Low Power State Machine Design for AES Encryption Coprocessor

Liling Dong, Ning Wu, and Xiaoqiang Zhang

Abstract—**As AES algorithm has been widely used in the field of routing, wireless sensor network and RFID, how to implement the low power optimization design for AES encryption becomes the research emphasis. In this paper, the low power state machine design is studied and implemented. Firstly, three data path structures of AES encryption circuits, which are 128, 32 and 8bit respectively, are implemented. Then for each structure, three state machines are designed and implemented with Finite State Machine (FSM), Look-Up Table (LUT), and Decoder-Switch-Encoder (DSE) method respectively, as well as analyzed on the performance of area, frequency, power consumption, throughout and energy. Based on SMIC 0.18μm 1.62V CMOS standard library, the experimental results indicate that the AES encryption circuit with 8bit data path structure achieves the smallest area, whereas the one with 128bit data path structure performs the highest throughput and the lowest average power consumption. For three different data path structures, LUT state machine achieves superior low power consumption performance. However state machine with DSE method always used to implement low power consumption optimization of S-box, cannot meet low power requirement, in that the low power performance of DSE method should be combined with the nonlinearity of original combinational logic circuits.**

Index Terms—**Finite State Machine (FSM), low power, Look-Up Table (LUT), Decoder-Switch-Encoder (DSE), Advanced Encryption Standard (AES)**

I. Introduction

ADVANCED Encryption Standard (AES) is a kind of symmetric block cipher standard, which was issued by the National Institute of Standards and Technology (NIST) in November 2001 [1]. Due to its small area cost and low power consumption, AES algorithm has been widely used in the field of routing, wireless sensor network and radio-frequency identification (RFID). However, for those AES encryption with ultra high speed or small area, the low power consumption requirement cannot be met. Thus how to implement the low power optimization design for AES encryption has became the research emphasis. As the only nonlinear operation, S-box has been studied for low power consumption optimization by plenty of works, always with composite field arithmetic [2] or Decoder-Switch-Encoder (DSE) method [3], [4]. However there are few works on low power state machine.

Several works have paid attention to the low power optimization for Finite State Machine (FSM). To obtain low power consumption implementation of Elliptic Curve Cryptography (ECC) processor, the strategy of optimizing the state coding, which is operated by merging two-way branch states to compound states, is adopted in [5] for FSM optimization. Besides, a methodology for the decomposition of FSMs targeted towards low power dissipation is proposed in [6], which performs effectively on the network of interacting FSMs. Both of the above methods aim at the interacting FSM with significant branches, which is not suitable for the one of AES encryption coprocessor with few branches. In [7], an approach, which combines the use of distributed hardware tasks and power gating techniques to obtain ultra low-power FSM implementations, is proposed, controlling part of the design switched on/off according to their activity. To shut down the controller while no data or command is transferring for a long time, a SD card controller with low power structure composed of two asynchronous units (BIU and CIU) is presented in [8]. Whereas the controller of AES encryption coprocessor runs until the encryption process has finished, the method of [7] or [8] cannot be adopted

Motivated by this fact, this paper designs three different state machines, implemented with FSM, Look-Up Table (LUT) and DSE method respectively. Meanwhile all are applied to the design and implementation of AES encryption.

II. AES Algorithm

A. Basic Algorithm

AES encryption algorithm is a block cipher algorithm. The input 128bit plain test data block is divided into a 4×4 matrix which is called state matrix. The element of the state matrix is an 8bit data, namely a 1-byte data. According to the different key sizes: 128, 192 and 256bit, the state matrix is operated by Nr=10, 12 or 14 rounds transformation respectively. Each round is composed of four transformations: SubBytes (SB), ShiftRows (SR), MixColumns (MC) and AddRoundKey (AK), and the process of each round is shown in Fig. 1. For the last round, only three transformations of SB, SR and AK are used and the MC is eliminated, which is implemented by a MUX unit.

The SB operation is the only nonlinear operation in AES algorithm, and each byte in the state matrix is replaced by the substitution function S-box. The S-box is an inverse function in the finite field $GF(2^8)$ followed by an affine transformation. SR is a cyclic shift operation in each row by 0-3 byte offsets

Manuscript received December 29, 2014. This work was supported by the National Natural Science Foundation of China (61376025), Industry-academic Joint Technological Innovations Fund Project of Jiangsu (BY2013003-11).

Liling Dong is with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing 210016, China (e-mail: 820365078@qq.com).

Ning Wu is with the College of Electronic and Information Engineering, NUAA, Nanjing 210016, China (e-mail: wunee@nuaa.edu.cn).

Xiaoqiang Zhang is with the College of Electronic and Information Engineering, NUAA, Nanjing 210016, China (e-mail: zxq198111@qq.com).

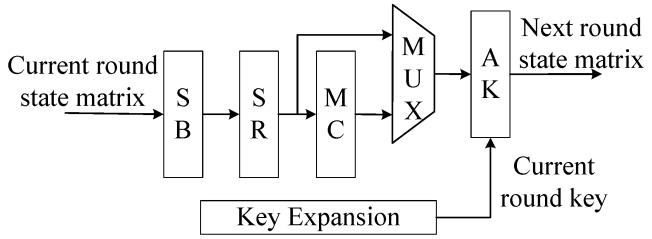

Fig. 1 The process of round transformation.

from row 0 to row 3 respectively. The MC operation takes the 4 bytes in each column as the polynomial coefficients on $GF(2^4)$, multiplied with a Constant polynomial $c(x)$ on the irreducible polynomial x^4+1. The $c(x)$ is given by

$$c(x) = '03'x^3 \oplus '01'x^2 \oplus '01'x \oplus '02'. \quad (1)$$

The multiplication in MC is operated as the bit multiplication in $GF(2^8)$, on the irreducible polynomial $x^8+x^4+x^3+x+1$. AK is a simple bitwise XOR operation on 128bit round data and round key.

The cipher key adopted in this paper is 128bit, treated into a state matrix as the plain test similar to the round data. Based on the cipher key, the Key Expansion module is to generate each round key, and is composed of three transformations: the cyclic shift permutation of the column, the column SB operation and the bitwise addition with the round constant array Rcon, which records the round count and eliminates the symmetry.

B. AES encryption architecture design

According to the basis flow of AES algorithm, AES encryption structure is shown in Fig. 2, in which the core parts are Round transformation module and Key Expansion module, while the auxiliary parts are AddRoundKey module and Rcon module. All these modules are controlled by Controller module, which is the research emphasis of this paper. For each round, Round transformation operation is implemented with sequential structure, and Key Expansion module generates round key. Besides, in the auxiliary section, round transformation data and key data are operated on modulo 2 addition by AddRoundKey, while round transformation is recorded by Rcon feeding back the count record to Controller.

As the input data of AES round transformation is 128bit, three different data path structures for AES encryption are designed and implemented, which are 128bit, 32bit and 8bit respectively [10]. Fig. 2 shows the structure of AES encryption with d-bit (d=128, 32, 8) data path. For detailed operation of MixColumns and Key Expansion in three structures, [3], [9] and [11] are referred to, respectively. For 128bit structure, ten rounds can be implemented with sequential structure. Yet, to get the 128bit data for next round transformation, 32bit structure requires a register to store the 32bit output data. So does 8bit structure.

III. Implementation of Low Power State Machine

A. State Transition Diagram

128bit AES encryption round transformation circuit is implemented with pure combinational logic, in which each round transformation operation just requires one clock. As

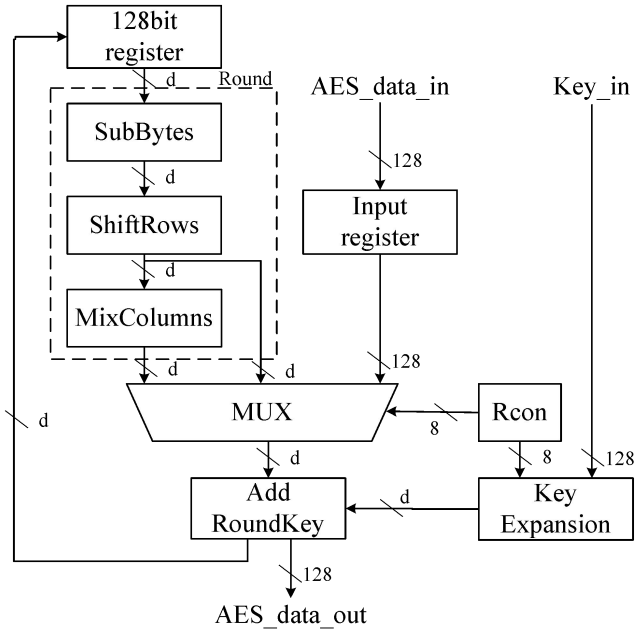

Fig. 2 AES encryption structure with d-bit data path (d=128, 32, 8).

shown in Fig. 3, the Mealy state transition diagram contains two input control vectors {AES_en, C_Rcon_end}, i.e. AES enable signal and count end signal, and five output vectors control_reg={C_r_en, C_lr_en, C_k_en, C_Rcon_en, C_x_en}, which represent original round enable, last round enable, key expension enable, count enable and add round key enable respectively. Besides the Idle state (which represents the initial state), only two states are required. State S1 represents the round transformation state which starts with the signal AES_en="1", and the next state is still S1 until ten rounds have been completed, i.e. the count end signal C_Rcon_end="1". Then State S2 starts with Idle followed, which represents the AES process finished.

In the 32bit AES encryption round transformation circuit, SubBytes and MixColumns modules are implemented with serial structure, and each round transformation operation requires four clocks. The state transition diagram is shown in Fig. 4. Compared with the 128bit structure, one input control signal named C_m_end, which marks the store module finished, is additive. Besides the Idle state, three states are required. State S1 marks each round active, with State S2 followed, which represents the middle two 32bit operations in each round controlled by C_m_end=0. If C_m_end=1, State S3 starts, i.e. the count module is active. Then for the original rounds (i.e. the first nine rounds or C_Rcon_end=0),

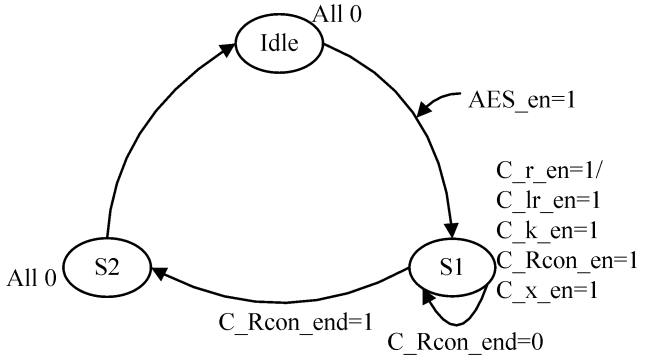

Fig. 3 The state transition diagram for 128bit AES encryption state machine.

ISBN: 978-988-19253-9-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

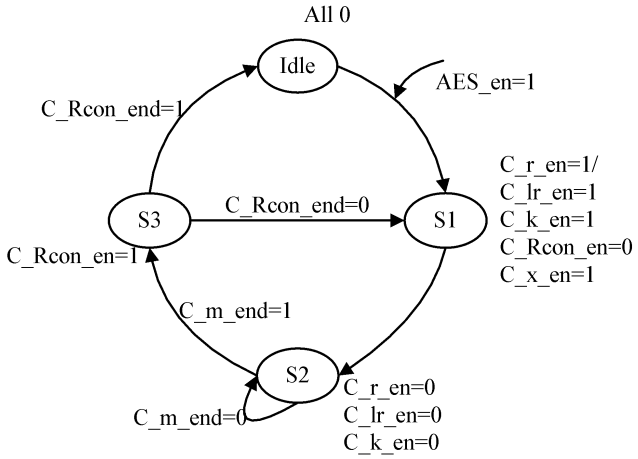

Fig. 4 The state transition diagram for 32bit AES encryption state machine.

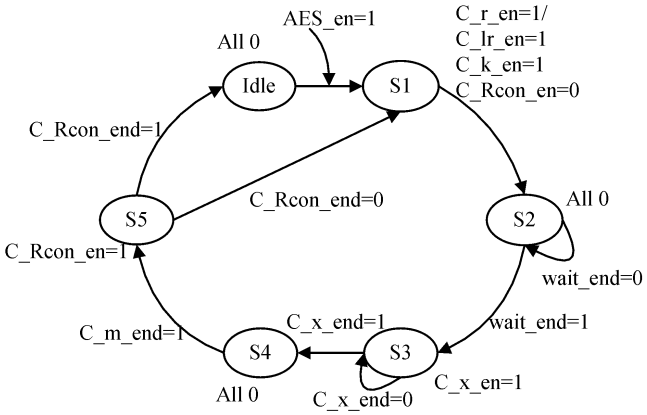

Fig. 5 The state transition diagram for 8bit AES encryption state machine.

the next state is transited to S1 to start next round transformation. And for the last round (i.e. C_Rcon_end=1), the next state is transited to Idle, which represents the AES process finished.

In the 8bit AES encryption round transformation circuit, 2 S-boxes are required, one for SubBytes modules, the other one for key expression. Each round transformation operation requires 21 clocks, due to the additional 4 clocks for MixCilumns module 32bit operations and 1 clock for storing 128bit data. The state transition diagram is shown Fig. 5. Compared with the 32bit structure, two input control signals are additive, which are C_wait_end for masking the MixColumns module prepared and C_x_end for marking the AddRoundKey module end. Besides the Idle state, five states are required. State S1 marks each round active, with State S2 followed to wait MixColumns module data preparation. If 32bit data has been prepared, the next state is transited to S3 to operate round key addition, which is controlled to finish by C_x_end=1. Thus the next state is S4. If C_m_end=1, State S5 starts to enable the count module. Then for the original rounds, the next state is transited to S1 to start next round transformation. And for the last round, the next state is transited to Idle, which represents the AES process finished.

B. The Implementation of State Machines

State machine, short for FSM, represents the mathematical model for finite states as well as the transition and operation among those. In this paper, FSMs are implemented with Mealy method according to each state transition diagram. And output control_reg is both based on input signal and current state.

LUT state machine is designed to implement FSM with look-up table, which in detail describes the state of circuits in each clock. In this paper, the input registers of AES round transformation state machines with three different data path structures, i.e. 128, 32 and 8bit, are control_in = {AES_en, C_Rcon_end} , control_in = {AES_en, C_m_end, C_Rcon_end}, control_in = {AES_en, wait_end, C_x_end, C_m_end, C_Rcon_end}, respectively. Combined with control_in, a new register control_cnt is required to transit among states. Hence, the input state LUT_in is represented as LUT_in={control_in, control_cnt}.

DSE state machine is implemented with decoder-switch-encoder method, which is always called DSE for short, from LUT state machine. For N×N nonlinear mapping circuits, decoder transforms Nbit input signals to 2^Nbit one-hot codes, i.e., decoder transforms the mapping table of N×N to the one of $2^N \times 2^N$, on the basis of which switch unit is directly wired performing one bit mapping, without resource cost and power consumption. Encoder transforms the 2^Nbit one-hot codes to Nbit output signals. It has been shown that the zero power consumption performance of switch unit, and one-hot codes used in decoder and encoder unit, play a significant role in reducing the power consumption of the circuits. In this paper, the input registers of DSE method are the same as these of LUT method, for the three different data path structures.

TABLE I
DIFFERENT AES STATE MACHINES IMPLEMENTATION (@20MHz)

Data Path (bit)	Implement-ation	Area (μm^2)	f_{max} (MHz)	Power (μW)
128	FSM	309.36	38.68	3.88
	LUT	262.79	38.45	3.72
	DSE	572.14	38.3	5.07
32	FSM	435.76	38.51	5.35
	LUT	482.33	38.2	3.91
	DSE	1520.16	36.7	5.48
8	FSM	798.34	37.74	10.26
	LUT	908.11	37.48	7.42
	DSE	4217.88	35.97	10.34

f_{max}: the maximum frequency of circuit

IV. PERFORMANCE ANALYSIS

This paper implements FSM, LUT and DSE state machine for the AES round transformation of 128, 32 and 8bit data

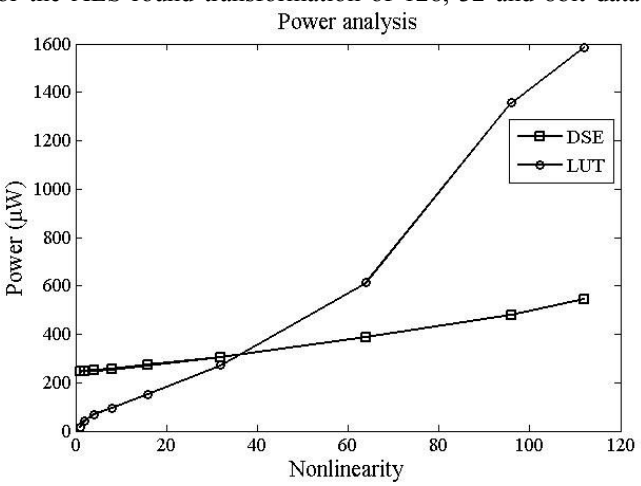

Fig. 6 The relationship between power consumption and nonlinearity.

ISBN: 978-988-19253-9-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE II
DIFFERENT DATA PATH STRUCTURES AES IMPLEMENTED WITH LUT STATE MACHINE (@20MHZ)

Data Path (bit)	Area (μm^2)	f_{max} (MHz)	T_{max} (Mbps)	T_{work} (Mbps)	Power (μW)	P_{ever} (μW/MHz)	E_{ever} (μJ/Mb)	Energy (μJ)
128	248957.76	25.24	3230.69	2560	1477	73.85	0.58	73.85
32	147898.40	26.75	856	640	1035	51.75	1.62	207
8	104838.15	26.82	171.65	128	782	39.1	6.11	782

T_{max}: the maximum throughout that circuit receives; T_{work}: the throughout on the work frequency; P_{ever}: the average power on the work frequency; E_{ever}: the average energy on the work frequency

path structures, respectively. Synthesized with Synopsys DC Tools and SMIC 0.18μm 1.62V CMOS standard library, the experimental results are listed in TABLE I. For three different data path structures, LUT state machine performs optimal power consumption, with an operating frequency of 20 MHz. TABLE II shows the synthesis results of different data path AES structures implemented with LUT state machine. The results indicate that AES round transformation circuit with 8bit data path structure achieves the smallest area which is 104838.15μm^2, whereas the one with 128bit data path structure performs the highest throughput and the lowest average power consumption, which are 3230.69 Mbps and 0.58 μJ/Mb respectively.

It can be known from TABLE II that, the AES state machine implemented with DSE method cannot meet low power requirement. Motivated by this fact, the relationship between the power consumption of combinational logic circuit and nonlinearity is studied, and 8×8 pure combinational logic circuits is researched as a typical example. The synthesis result is shown in Fig. 6. And the result shows that the higher nonlinearity pure combinational logic circuit performs, the better low power consumption performance DSE method achieves.

V. CONCLUSION

This paper implements FSM, LUT and DSE state machines for AES round transformation of 128, 32 and 8bit data path structures, respectively. Synthesized with Synopsys DC Tools and SMIC 0.18μm 1.62V CMOS standard library, the analysis results indicate that AES round transformation circuit with 8bit data path structure achieves the smallest area, whereas the one with 128bit data path structure performs the highest throughput and the lowest average power consumption. For three different data path structures, LUT state machine achieves superior low power consumption performance. However DSE state machine cannot meet low power consumption requirement, in that the low power performance of DSE method should be combined with the nonlinearity of original circuits.

REFERENCES

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

[2] Kumar Munusamy, C.Senthilpari, Daniel C.K. Kho. "A Low Power Hardware Implementation of S-Box for Advanced Encryption Standard," *2014 11th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON 2014), IEEE Press*, 2014, pp. 1-6.

[3] XING J., ZOU X., GUO X., "Ultra-low power S-Boxes architecture for AES," *the Journal of China Universities of Posts and Telecommunications*, vol. 15, no. 1, March 2008.

[4] Chen Y., Zou X., Liu Z., Han Y., Zheng Z, "Energy-efficient and security-optimized AES hardware design for ubiquitous computing," *Journal of Systems Engineering and Electronics*, vol. 19, no. 4, pp. 652–658, 2008.

[5] Peng Luo, Xinan Wang, Jun Feng, and Ying Xu. "Low-Power Hardware Implementation of ECC Processor suitable for Low-Cost RFID Tags," *Proc. 9th International Conference on Solid-State and Integrated-Circuit Technology, 2008. ICSICT 2008, IEEE Press*, 2008, pp. 1681-1684.

[6] Himani Mittal, Dinesh Chandra, and Arvind Tiwari. "Design of Low Power FSM Using Verilog in VLSI", *Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2013, QSHINE 2013*, LNICST 115, pp. 377–386, 2013.

[7] Muhammad Adeel Pasha, Steven Derrien, and Olivier Sentieys. "Ultra low-power FSM for control oriented applications," *IEEE International Symposium on Circuits and Systems, ISCAS 2009*, pp. 1577-1580.

[8] Pan Zhou, Teng Wang, Xin'an Wang, and Yinhui Wang. "Hardware Implementation of a Low Power SD Card Controller," *2014 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), IEEE Press,* 2014, pp. 158-161.

[9] LI Z., ZHUANG Y., ZHANG C., JIN G., "Low-power and area-optimized VLSI implementation of AES coprocessor for Zigbee system," *the Journal of China Universities of Posts and Telecommunications*, vol. 16 no. pp. 89–94, June 2009.

[10] L. Huai, X. Zou, Z. Liu, Y. Han, "An Energy-Efficient AES-CCM Implementation for IEEE802.15.4 Wireless Sensor Networks," *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC.2009)*, pp. 394-397, 2009.

[11] P. Hämäläinen, T. Alho, Marko Hännikäinen, and T. D. Hämäläinen, "Design and Implementation of Low-area and Low-power AES Encryption Hardware Core," *Proc. 9th Euromicro Conference Digital System Design (DSD2006),* Cavtat, Croatia: IEEE Press, 2006, pp. 577-583.

ISBN: 978-988-19253-9-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)