An Energy Efficient AES Encryption Core for Hardware Security Implementation in IoT Systems

Manh-Hiep Dao[1,3], Van-Phuc Hoang[1*], Van-Lan Dao[1] and Xuan-Tu Tran[2]
[1]Le Quy Don Technical University, 236 Hoang Quoc Viet Str., Hanoi, Vietnam
[2]SISLAB, VNU University of Engineering and Technology, 144 Xuan Thuy road, Hanoi, Vietnam
[3]Viettel IC Design Center, Viettel Group, Hanoi, Vietnam
Email: *phuchv@lqdtu.edu.vn

Abstract— **This paper presents a low energy AES encryption core targeting for hardware security implementation in IoT systems. The proposed AES core architecture employs the improved shared S-box scheme with 32-bit datapath and low switching activity shift-row operation. Consequently, the proposed AES encryption core can provide good tradeoff with the area of 4.3 *kgates* and the energy consumption of 4 *pJ/bit* in 32 *nm* CMOS technology library.**

Keywords— AES; ASIC; low energy; Internet of Things

I. INTRODUCTION

Currently, emerging Internet of Things (IoT) applications highly require the hardware security assurance [1]. Hardware cryptography is one of popular solutions for these issues. Advanced Encryption Standard (AES) is a recommended security standard of data encryption [2]. Although AES encryption/decryption algorithms have been standardized, the efficient hardware architecture and implementation methods are the topics which many researchers are focusing on. However, with the fast development of many portable, wearable applications and devices, especially in IoT systems, the low area, low power and secure hardware implementations are highly required. Therefore, the higher energy efficiency VLSI implementations are highly expected. In the era of IoT, low power and high security requirements can be promisingly fulfilled by hardware cryptography implementation.

The objective of this paper is to design an energy efficient AES encryptiom for such area and power constrained IoT systems. Our main contribution is that a low area, low power AES encryption core implementation is proposed by combining several optimized components in the AES core and some modifications in the core architecture for the high hardware resource efficiency in the ASIC platform.

In recently published paper, the researchers proposed a wide range of optimization hardware architectures carrying out the AES algorithm [3]-[6]. With special purposes requiring high throughput, the architecture with 128-bit datapath could be used. The other methods are unrolled architecture or pipeline implementations. The disadvantages of these designs are the large area and high power consumption. For IoT applications, we need an encryption core with low area and low energy consumption. Therefore, some papers have presented the designs with AES algorithm implemented in the serial architecture using 8-bit datapath with one or two Substitution Boxes (S-boxes) although they reduce the AES encryption core throughput [6]. Meanwhile, some power optimization techniques such as back biasing and low supply voltage are used to reduce power consumption.

Therefore, in this paper, to provide good tradeoff between computation speed and energy efficiency of the AES encryption core, we propose an efficient AES implementation which is a balance between throughput, area and power consumption. Our architecture uses 32-bit datapath to achieve acceptable AES core throughput. Especially, it uses 4 S-boxes instead of 8 S-boxes to reduce the 2.3% total area and save 10% power consumption though the processing time rise by 10 clock cycles per 128-bit encryption compared to the previous 32-bit datapath designs. Furthermore, in order to save more area and power consumption, we implemented our proposed architecture in an advanced 32nm CMOS standard library.

The rest of this paper is organized as follows. Section II describes the proposed AES core architecture. Section III illustrates the synthesis, post synthesis results about area as well as power/energy consumption and compared them to the other researches. Then, section IV concludes the paper.

II. PROPOSED AES CORE ARCHITECTURE

AES is symmetric cipher model, which uses same key for both encryption and decryption process. This algorithm could process 128-bit blocks of input data with the key lengths of 128, 192 or 256 bits in 10, 12 or 14 encryption/decryption rounds, respectively [2]. This is standardized by National Institute of Standard and Technology (NIST) in 2001. In this paper, we focus on the encryption path with 128-bit key length. The decryption process and other encryption architectures with different key lengths can be implemented in the similar way.

The proposed architecture is different with others in that the shared S-box with the 32-bit datapath is used and the shift-row block with reduced switching activities. There are four principal operations: Subsitution Bytes, Shift Rows, Mix Columns and AddRoundKey. Meanwhile, Key expansion involves three operations: Rotate Words, Substitution Words, XORs of data and the key. Substitution Bytes and Substitution Words are similar processes. The next section will discuss in detail about our architecture.

A. Encryption Process

The AES algorithm involves two different principal subprocesses: Encryption and KeyExpansion. KeyExpansion

978-1-5386-6542-8/18/$31.00 ©2018 IEEE

process will be dicussed in the next section. We will describe the Encryption process in this part. The Encryption path of our proposed architecture have three sub-components of MixColumns, ShiftRows and 4 S-boxes which are also reused for KeyExpansion procedure. Because this design uses 32 bit datapath, the input data and cipher key will be separate into 32-bit packets. They are loaded simultaneously at 32-bit *data_in* and *key_in* ports.

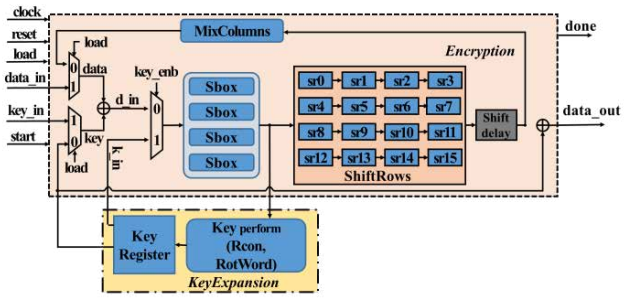

Figure 1. AES 32-bit datapath architecture using 4-Sbox for both Encryption and KeyExpansion procedure.

Firstly, after loading 32 bits of data and the corresponding cipher key, a XOR operation will be performed before a subsituting step occuring in 4 S-boxes. The temporary consequence of this step will be saved and processed in ShiftRows component. In this block, data will be sequentially processed that leads to an decrease of area and power consumption compared to [6]. Due to the use of 128-bit shift register, this step could be completed in four clock cycles. The output of ShiftRows block will be hold in one clock cycle in *Shift-delay* block before performing Mix-Columns. In this paper, we use a pure combinational MixColumns, followed by a XOR operation that will performs a computation between data and key.

In the AES standard for 128-bit cipher key, a completed encryption process will be performed in 10 round. In this paper, each round occurs in 5 clock cycles shown in Fig.2. Therefore, to encrypt 128 bits of data with 128 bits of cipher key, this process will complete fully in 54 clock cycles.

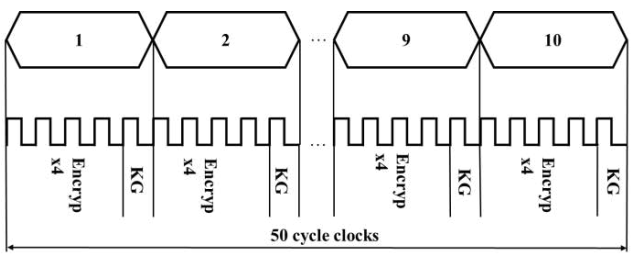

Figure 2. Time schedule.

B. KeyExpansion Process

Different from the other previous architectures, our proposed architecture shares 4 S-boxes with the encryption process. It means that we need create 16 bytes of new key in only one clock cycle, as Figure 2, the key expanded performs in the fifth clock cycle per round. In our design, we use four 32-bits of shift register to save all key, and a 32-bit XOR.

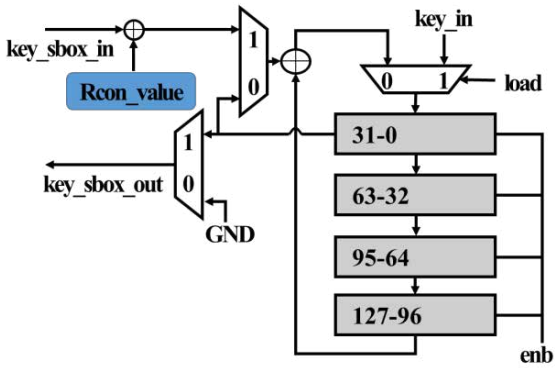

Figure 3. Key Expansion block.

C. ShiftRows

As we known about the switching activities, it is one of the major factors consuming the energy. With the targeting for IoT applications requiring low-power hardware, we minimized the activities in the datapath, especially ShiftRows block. By using 128-bit shift register, and reducing switching activities compared to the proposed ShiftRows block in [6], our proposed architecture saves up to 10% of the area and 50% of the power consumption.

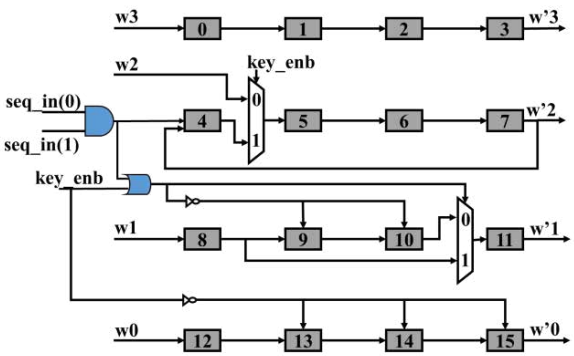

Figure 4. ShiftRows block.

The input data of the ShiftRows block is updated in particular flip-flops. The updating of all flip-flops is controlled by the '*enb*' signal. Thus, they only update the useful information that means flip-flops only switch their status in certain period with the effective data. This block needs 4 clock cycles to complete permuting 128 bits of data.

D. Substitution Box (S-box)

As mentioned in [4], S-box significantly affects area and power consumption parameters. In our architecture, we use only four S-boxes for both encryption and key expansion processes. The S-box blocks, therefore, occupy 34% of the total area.

There are various S-box optimization strategies with different aspects. While Canright's S-box [4] is the smallest S-

box until now, a Look-up-Table based S-box is more popular and easily understood. Canright's one uses 292 gates but consume more energy because of creating more activities in this architecture. Meanwhile, the most popular and straight-forward S-box implementation is the LUT-based S-box. The LUT-based S-box occupies 434 gates. In our architecture, as targeting to IoT applications, we reuse Canright's S-box. The most efficient S-box in terms of power consumption is Decode Switch-Encode (DSE) S-box [5]; however, it occupies a larger area (466 gates/S-box).

III. IMPLEMENTATION RESULTS

The 32-bit AES architecture was implemented with VHDL, simulated by Questar Sim, synthesized and estimated the area, power consumption by using Design Compiler and PrimeTime with 32nm CMOS technology library.

A. Area Estimation

Our proposed AES architecture has been implemented with 32nm CMOS standard library by using Design Compiler tool. The PVT condition applied in this estimation is 1.05V and 25ºC. Figure 5 shows that the Key Expansion is the largest block while Mix Columns is the smallest one. Due to a complex controlling process, the area of net and control unit makes up 18% of total area, which is equal to Shift Rows block. Meanwhile, four S-boxes occupy more than a quarter of total area. Compared to other encryption architectures using 32-bit datapath described in [6], our design saves 2.3% of total area as described in Fig.6. In this figure, the proposed AES core is compared with the conventional LUT based, Canright [4], LBS-CRS [6], DSE [6] and DSE-CRS [6] approaches.

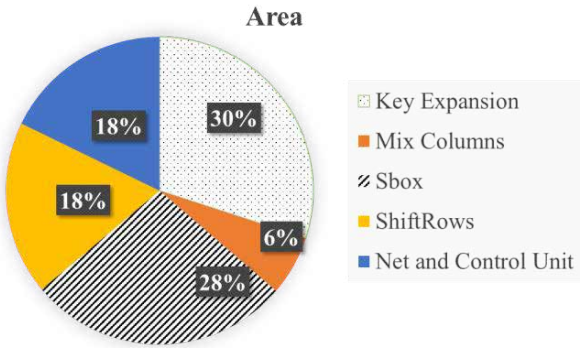

Figure 5. Area percentage of each block.

As shown in Fig.6, although a half of reduction in the number of S-boxes which impact significantly in both area and power consumption parameters, the trade-off is the complexity control processes. It means that the control unit of our proposed architecture uses more registers, combinational logic, and MUXs than that of the other designs. Consequently, the area of the proposed architecture slightly decreases when compared with the other architectures.

B. Energy Estimation

After being synthesized by Design Compiler, a net-list file which is the input for post-synthesis simulation was created. This simulation allows us to verify more exactly than behavioral simulation. The output of this simulation is a VCD (Value Change Dump) file. It contains the changes of all signals in the top module. It will be one of the input files for the energy estimation process using the PrimeTime tool. To ensure a fair comparison in a specific aspect such as energy per bit, we evaluate our power consumption parameter with other designs which use same datapath size, perform only encryption path, and use the same operation frequency.

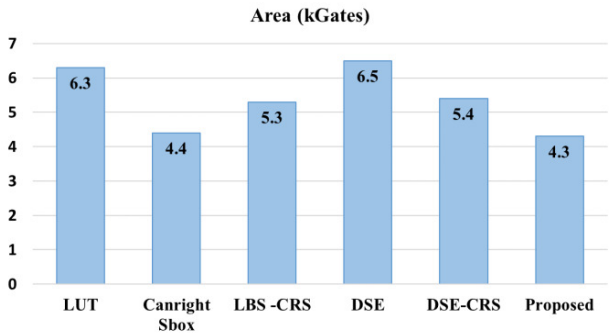

Figure 6. Area comparison with other existing designs.

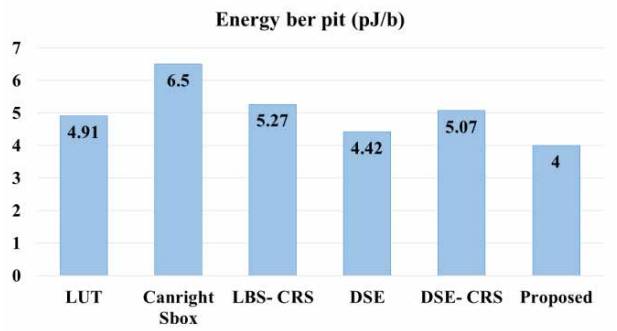

Figure 7. Energy comparison with other existing designs.

Due to estimating by PrimeTime, we got the result of power consumption (in µJ). We used the expression (1) to compute the energy per bit parameter before a comparison with other previous designs.

$$E = \frac{P \times N}{F \times 128} \quad (1)$$

where:

- P is the estimated power consumption by PrimeTime (µJ)
- N is the number clock cycles (here, N=54)
- F is the implemented frequency (F= 10MHz)
- E is energy per bit parameter (pJ)

The comparison results of AES core implementation are described in Fig.7. These results include area and energy comparison are compared to the designs presented in [6]. Compared to the Canright Sbox [4], it is obvious that our proposed architecture is significant smaller, about 38.46%. It also consumes less energy than the LBS-CRS (involving LBS encryption and CRS key expansion) and DSE-CRS (involving

DSE encryption and CRS key expansion), about 20-25%. As we can see in Fig.7, DSE approach, as presented in [6], consumes 13% energy higher than our proposed core.

IV. CONCLUSIONS

This paper has presented a low-area, low-power AES encryption core which uses 32-bit datapath and only four S-boxes for both encryption and key generation processes. The implementation results in 32nm CMOS technology library show that by reduction in the number of S-boxes in the hardware architecture, using an optimized S-box, the AES core area and power consumption can be reduced significantly. The proposed architecture requires less S-boxes and achieves lower power consumption as well. Thus, this AES encryption core is highly promising to be used for IoT systems.

ACKNOWLEDGMENT

This research is funded by the project of Fostering Innovation through Research, Science and Technology (FIRST) in "Hardware Cybersecurity: Methods, Technologies and Applications" under grant number 28/FIRST/1a/LQDTU.

The authors would like to thank Viettel IC Design Center with the partial support for this research.

REFERENCES

[1] J. Dofe, J. Frey and Q. Yu, "Hardware security assurance in emerging IoT applications," Proc. 2016 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 2050-2053, 2016.

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

[3] V. P. Hoang, V. L. Dao and C. K. Pham, "Design of ultra-low power AES encryption cores with silicon demonstration in SOTB CMOS process," in Electronics Letters, ISSN: 0013-5194, vol. 53, no. 23, pp. 1512-1514, Nov. 2017.

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

[5] G. Bertoni, M. Macchetti, L. Negri, and P. Fragneto, "Power-efficient ASIC synthesis of cryptographic S-boxes," Proc. 2004 ACM Great Lakes Symposium on VLSI (GLSVLSI'04), pp. 277-281, NY, USA, Apr. 2004.

[6] Duy-Hieu Bui, Diego Puschini, Simone Bacles-Min, Edith Beigné, "Ultra Low-Power and Low-Energy 32-bit Datapath AES Architecture for IoT Applications," Proc. 2016 International Conference on IC Design and Technology (ICICDT), pp.1-4, Jun. 2016.