An Ultra-Low Power AES Encryption Core in 65nm SOTB CMOS Process

Van-Phuc Hoang[1] 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
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 an efficient ASIC implementation of the low area and ultra-low power AES encryption core with an optimized S-box, Rcon and control blocks optimization, combined with a simple clock gating technique using an ultra-low power 65nm SOTB CMOS technology. The ASIC implementation results show that the proposed AES encryption core requires a small number of clock cycles with ultra-low power consumption and achieves higher resource usage efficiency compared with other designs.**

I. LOW-POWER, LOW-AREA AES CORE DESIGN

Advanced Encryption Standard (AES) is a well-known security standard for data encryption [1, 2] in many emerging wireless networks. Although the encryption is standardized, the efficient hardware architecture and implementation methods are the topics which many researchers are focusing on. Therefore, the objective of this paper is to design a low area and low power AES encryption core for emerging wireless networks.

In [2]-[5], authors have focused on optimizing AES encryption core for the low area implementation. However, they use an LUT-based (non-optimized) S-box that may result in a high area ASIC implementation. In some other papers [3]-[10], the authors focused on improving the S-box architecture, ultilizing FPGA embeded resources and some optimization techniques.

In this paper, AES encryption core processes data in 128-bit blocks with the key lengths of 128-bit. To reduce the AES encryption core area, we employ an 8-bit architecture with an optimized S-box so that the AES core encrypts an 8-bit data block in each clock cycle. The proposed AES encryption core architecture is shown in Fig. 1. This core includes a key expansion unit, a mixcolumn unit, a parallel to serial converter and a byte permutation unit. S-box 1 and S-box 2 blocks are the sub-blocks in the byte permutation unit and key expansion unit as described in [4].

For a low power consumption implementation, a simple clock gating technique is proposed by using *start_in* signal as shown in Fig. 1. The clock tree in the AES core is controlled by this signal. S-box is an important block in the AES core so that some papers on S-box optimization for the specific requirements have been published [2-5]. To reduce the complexity, we use the S-box architecture with the direct hardware implementation. In this paper, the S-box is transformed from GF(2^8) to GF(2^8)/GF(2^4)/GF(2^2) architecture [5].

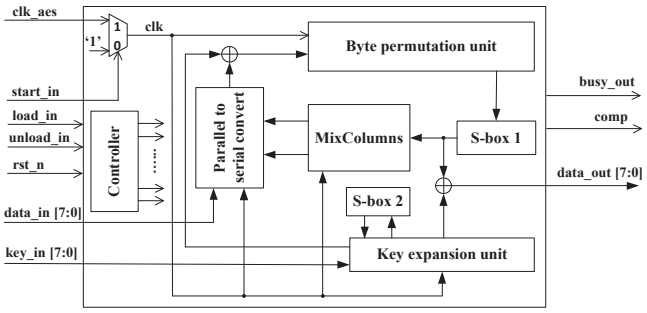

Fig. 1. The 8-bit AES encryption core architecture with iterative structure and simple clock gating technique

Moreover, according to [1], Rcon block takes the inputs from *r_in* signal which is the round index ranging from 0 to 9. Rcon also can be a multiplexer (MUX) circuit which uses *r_in* as the selection signal [4]. In our design, Rcon block is optimized by using the simple Karnaugh optimization.

For control part optimization, in the proposed AES encryption core, the control block in AES encryption core is a low power state machine. In this work, we propose a simple controller based on a counter as shown in Fig. 2. The control signal is generated from a simple 8-bit counter. The four maximal significant bits of counter output (counter[7:4]) are fed to key expansion block (*r_in* signal), and the 4-bit lower part (counter[3:0]) is used to select the operations in each AES encryption round. This simple control block is used to reduce the area and power consumption of the proposed AES encryption core.

Our main contribution in this paper is that an efficient AES encryption core for low area, ultra-low power systems is proposed based on the 8-bit iterative architecture with an optimized S-box, Rcon and control blocks optimization, combined with a simple clock gating technique.

II. IMPLEMENTATION RESULTS

The proposed 8-bit AES encryption core was modelled with VHDL, and then implemented with a 180 nm CMOS and 65nm SOTB CMOS [11] standard libraries by Synopsys Design Complier and Synopsys IC Complier tools. The ASIC implementation results of proposed and other AES encryption cores are shown in Table I in which the proposed AES encryption core area can be reduced to only 2.3kgates with 180nm CMOS library and requires the smallest number of cycles. Compared with other designs, the proposed AES

encryption core power consumption can also be reduced significantly to only 7.1µW/MHz with 180nm CMOS technology and especially to 0.38µW/MHz with 65nm SOTB CMOS technology. The proposed 8-bit AES encryption core is the lowest power consumption AES encryption core presented in literature. Figure 3 is the layout of proposed 8-bit AES encryption core with 65nm SOTB CMOS technology.

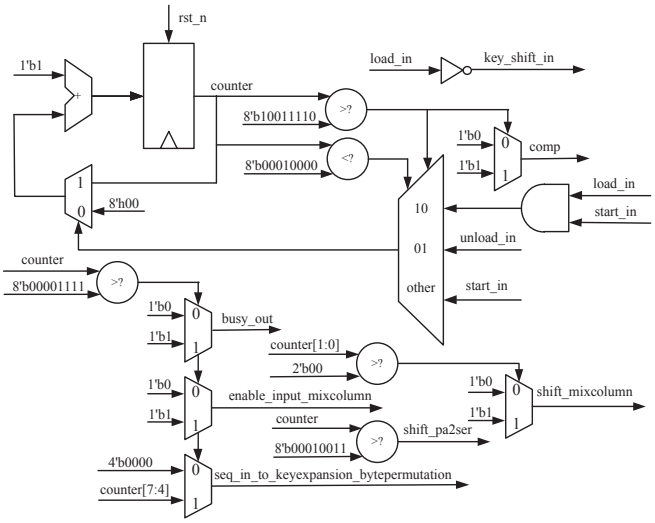

Fig. 2. The controller architecture for the 8-bit AES encryption core.

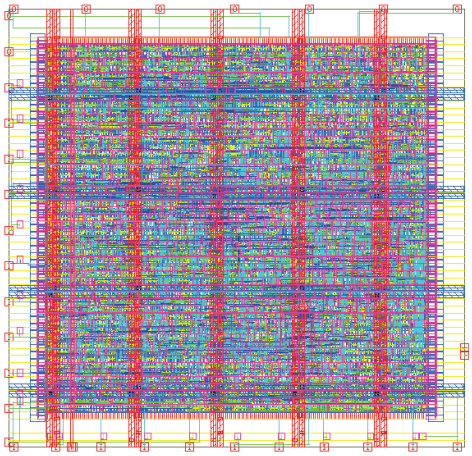

Fig. 3. Layout of the proposed 8-bit AES core using 65nm SOTB CMOS technology. The AES core layout dimension is 120µm×120µm.

TABLE I. IMPLEMENTATION RESULTS OF PROPOSED 8-BIT AES ENCRYPTION CORE COMPARED WITH OTHER PAPERS.

Design	Technology	No. of cycles	Area (kgates)	Power consumption
Our work	180nm	160	2.3	7.1 µW/MHz
Our work	65nm SOTB	160	2.6	0.38 µW/MHz
[4]	130nm	160	3.1	37 µW/MHz
[6]	22nm	336	2.0	13 mW (*)
[7]	-	226	2.4	3.7 µA @ 100KHz
[8]	130nm	356	5.5	99 µW/MHz
[9]	65nm	200	0.012 mm^2	4.6 µW @ 0.5V
[10] (**)	180nm	-	1.05×10^3 μm^2	39.1 µW/MHz

(*): @1.1GHz and 0.9V; (**): 8-bit architecture

III. CONCLUSIONS

This paper has presented a low area, ultra-low power AES encryption core which can be used for emerging wireless networks. The implementation results in ASIC show that by using an optimized S-box, Rcon block and control blocks optimization, combined with a simple clock gating technique, the AES core area and power consumption can be reduced significantly. The proposed AES encryption core requires the smallest number of cycles and achieves lowest power consumption as well. Therefore, this AES encryption core is highly potential to be used in wireless network nodes which require long battery duration. In the future, we will further improve the AES encryption core and apply it for a wireless network application.

ACKNOWLEDGMENT

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

This work is supported by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Synopsys, Inc. and Cadence Design Systems, Inc.

REFERENCES

[1] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," *FIPS Publication 197*, Nov. 2001.

[2] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-box optimization," *Proc. ASIACRYPT 2001*, pp.239-254, Dec. 2001.

[3] D. Canright. "A very compact S-box for AES," *Proc. 7th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES2005)*, pp.441-455, Sep. 2005.

[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 Conf. Digital System Design: Architectures, Methods and Tools (DSD2006)*, pp.577-583, 2006.

[5] T. Jarvinen, P. Salmela, P. Hamalainen, J. Takala, "Efficient byte permutation realizations for compact AES implementations," *Proc. 13th European on Signal Processing Conference*, pp.1-4, Sep. 2005.

[6] Sanu Mathew et al., "340mV-1.1V-289Gbps/W, 2090-gate NanoAES Hardware Accelerator with Area-optimized Encrypt/Decrypt GF$(2^4)^2$ Polynomials in 22nm tri-gate CMOS," *Proc. Symposium on VLSI Circuits Digest of Technical Papers*, 2014.

[7] Amir Moradi et al., "Pushing the limits: a very compact and a threshold implementation of AES," *Advances in Cryptology - EUROCRYPT 2011*, *Lecture Notes in Computer Science*, vol. 6632, pp.69-88, 2011.

[8] T. Good and M. Benaissa, "692-nW advanced encryption standard (AES) on a 0.13-µm CMOS," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol.18, no.12, pp.1753-1757, Dec. 2010.

[9] Wenfeng Zhao, Yajun Ha, Massimo Alioto, "AES Architectures for Minimum-Energy Operation and Silicon Demonstration in 65nm with Lowest Energy per Encryption," *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp.1-4, May 2015.

[10] Liling Dong et al., "Low Power State Machine Design for AES Encryption Coprocessor," *Lecture Notes in Engineering and Computer Science*, vol.2216, no.1, pp.714-717, Mar. 2015.

[11] Koichiro Ishibashi, Nobuyuki sugii, Shiro Kamohara, Kimiyoshi Usami, Hideharu Amano, Kazutoshi Kobayashi, Cong-Kha Pham, "A Perpetuum Mobile 32bit CPU on 65nm SOTB CMOS Technology with the Reverse-Body-Bias Assisted Sleep Mode," *IEICE Trans. Electron.*, vol.E98-C, no.7, pp.536-543, Jul. 2015.