# Design of ultra-low power AES encryption cores with silicon demonstration in SOTB CMOS process

V.-P. Hoang✉, V.-L. Dao and C.-K. Pham

The design of ultra-low power advanced encryption standard (AES) encryption cores for emerging wireless networks and Internet of things systems by combining optimised architectures, a simple clock gating technique and an advanced 65 nm silicon on thin buried oxide (SOTB) CMOS process is presented. The implementation results show that the proposed 2-Sbox AES encryption core requires the smallest number of clock cycles and achieves the lowest power consumption of 0.4 μW/MHz which is 3.3× lower than that of the best previous presented AES encryption core, with a very small area overhead. Moreover, the proposed 1-Sbox AES encryption core consumes very low hardware resources of 2.4 kgates gate equivalent.

*Introduction:* Advanced encryption standard (AES) is a highly recommended security standard of data encryption for emerging wireless networks and Internet of things (IoT) applications [1]. Therefore, many researchers have been focusing on AES efficient hardware architectures and implementation methods such as in [2–10].

Previous works such as in [2–5] have proposed some techniques to reduce the area of AES encryption cores with a non-optimised lookup table-based Sbox in application-specific integrated circuit (ASIC) platforms. Other papers [3–10] concerned the improvement of Sbox architecture, field programmable gate array-embedded resources utilisation and some optimisation techniques. Zhao *et al.* [9] presented an efficient, low-energy operation AES implementation in a standard 65 nm CMOS process. However, with the fast development of many portable, wearable applications and devices, especially in IoT systems, the low-area, ultra-low-power and secure hardware implementations with more improvements are highly required. In the IoT era, the low-power and high-security hardware implementation becomes an essential issue [11].

On the other hand, recently, silicon on thin buried oxide (SOTB) CMOS is an advanced technology for the ultra-low-power integrated circuit (IC) design and a good candidate for low-power electronics [12]. In [13], a compact design of 8 bit AES encryption core in 65 nm SOTB CMOS was presented with synthesis-based results. However, detail design tradeoffs and more improvements are expected, especially with silicon demonstration. In addition, there is no research presented in the literature about the ultra-low-power consumption AES core in this advanced technology with silicon demonstration. Therefore, to provide more efficient AES encryption cores, this Letter targets ultra-low-power AES encryption cores with silicon demonstration for emerging wireless networks and IoT systems by proposing optimised architectures and utilising a simple clock gating technique in an advanced 65 nm SOTB CMOS process.

*Ultra-low-power AES encryption core design:* In this work, for resource constraint applications such as IoT, the plaintext and key lengths are chosen as 128 bit. The proposed 2-Sbox architecture for the AES encryption core is shown in Fig. 1 with the parameters in Table 1. In this table, $w$ is the datapath width and $n$ is the bit-width of the mixcolumn block. The AES core encrypts a $w$-bit data block in each clock cycle. The AES encryption core includes a key expansion unit, a mixcolumn unit, a shift-row unit, a shift register and a byte permutation unit using Sbox. In the shift register as depicted in Fig. 2, the control signals (E1, E2) are generated from the controller. As shown in Fig. 3, the proposed AES core employs a simple counter-based controller. The control signal is generated from a counter, comparators and a simple logic circuit. The upper half (with higher significant bits) of the counter output (CNT) is fed to key expansion block and the lower half is used to select the operations in each AES encryption round. To provide more detail implementation results showing the area–speed–power tradeoffs, the proposed 2-Sbox AES encryption core was implemented with different datapath width values ranging from 8 to 64 bit. However, in the silicon demonstration, due to the limited chip area allocated for the core, an 8 bit architecture ($w = 8$) with the optimised Sbox is chosen to reduce the AES core area. Two Sbox blocks are used in byte permutation and key expansion units [4]. In this work, to reduce the hardware complexity, Sbox is transformed from Galois field (GF)($2^8$) to GF($2^8$)/GF($2^4$)/GF($2^2$). After some processing steps, the result is mapped back to GF($2^8$) [6].

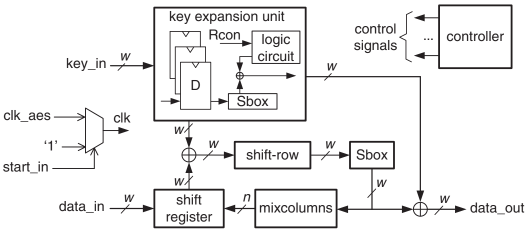

**Fig. 1** *Proposed 2-Sbox AES encryption core architecture*

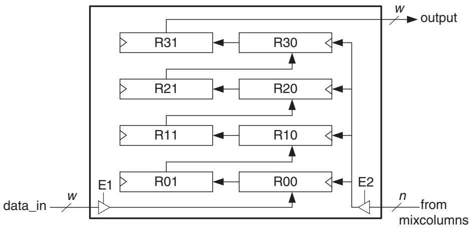

**Fig. 2** *Shift register block in proposed AES encryption cores*

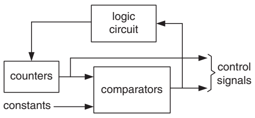

**Fig. 3** *Counter-based controller in proposed AES encryption cores*

**Table 1:** Datapath width and mixcolumn bit-width values

| $w$ | 8 | 16 | 32 | 64 |
|---|---|---|---|---|
| $n$ | 32 | 32 | 32 | 64 |

Moreover, to further improve the area efficiency of the core, in this Letter, 1-Sbox architecture is proposed as in Fig. 4 in which control signals are fed to multiplexer (MUX), demultiplexer (DEMUX) and some other simple circuits. Each round is performed in 20 cycles including 16 cycles for 16 data bytes and 4 cycles for key expansion with a shared Sbox using selection signal (Sel). A simple counter-based control method as shown in Fig. 3 is also applied for this architecture with a modified control method as presented in Table 2 in which CNT is the value of the cycle counter register in each round and *r_in* is the round index ranging from 0 to 9.

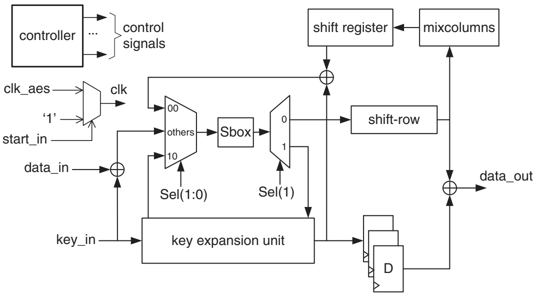

**Fig. 4** *Proposed architecture for 1-Sbox AES encryption core*

**Table 2:** Control method for proposed 1-Sbox AES encryption core

| *r_in* | >0 | >0 | 0 |
|---|---|---|---|
| CNT | 0 ÷ 15 | 16 ÷ 19 | — |
| Sel(1:0) | 00 | 10 | others |

For the key expansion unit, according to [1], Rcon block takes the inputs from *r_in* signal which is the round index. Rcon block can also be implemented by an MUX circuit using *r_in* as the selection signal [4]. For both architectures in this work, Rcon block is implemented by using a simple logic optimisation. Finally, for a low-power consumption implementation, a simple clock gating technique is proposed by using *start_in* signal to control the clock tree in the AES encryption cores as shown in Figs. 1 and 4.

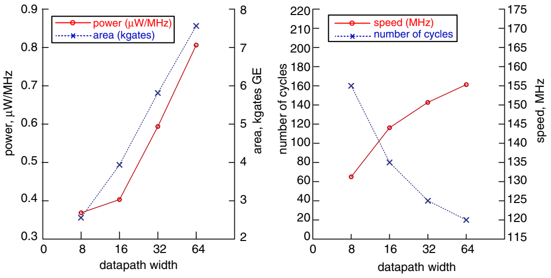

**Fig. 5** *ASIC implementation results of proposed 2-Sbox AES encryption core in 65 nm SOTB CMOS process with different values of datapath width (w)*

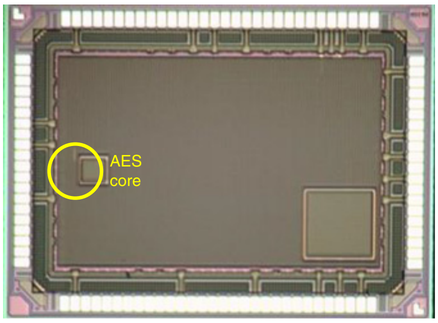

**Fig. 6** *Chip microphotograph of proposed 8-bit 2-Sbox AES encryption core in 65 nm SOTB CMOS process with core dimension of 120 μm × 120 μm*

**Table 3:** Implementation results of proposed 8 bit AES encryption cores compared with others

| Design | Technology (CMOS) | Number of cycles | Maximum Frequency (MHz) | Area (kgates GE) | Power (μW/ MHz) |
|---|---|---|---|---|---|
| our work (2-Sbox) | 65 nm SOTB | 160 | 130.9 | 2.6<br>(0.014 mm$^2$) | 0.40 |
| our work (1-Sbox) | 65 nm SOTB | 210 | 127.2 | 2.4<br>(0.013 mm$^2$) | 0.77 |
| [4] | 130 nm | 160 | 130.0 | 3.2 | 30 |
| [7] | 22 nm | 336 | 1133.0 | 2.0 | 11.82 |
| [8] | 130 nm | 356 | 13.2 | 5.5 | 99.0 |
| [9] | 65 nm | 200 | 11.0 | 0.012 mm$^2$ | 1.33 |
| [10] | 180 nm | — | 26.8 | 1.05 × 10$^3$ μm$^2$ | 39.1 |

*ASIC-based hardware implementation results:* The proposed AES encryption cores were modelled with very-high-speed integrated circuit hardware description language (VHDL), and then implemented with a 0.55 V, 65 nm SOTB CMOS standard library by Synopsys Design Compiler and IC Compiler tools. An AES reference model is used for verification with a multiple-level verification environment. Fig. 5 provides the area–speed–power tradeoffs of the post-layout ASIC implementation of the proposed 2-Sbox AES encryption core in 65 nm SOTB CMOS process with different values of datapath width. In practise, a suitable value of the datapath width can be chosen based on specific application requirements and constraints. Also, the detail implementation results of the proposed 8 bit and other AES encryption cores are shown in Table 3 in which the area of the proposed 8 bit 2-Sbox AES encryption core can be reduced to only 2.6 kgates [gate equivalents (GEs)] and requires the smallest number of cycles. It is noted that the AES encryption core in [10] is also based on an 8 bit architecture and the supply voltage of the design in [9] is 0.5 V which is similar to our designs. The power consumption of the proposed 8 bit 2-Sbox AES encryption core can also be reduced to 0.4 μW/MHz which is the lowest value compared with other AES encryption cores presented in the literature. For example, its power consumption is 3.3× lower than that in [9] with a very small area overhead (0.014 mm$^2$ against 0.012 mm$^2$). On the other hand, the maximum frequency of the proposed AES cores is much higher than that in [9]. Fig. 6 is the chip microphotograph of the proposed 8 bit AES encryption core using the 2-Sbox architecture in 65 nm SOTB CMOS process in which the top-level metal is hidden with the dummy. Compared to the 2-Sbox architecture, the area of 8 bit 1-Sbox AES encryption core can be reduced by 8%. However, its power consumption is 1.9× higher than the 2-Sbox counterpart.

*Conclusion:* Low-area, ultra-low-power AES encryption cores in the advanced 65 nm SOTB process with detail implementation tradeoffs were presented. The ASIC implementation results have clarified the improvements of the proposed AES cores. The proposed 2-Sbox AES encryption core requires the smallest number of cycles and achieves the lowest power consumption as well. Moreover, the proposed 1-Sbox AES encryption core consumes very low hardware resources of 2.4 kgates GE. Therefore, the proposed AES encryption cores are highly potential to be used for the hardware-based security solutions in emerging wireless networks and IoT systems.

*Acknowledgments:* This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.02-2015.20. This chip design was supported by VDEC, The University of Tokyo in collaboration with Synopsys, Inc. and Cadence Design Systems, Inc.

Submitted: *8 June 2017* E-first: *5 October 2017*
doi: 10.1049/el.2017.2151
One or more of the Figures in this Letter are available in colour online.

V.-P. Hoang and V.-L. Dao (*Faculty of Radio-Electronic Engineering, Le Quy Don Technical University, Hanoi, Vietnam*)

✉ E-mail: phuchv@mta.edu.vn

C.-K. Pham (*Graduate School of Informatics and Engineering, The University of Electro-Communications, Tokyo, Japan*)

## References

1 National Institute of Standards and Technology (NIST): 'Advanced encryption standard (AES)' (FIPS Publication 197, 2001)

2 Satoh, A., Morioka, S., Takano, K., *et al.*: 'A compact Rijndael hardware architecture with S-box optimization'. Int. Conf. Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 2001, pp. 239–254

3 Canright, D.: 'A very compact S-box for AES'. Int. Workshop on Cryptology Hardware and Embedded Systems, Edinburgh, UK, September 2005, pp. 441–455

4 Hamalainen, P., Alho, T., Hannikainen, M., *et al.*: 'Design and implementation of low-area and low-power AES encryption hardware core'. EUROMICRO Conf. Digital System Design (DSD), Dubrovnik, Croatia, August 2006, pp. 577–583

5 Jarvinen, T., Salmela, P., Hamalainen, P., *et al.*: 'Efficient byte permutation realizations for compact AES implementations'. 13th European Signal Processing Conf., Antalya, Turkey, September 2005, pp. 1–4

6 Canright, D., and Batina, L.: 'A very compact 'perfectly masked' S-Box for AES', *Springer Lect. Notes Comput. Sci.*, 2008, **5037**, pp. 446–459

7 Mathew, S., Satpathy, S., Suresh, V., *et al.*: '340 mV–1.1 V, 289 Gbps/W, 2090-gate nanoAES hardware accelerator with area-optimized encrypt/decrypt GF$(2^4)^2$ polynomials in 22 nm tri-gate CMOS', *J. Solid-State Circuits*, 2014, **50**, (4), pp. 1048–1058

8 Good, T., and Benaissa, M.: '692 nW advanced encryption standard (AES) on a 0.13 μm CMOS', *Trans. Very Large Scale Integr. Syst.*, 2010, **18**, (12), pp. 1753–1757

9 Zhao, W., Ha, Y., and Alioto, M.: 'AES architectures for minimum-energy operation and silicon demonstration in 65 nm with lowest energy per encryption'. IEEE Int. Symp. Circuits and Systems (ISCAS), Lisbon, Portugal, May 2015, pp. 1–4

10 Dong, L., Wu, N., and Zhang, X.: 'Low power state machine design for AES encryption coprocessor'. Int. Multi-Conf. Engineers and Computer Scientists, Hong Kong, March 2015, pp. 714–717

11 Dofe, J., Frey, J., and Yu, Q.: 'Hardware security assurance in emerging IoT applications'. IEEE Int. Symp. Circuits and Systems (ISCAS), Montreal, Canada, May 2016, pp. 2050–2053

12 Ishibashi, K., Sugii, N., Kamohara, S., *et al.*: 'A perpetuum mobile 32 bit CPU on 65 nm SOTB CMOS technology with the reverse-body-bias assisted sleep mode', *IEICE Trans. Electron.*, 2015, **E98-C**, (7), pp. 536–543

13 Hoang, V.-P, Dao, V.-L., and Pham, C.-K.: 'An ultra-low power AES encryption core in 65 nm SOTB CMOS process'. Int. SoC Design Conf. (ISOCC), Jeju, Japan, September 2016, pp. 89–90