World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:1, No:8, 2007

Low Power Circuit Architecture of AES Crypto Module for Wireless Sensor Network

MooSeop Kim, Juhan Kim, and Yongje Choi

***Abstract*—**Recently, much research has been conducted for security for wireless sensor networks and ubiquitous computing. Security issues such as authentication and data integrity are major requirements to construct sensor network systems. Advanced Encryption Standard (AES) is considered as one of candidate algorithms for data encryption in wireless sensor networks. In this paper, we will present the hardware architecture to implement low power AES crypto module. Our low power AES crypto module has optimized architecture of data encryption unit and key schedule unit which could be applicable to wireless sensor networks. We also details low power design methods used to design our low power AES crypto module.

***Keywords*—**Algorithm, Low Power Crypto Circuit, AES, Security.

I. Introduction

THE concern with wireless sensor networks has been growing for the last several years. Sensor networks mean the networks of large numbers of sensor nodes which have computation and communication abilities. These sensor networks can be used such applications as smart home, logistics, military and so on.

Generally, sensor nodes have limited computing power and very small chip size. Despite their strict constraints, sensor network systems constructed with many components such as operating system, at least one or two sensors, microcontroller, communication modules, and other peripheral systems. Considering security issues, sensor network systems are forced to include security systems which prevent such threats as eavesdropping, message modification, impersonation and even side channel analysis.

So, the major challenges to implement efficient sensor network systems are narrowed into two issues: how to design sensor network system to consume low power and how to implement security system in effective.

There have been many studies for security of sensor network systems. Perrig et al suggested Sensor Network Encryption Protocol (SNEP) in [1] to provide sensor network security feature such as confidentiality, two-party authentication and integrity. Advanced Encryption Standard (AES)[2], [3] is one of candidate algorithms for SNEP.

In this paper, we will present the hardware architecture to implement low power AES crypto module. We focused to optimize the architecture of data encryption unit and key schedule unit. In addition, we describe the low power design methods used in our low power AES crypto module.

Section 2 describes characteristics of AES algorithm and consideration of architecture for low power AES module. Section 3 details the building blocks of our low power AES crypto module such as data encryption unit, key schedule unit and so on. We also represent implementing results of each unit. Section 4 reviews our implementation and states our plans for future work.

II. Low Power AES Architecture

Wireless sensor network systems have limited circuit area and computing power by its nature. A special architectural consideration is needed to design AES algorithm.

In this chapter we review the characteristics of AES algorithm and analyze its structure for hardware implementation at first. And then, we describe the architectural features of our low power AES crypto module.

A. Characteristics of AES Algorithm

The AES is a symmetric encryption algorithm which was selected FIPS standard in 2001. AES can support 3 types of key length of 128, 192, and 256 bits and operate on fixed 128-bit data blocks.

The operations of AES are conducted by two dimensional arrays of bytes which is called the state. The state consists of four columns and four rows of bytes. AES algorithm uses a round function which performs internally 4 different data transformation except the final round to modify the state for both encryption and decryption. As shown in figure 1, the transformation functions conducted in the round function are SubByte, ShiftRow, MixColumn, and AddRoundKey [2].

Because the state of AES algorithm consist byte of arrays, most operations of round function could be processed by unit of byte. Therefore, we could expect to find a clue to implement low power AES circuit from these structural characters. Before describing architectures of our low power AES circuit, we examine structural features of each transformation function performed in round function in detail.

SubByte transformation function is non-linear permutation consisting of S-box applied to the each byte of the state. Byte-based operation enables us to implement using just one S-box. Reducing the number of S-box means the reduction of circuit area and power consumption at the same time.

Mooseop Kim, Juhan Kim and Yongje Choi are with the Electronics and Telecommunications Research Institute (ETRI), 161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea (e-mail: gomskim, juhankim, choiyj@ etri.re.kr).

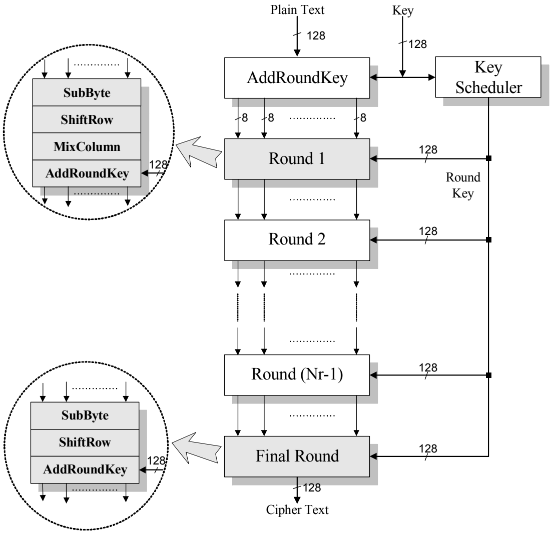

Fig. 1 AES operation and transformations of round function

ShiftRow transformation function performs a byte transposition using cyclic shifts the row of state according to predefined offsets. Knowing offset value enables us to make simple data path. So, it reduces the effort to make logical data paths.

MixColumn transformation substitutes the columns of the state. It uses modulo $x^4 + 1$ multiplication of fixed polynomials: $c(x) = '03'x^3 + '01'x^2 + '01'x + '02'$. This multiplication could be represented as the matrix multiplication.

$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} \qquad (1)$$

AddRoundKey transformation adds the state with round-key which is derived from initial secret key in the key schedule unit. This function could be performed by each byte XOR operation of state and round-key.

The round-key is calculated before the beginning of each round function in parallel with the operation of data encryption unit. Round-key generating is divided into two operations: key expansion and key selection. Because the key expansion of key schedule unit is byte-oriented structure, it could be converted and implemented with low efforts.

Above reviews of structural features of AES algorithm show us the fact that the main concern of design for our low power AES crypto module is how to implement SubByte and MixColumn transformation.

B. AES Architecture for Low Power Computing

In this section, we discuss the structural access to implement low power AES crypto module. From view point of low power consumption, we designed each component used in AES crypto module and optimized each modules. Then, optimized components are assembled for bigger functional unit.

What needs to be emphasized in the design of low power AES crypto module for wireless sensor network is the consideration of circuit area and power consumption. So, sharing and reusing circuit components and well defined data path for circuit modules are necessary to implement low power AES crypto module.

Our low power AES crypto module can be divided into two functional modules: data encryption unit and key schedule unit. For design efficiency, each unit implemented separately and then unified.

Data encryption unit: This functional module mainly conducts cryptographic operations. These cryptographic operations are performed predefined number of round functions according to the key size. If the key size is defined to 128bits, data processing unit performs 10 times of round operations. For efficiency and low power consumption, we design compact single round operation block and reuse it for remain round operations.

As mentioned above, the most important modules for low power AES crypto modules are S-box and MixColumn module. We focused the optimization of these modules to achieve our design goals, low power consumption and small area.

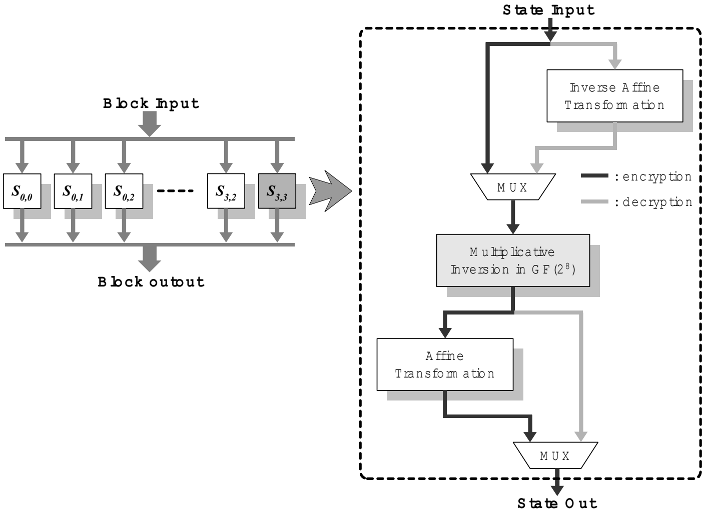

Fig. 2 AES SubByte and functional block of S-box

A straightforward implementation of SubByte is the use of separate 16 256-byte look-up tables. But this method requires large circuit area and a lot of power consumption.

As shown in Fig. 2, S-box function is composed with affine transforms and multiplicative inversion in GF(2^8). There are three methods to implement S-box. First method is using look-up table. This method requires 256-byte memory for each S-box. Second method uses the combination of a look-up table and combinational logic. In this case, Multiplication inversion uses look-up table and affine transform can be implemented by simple logics. Finally, S-box can be fully implemented by combinational logic. V. Rijmen[5] and J. Wolkerstorfer et al[6] suggested a compact method to implement AES S-box with combinational logics. We use just one S-box implemented by combinational logic for low power consumption and small area.

We also optimized the area of MixColumn. The matrix multiplication of MixColumn could be represented as follows;

$$\begin{aligned} b_0 &= xtime(a_0 \oplus a_1) \oplus (a_0 \oplus a_1 \oplus a_2 \oplus a_3) \oplus a_0 \\ b_1 &= xtime(a_1 \oplus a_2) \oplus (a_0 \oplus a_1 \oplus a_2 \oplus a_3) \oplus a_1 \\ b_2 &= xtime(a_2 \oplus a_3) \oplus (a_0 \oplus a_1 \oplus a_2 \oplus a_3) \oplus a_2 \\ b_3 &= xtime(a_3 \oplus a_0) \oplus (a_0 \oplus a_1 \oplus a_2 \oplus a_3) \oplus a_3 \end{aligned} \quad (2)$$

From above representations, we could know that MixColumn could be designed easily using just one basic module which imposes one xtime block, two or three byte-XOR logics and additional data path selector. This idea is depicted in Fig. 3. The basic module of MixColumn is represented by the dashed line box in Fig. 3.

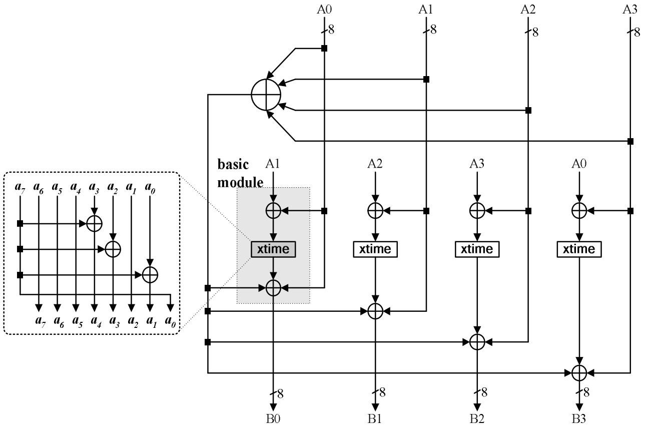
A0
A1
A2
A3
8
basic module
A1
A2
A3
A0
xtime
xtime
xtime
xtime
a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0
a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0
B0
B1
B2
B3

Fig. 3 MixColumn and its basic module

By repeating four times of basic module, MixColumn operation is executed. Xtime module used in MixColumn can be implemented easily with combinations of XOR gates and hard-wired logic shift operations.

From what have discussed above, we could design the architecture of optimized data encryption unit using 16-byte of data memory, one combinational S-box, MixColumn basic module, data path selectors and some 8-bit length data registers used to contain intermediate data.

Key schedule unit: This unit calculates round keys used in data encryption unit in prior to the beginning of each round operation. This unit is made up of 16-byte key memory, S-box; round constant module, data path selectors and additional 8-bit register to stores intermediate key values.

Compared with data encryption unit, the structure of key schedule unit is simple, but special attention is needed for efficient path controls for round key generation.

III. Low Power AES Crypto Module Design

There are many technical methods to design a low power circuit from algorithm to bottom level of circuit design. An architectural design combined with some low power techniques are needed to design our low power AES crypto module.

In this chapter, we first examine general low power techniques and then select some of them for our design. The later part of this chapter details the design of our low power AES module. We also describe power analysis results of some building blocks.

A. General Low Power Circuit Design Technologies

Low power consumption of electronic circuits can be achieved by using the combination of different techniques including algorithm and architectural design choice, logical and physical circuit design, and selection of silicon library [4]. We check here some power reduction techniques which could be used in our design.

Architectural design and optimization can be used to design a well defined data path and system structure. We also minimize circuit area using architectural access.

Logic/RTL level low power design techniques can be used to reduce the switching activity of each cell and to block circuit input data when it is in the idle state. These methods are called as gated clock and operand isolation respectfully. Logic synthesis level techniques optimize and minimize the area of the data path and circuit modules by effectively translate designs.

We first design the structure for low power AES crypto module using architectural design. Then we designed sub-blocks of AES crypto module and applied aforementioned low power techniques to each sub-block design. The design step can be divided into follows: architectural design, modify the module using low power techniques, power estimation, if necessary, module redesign. All of these design steps were repeated until each module optimized in area and power consumption.

B. Low Power AES Design

The low power AES crypto module could be divided into two functional blocks. One is data encryption unit which operates cryptographic functions using optimized single round data block. The other is key schedule unit offers round keys to data encryption unit.

Both functional blocks are designed using optimized architecture for low power consumption. After we design an optimized architecture of each unit, the synthesis and measurement of power estimation for each unit were followed.

We used Modelsim and Active-HDL simulator for the functional and timing simulations. After functional simulation, Synopsys Design Compiler was used to synthesis our low power AES crypto module. We also used Power Compiler tools to estimate and evaluate the power consumption of designed circuit. The 0.35um CMOS standard cell library of Samsung was used for synthesis and power estimations.

Data encryption unit for low power AES: The architecture of data encryption unit for our low power AES crypto module is depicted in figure 4. The unit consists basically of four parts: memory including registers, S-box, MC block, data path selectors.

Memory stores 128-bit initial state and iteration state of each round operation. It is expected to take the major part of area and power consumption of data encryption unit.

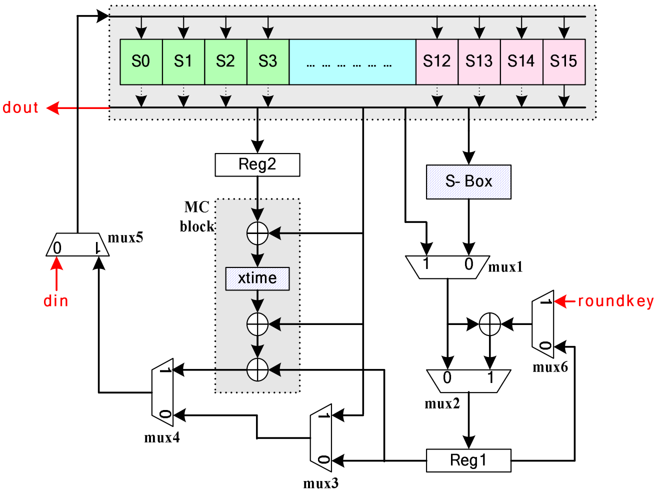

Fig. 4 Data encryption unit for low power AES crypto module

We designed memory using arrays of register to reduce circuit area and power consumption. Clock gating and operand isolation techniques were used to reduce the power consumption of memory block. The Table I represents the feature of our memory block.

TABLE I
FEATURES OF MEMORY BLOCK (CG: CLOCK GATING)

Op. Condition		Features		
Frequency (MHz)	Voltage (V)	Area (gates)	Power(uW)	
			before CG	after CG
10	2.5	2,800	4.46	1.23

We use two registers, Reg1 and Reg2, to store intermediate state value during round operations and shorten the delay of data paths. During transformation of one byte, the next byte could be read from memory. The transformed data is written to the memory of current reading address. Reg1 used for SubByte, ShiftRow, AddRoundKey and some part of MixCoulmn transformations. Reg2 mainly used for MixColumn operation. Each register could be implemented using 67 gates.

S-box could be implemented simply using 256 bytes ROM for 8-bit look-up table operation. But, ROMs do not have a good electrical characters and low response time. In Addition, using 256 byte for 8bit data processing is not efficient in the view point of circuit area. So, we use an alternative method which using combinational logic as suggested in [5], [6]. We could design the S-box using just 540gates.

MC block is a basic building block to perform MixColumn transformation. We mentioned the possibility to optimized structure for MixColumn operation from equation 2. As shown in figure 3, the MixColumn could be implemented by design simple basic module and reuse it with proper control of input path selection. Xtime in the basic module can be implemented with easy using three bit-wise XOR and wired shift operations. The MC block is implemented using 162gates.

We used six data path selectors for efficient round function operations. Mux1, 2, 3, 4 are mainly used for the data path of SubByte, ShiftRow transformation. Mux1, 2, 4 are used for MixColumn. Mux5 is used for the input data selection of data memory. All of these data selectors are implemented using 288 gates.

Table II shows the features of data encryption unit. It takes 3,972 gates to implement data encryption unit and uses 86 clocks to operate each round operation.

TABLE II
FEATURES OF DATA ENCRYPTION UNIT

Features				
Frequency (MHz)	Voltage (V)	Tech. Lib.	Area (gates)	Clock cycles
10	2.5	0.35um CMOS (Samsung)	3,972	86 clocks

Key schedule unit for low power AES: Key schedule unit consist register-based key data memory, round constant generator, S-box, key register, 2 byte XOR, and three data path selectors. The structure of key schedule unit appears in Fig. 5.

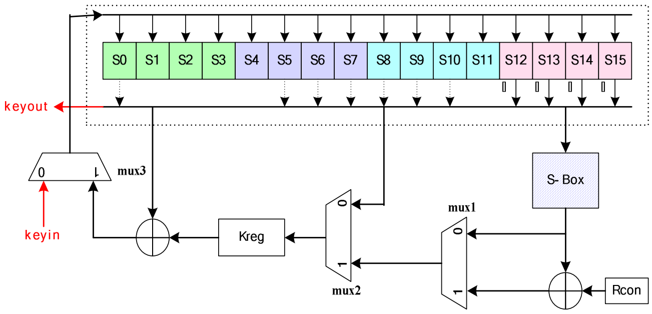

Fig. 5 Key schedule unit for low power AES crypto module

Register-based key data memory block loads initial secret key and then stores round key at each iteration of the key generate rounds. The structure of memory and S-box is the same as the one of data processing unit. Round constant generator can be implemented using simple 8-bit shift and rotate register which has initial binary value.

Mux1 is a data path selector which selects data in case of either using round constant value or not. Mux2 selects the data path in case of between when it needed to using S-box output and when using key memory data. Mux3 selects data path for key memory's input data. Kreg in figure 5 is 8-bit register used to store intermediate key data during the key scheduling. The key schedule unit can be implemented by 3714 gates and uses 17 clock cycles for single round key generation.

IV. CONCLUSION

We have described about the hardware architecture for low power AES crypto module. The designed low power AES crypto module using optimized architecture of data processing unit and key schedule unit are applicable to security applications which require low power characteristics such as a sensor node for sensor network and ubiquitous computing systems.

We have designed our low power AES crypto module using several low power techniques such as architectural optimization, clock gating, operand isolation, synthesis level optimization, and etc. Among applied low power design techniques, clock gating and operand isolation was effective to reduce the switching power of data and key memory and other register units. Using combinational S-box also reduced the operating power. We believe that there are a lot of alternatives and other techniques to reduce operating power if we use more techniques.

From the low power consumption and low hardware complexity of our designed AES crypto module, we can say our low power AES crypto module is suitable to use at the systems which have resource constrained environments.

REFERENCES

[1] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar. *Spins: Security protocols for sensor networks*. Wireless Networks, 8:521-534, 2002.

[2] J. Dijmen and V. Rijmen. AES Proposal: Rijndael. NIST AES Proposal, June 1998. Available at http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf.

[3] J. Dijmen and V. Rijmen. *The Design of Rijndael.* Springer-Verlag 2002.

[4] JoonDong Cho and YoungHoon Chang, *Low Power Digital Core Design for Multimedia and Communication Systems*, 2002.

[5] V. Rijmen, *Efficient Implementation of the Rijndael SBox*, http://www.esat.ku-leuven.ac.be/~rijmen/rijndael/.

[6] Johannes Wolkerstorfer, Elisabeth Oswald, and Mario Lamberger, An ASIC Implementation of the AES SBox, *CT-RSA 2002, LNCS 2271*, pp67-78, 2002.