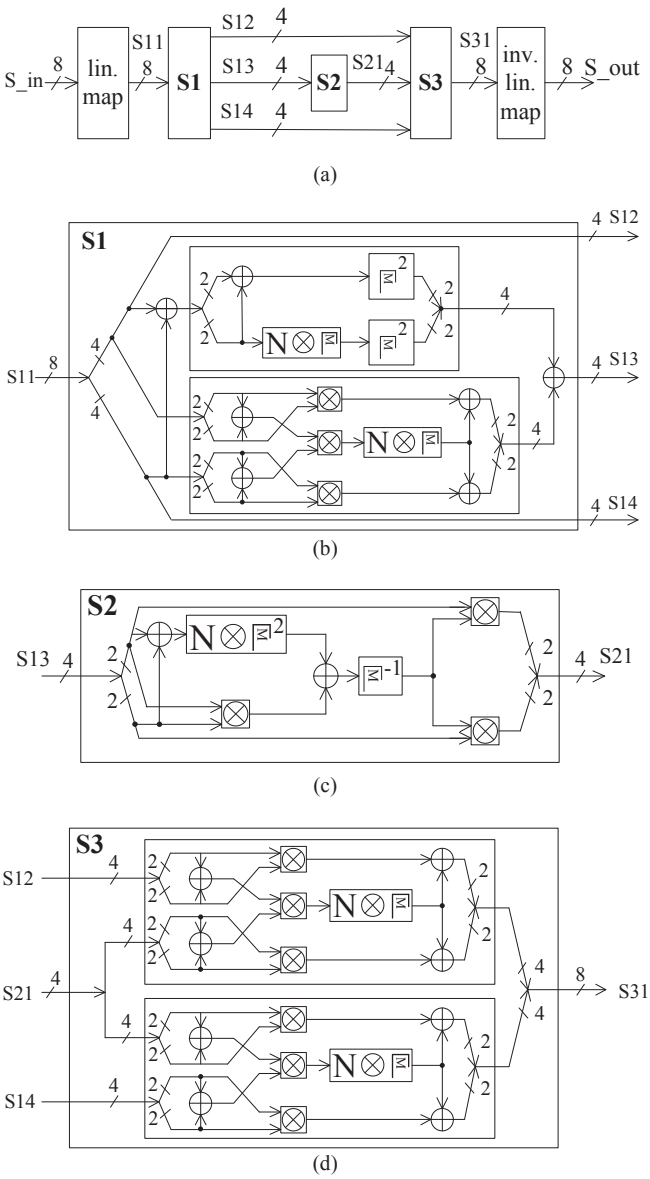

Fig. 5. Compact S-box architecture for AES encryption core.

IV. IMPLEMENTATION RESULTS

The AES-CCM encryption core was implemented with VHDL code, simulation on ModelSim-Altera 10.1d and then synthesized with different FPGA devices. The function of each signal in block diagram in Fig. 6 is described in Table I. Figure

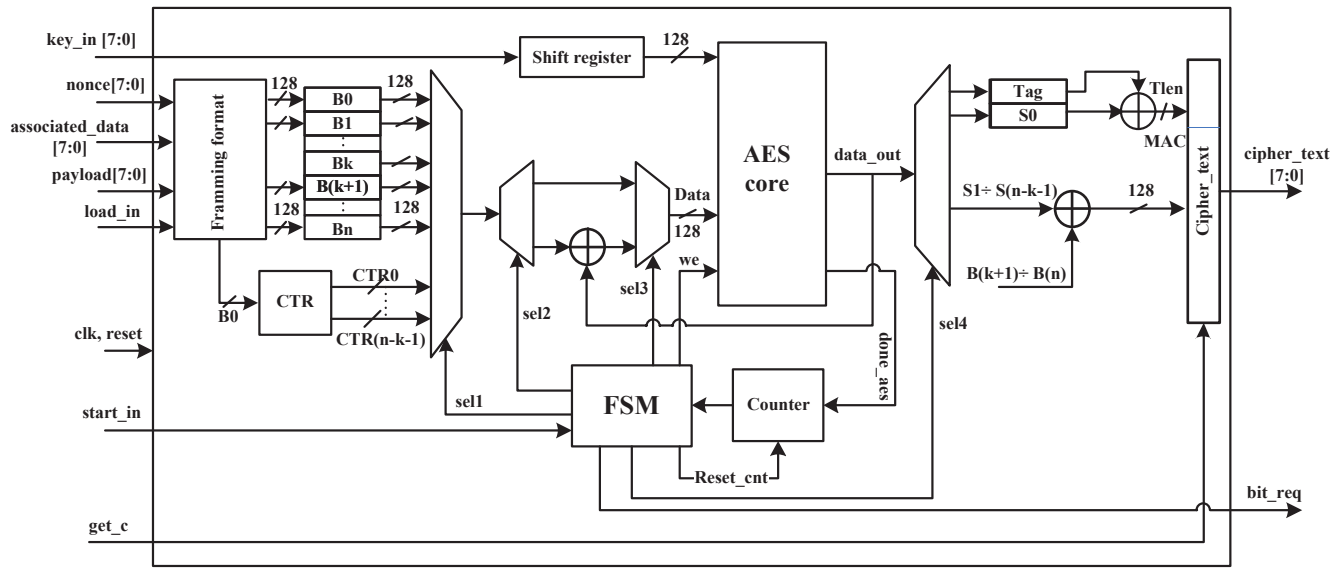

Fig. 6. The proposed AES-CCM IP core architecture.

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

Signal	Direction	Function
clk	Input	System clock
reset	Input	System reset
load_in	Input	Control signal to load payload, nonce, associated data and key
get_c	Input	To get data output
start_in	Input	Control signal to start the encryption
key_in	Input	Key input
nonce	Input	Nonce input
payload	Input	Payload input
associated_data	Input	Associated data input
cipher_text	Output	Data output
bit_req	Output	To indicate that the output is ready to read next data

7 presents the simulation results in Modelsim tool. In this example, the following parameters are chosen: Klen=128, Nlen=64, Tlen=48, Alen=128 and Plen=128. An example of the test vector for the proposed AES-CCM core is shown in Table II in which Klen is the length of key_in signal. With the input data as shown in this table, the proposed AES-CCM core requires 5 AES encryption loops (i.e. 800 clock cycles) to complete one authenticated encryption operation.

The FPGA-based implementation results of proposed AES-CCM core designs are shown as Table III. As pointed out in this table, due to the use of a compact 8-bit AES core and an optimized AES-CCM architecture, the proposed AES-CCM authenticated encryption core can reduce the FPGA hardware resource usage significantly. Although the maximum clock frequency of this core is a little lower as well, the proposed

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

key_in (128-bit)	0x40, 0x41, 0x42, 0x43, 0x44, 0x45, 0x46, 0x47, 0x48, 0x49, 0x4a, 0x4b, 0x4c, 0x4d, 0x4e, 0x4f
nonce (64-bit)	0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17
associated_data (128-bit)	0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f
payload (128-bit)	0x20, 0x21, 0x22, 0x23, 0x24, 0x25, 0x26, 0x27 0x28, 0x29, 0x2a, 0x2b, 0x2c, 0x2d, 0x2e, 0x2f
cipher_text (176-bit)	0xd2, 0xa1, 0xf0, 0xe0, 0x51, 0xae, 0x5f, 0x62, 0x08, 0x1a, 0x77, 0x92, 0x07, 0x3d, 0x59, 0x3d, 0x1f, 0xc6, 0x4f, 0xbf, 0xac, 0xcd

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

Design	FPGA Device	No. of Slices	BRAM/ ROM	Speed (MHz)
[7]	3S4000FG900	2154	2048 bit	-
Our	**3S4000FG900**	**1691**	**552 bit**	**44**
[8]	XC5VLX50F676	3942	10 blocks	114
Our	**XC5VLX50F676**	**979**	**552 bit**	**56.1**
[9]	XC3S700AFG484	1803	2048 bit	105
Our	**XC3S700AFG484**	**1686**	**552 bit**	**72.4**

AES-CCM core is suitable for WBAN applications where the data rate is not required to be high. Moreover, the proposed design uses less memory than others.

V. CONCLUSIONS

In this paper, we have presented an efficient iterative architecture of the AES-CCM IP core which requires only one AES encryption core targeted the FPGA hardware flatform. The low hardware complexity of the proposed AES-CCM IP core makes it suitable for IEEE 802.15.6 WBAN standard. In

the future, we will improve the proposed AES-CCM IP core and implement it in an ASIC hardware platform for resource and power constraint applications.

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] D. Canright and L. Batina, "A Very Compact "Perfectly Masked" S-Box for AES," *Proc. Applied Cryptography and Network Security (ACNS 2008)*, vol. 5037, LNCS, pp.446-459, Springer, 2008.

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

[8] 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.

[9] 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.

[10] Van-LanDao, Van-Phuc Hoang, Anh-Thai Nguyen, Quy-Minh Le, "A Compact, Low Power AES Core on 180nm CMOS Process," *Proc. IEEE International Conference on IC Design and Technology (ICICDT2016)*, pp.1-4, Jun. 2016.

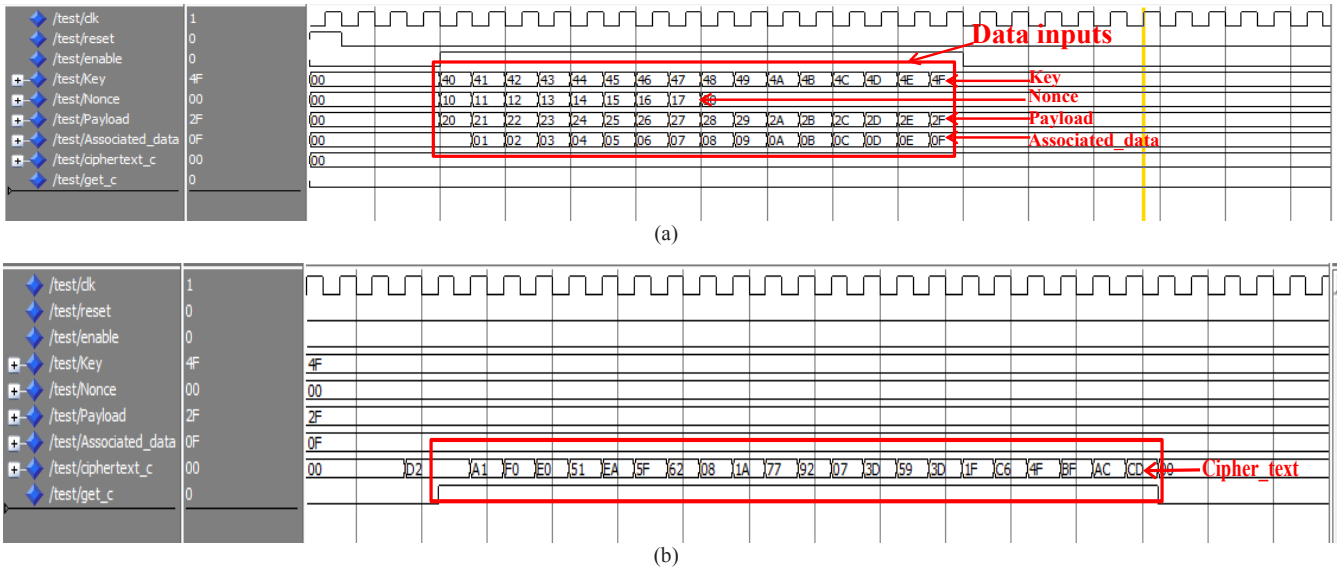

Fig. 7. Simulation results in Modelsim tool (a) Data and key input; (b) Data output.