

# OPTIMIZED AES CRYPTO DESIGN FOR WIRELESS SENSOR NETWORKS WITH A BALANCED S-BOX ARCHITECTURE

XU GUO<sup>1</sup>, ZHENG-LIN LIU, JI-PENG XING, WEN FAN, XUE-CHENG ZOU

Dept. of Electronic Sci. & Tech., Huazhong University of Sci. & Tech., Wuhan, 430074, China  
E-MAIL: <sup>1</sup>guoxuknight@gmail.com

## Abstract:

Advanced Encryption Standard (AES) has been widely adopted in security suits for wireless sensor networks, which has a considerable impact on the area, power consumption and lifetime of sensors. We find that the S-Box consumes much of the total AES circuit power, and the power dissipation and silicon area can vary more than several-fold, due to different implementation strategies. In this paper, a comprehensive study of different standard-cell implementations of the AES S-Box was presented, with respect to silicon area, critical path delay, and average power consumption. By analyzing the power consumption of the AES circuits, we proposed a compact, power-efficient S-Box circuit architecture: a full-balanced Decoder-Switch-Encoder (DSE) architecture. This approach can further reduce the silicon area and power consumption by 14% and 9%, respectively, compared to the original DSE S-Box. Also, our simulation results show that the proposed S-Box is the best choice among nine different S-Box implementations in terms of power-area product, and is optimal for AES crypto design for wireless sensor networks.

## Key words:

AES; Wireless sensor networks; S-Box; Power-efficient design

## 1. Introduction

Recent advances in technology have made the wireless sensor networks attract much attention due to its wide-range of potential applications, such as logistics, surveillance, military, environmental monitoring, and so on. Also, wireless sensor networks pose a number of challenging optimization problems. Generally, wireless sensor network systems have very limited circuit area and power supply by its nature. One of the most critical issues in wireless sensor networks is power efficiency, which is due to the characteristics of battery powered sensors and greatly affects the application lifetime [1].

Considering most of the applications, sensor network systems are forced to include security systems which prevent such threats as eavesdropping, message modification,

impersonation and even side channel analysis [2]. Advanced Encryption Standard (AES) is a new symmetric block cipher standard, which was issued by the National Institute of Standards and Technology (NIST) in 2001 [3]. Since AES has special particularities for wireless sensor networks, it has been adopted by several protocols. AES crypto module supports all security suites in IEEE 802.15.4 which is widely utilized in wireless sensor networks as the standard in Low-Rate Wireless Personal Area Network (LR-WPAN) [4]. Also, AES is one of candidate algorithms for Sensor Networks Encryption Protocol (SNEP) [5]. Hence, the area and power-efficiency of AES hardware implementations can greatly affect the sensors in severely resource-constrained networks.

So, the major challenges to implement efficient AES crypto module for sensor network systems are simplified into two issues: how to achieve high power-efficiency and meet the requirement of limited size in the AES design. In the following section, a reusing AES circuit implementation is shown, and the results of power evaluation of the AES circuits are described and analyzed. In Section 3, the proposed full-balanced S-Box architecture and its ASIC implementation results are compared. Finally, concluding remarks are made in Section 4.

## 2. Power consumption evaluation

### 2.1. Power analysis method

For analyzing the power consumption of the AES circuits, a simulation-based analysis method was used. In this method, after functional simulation a netlist was acquired with the UMC 0.25  $\mu\text{m}$  1.8V technology library using Synopsys Design Compiler. Then, a timing simulation at the gate level is performed using a given set of test input data, and the switching activities of all internal gates are logged. The simulation is performed at the clock frequency of 10MHz with all patterns of the primary input switching. The circuit average power is computed using

Synopsys Prime Power. It should be pointed out that although the absolute values of the circuit performance are different between different ASIC libraries, the ratios of the parameters are almost the same.

## 2.2. Power consumption of AES circuits

There have been many studies for hardware implementations of the AES algorithm using ASIC libraries [6] [7], in most of which high throughput and low cost AES designs were presented.

The AES consists of an initial round key addition, variable Nr-1 rounds and a final round, and Nr is 10, 12, or 14 depending on the key length. The round is composed of sixteen 8-bit S-boxes computing SubBytes, 128-bit block ShiftRows, and four 32-bit MixColumns operations. Equivalent decryption structure has exactly the same sequence of transformations as in the encryption structure [8]. Taking advantages of this feature, it is more efficient to integrate the encryption and decryption into the same hardware. The AES reusing structure for the encryption/decryption algorithm is exhibited in Figure 1, including SubBytes, MixColumns, ShiftRows, AddRoundKey and KeyExpansion units.

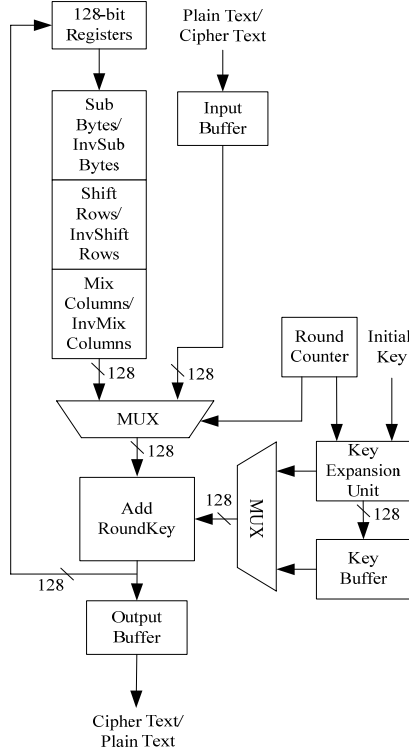


Figure 1. AES reusing architecture

The total power consumption of the AES encryption chip  $P_{AES}$  can be obtained as follows:

$$P_{AES} = P_{subbytes} + P_{mixcolumns} + P_{shiftrows} + P_{addroundkey} + P_{keyschedule} + P_{others} \quad (1)$$

$P_{subbytes}$ ,  $P_{mixcolumns}$ ,  $P_{shiftrows}$ ,  $P_{addroundkey}$ ,  $P_{keyschedule}$ , and  $P_{others}$  are power consumptions of SubBytes, MixColumns, ShiftRows, AddRoundKey, KeyExpansion, and Registers, respectively.

The power estimation results for each primitive AES component are shown in Table 1. In this table, the S-Box in a composite field  $GF(2^4)$  [9] is used. It is obvious that the SubBytes operations contribute to much of the total power consumption in AES encryption operations. The same fact was reported in S. Morioka's research [10]. Generally, there are twenty S-boxes in basic AES structure, including sixteen S-boxes for SubBytes unit, and the other four S-boxes for KeyExpansion unit. So the main concern of designing our low power AES crypto module is how to optimize the implementation of SubBytes transformation.

Table 1. Power consumption of each AES component (UMC 0.25 $\mu$ m 1.8v CMOS standard cell)

|            | Average Power<br>(mW@10MHz) | Ratio<br>(%) |
|------------|-----------------------------|--------------|
| SubBytes   | 24.7                        | 46           |
| MixColumns | 10.7                        | 20           |
| KeyShedule | 9.30                        | 17           |
| Others     | 8.90                        | 17           |

## 2.3. Power analysis of the S-Box

In order to find an optimal structure of S-Boxes to reduce the power consumption we investigate the origins of the power dissipation in various aspects at first. Since the S-Box only contains combinatorial circuits, the power dissipation consists of several main components, as shown in Equation (2):

$$P_{total} = P_{switching} + P_{internal} + P_{leak} \quad (2)$$

Where  $P_{switching}$  is dynamic switching power due to the load capacitance charge or discharge,  $P_{internal}$  is the power dissipated within a cell, and  $P_{leak}$  is the leakage power due to the reverse-biased junction leakage and sub-threshold leakage. Dynamic switching power is the dominant active power dissipation component in CMOS circuits, which is defined as [11]

$$P_{dynamic} = \alpha_{0 \rightarrow 1} C_L V_{dd}^2 f \quad (3)$$

Where  $\alpha_{0 \rightarrow 1}$  is the switching activity,  $C_L$  is the load capacitance,  $V_{dd}$  is the supply voltage, and  $f$  is the frequency of the operation.

Again, we take the S-Box in composite field  $GF(2^4)$  as an example to illustrate the percentage of the total power

consumption by each part.

Table 2. Average Power of the S-Box (UMC 0.25 $\mu$ m 1.8v CMOS standard cell)

|           | Average Power<br>(mW@10MHz) | Ratio<br>(%) |
|-----------|-----------------------------|--------------|
| Dynamic   | 4.78e-1                     | 100          |
| Internal  | 2.89e-1                     | 60.5         |
| Switching | 1.89e-1                     | 39.5         |
| Glitch    | 2.20e-2                     | 4.60         |
| Leakage   | 3.08e-6                     | $\approx 0$  |

According to Table 2 the dynamic power, composed of switching power and internal power, is the main source of the total consumption, while the leakage power, also called static power, can be almost neglected. Since the internal power, determined by different requirements for clock speed and technology library, is due mostly to either short-circuit power or the charging and discharging of internal capacitance within library cells, our work focuses on the logic level optimization to reduce the switching power. The switching power of a driving cell is the power dissipated by the charging and discharging of the load capacitance at the output of the cell. Because such charging and discharging are the result of the logic transitions at the output of the cell, switching power increases as logic transitions increases. The glitch power, as a part of the dynamic switching power caused by dynamic hazards, is also considered. Regarding the illustrated S-Box in composite field, it involves many crossing and branching signal paths. The signal arrival times of the internal gates are very different, and hence if multiple gates are connected serially, the hazards propagate into the circuit path and some extra power is consumed. Note that the estimation of glitch power here is based on the pulse width, which is less than the rise and fall ramp. It is possible that if glitches, generated in the circuits with long chains of gates, have greater pulse width than that, they would be confounded with full transitions. Therefore, the power ratio of glitch power may be higher in actual operations.

Based on above analysis, we considered that the power consumption of the S-Boxes was strongly influenced by the number of dynamic hazards. So our strategy is to eliminate the differences of signal arrival time at each gate in S-Box circuits.

### 3 Implementation of proposed S-Box

#### 3.1. Different strategies for S-Box implementation

There exists a rich literature devoted to the efficient design of cryptographic S-Boxes, all of which can be attributed to three basic ways. The first one is constructing cir-

cuit directly from the truth-table of the S-box. Simply, an asynchronous ROM with 256 bytes for each S-box could be instantiated. Since ROMs do not have good electrical characteristics and short response time, combinatorial logic is chosen for the implementation of S-Box. The second method is implementing multiplicative inverse and affine transform with combinatorial circuits using look-up tables or direct relationship between input and output values of the S-Box. The third approach is implementing the S-Box by combinatorial logic using its arithmetic properties.

For the second approach, the S-Box hardware can be achieved from its truth table by using two-level logic, such as SOP (Sum of Products) (denoted as **SOP**), or by using decision diagrams, such as BDD (Binary Decision Diagram) (denoted as **BDD**) [12]. In addition, the Decoder-Switch-Encoder structure (denoted as **DSE**) [13] is developed, which is more efficient than straight-forward implementation of a hardware look-up table (denoted as **LUT**) in terms of delay and power, while both of them directly use the input-output relations.

For the third approach, implementation of multiplicative inverse in the composite field (denoted as **GF**) [9], which can create compact structures, is well studied to substitute the original implementation in the Galois field GF(2<sup>8</sup>). Then, by converting some parts of the **GF** S-Box into two-level logic, a power-optimized structure called 3-stage PPRM (Positive Polarity Reed-Muller) (denoted as **PPRM**) [14] is also developed.

Table 3. Comparison of various AES implementations (UMC 0.25 $\mu$ m 1.8v CMOS standard cell, 1 gate=NAND2XL)

|      | Area<br>(gate) | Delay<br>(ns) | Average Power<br>(mW@10MHz) |
|------|----------------|---------------|-----------------------------|
| LUT  | 573            | 4.54          | 1.79e-1                     |
| SOP  | 575            | 4.46          | 1.56e-1                     |
| BDD  | 1811           | 2.65          | 1.02                        |
| DSE  | 780            | 3.17          | 7.58e-2                     |
| GF   | 373            | 8.04          | 4.78e-1                     |
| PPRM | 577            | 6.70          | 4.15e-1                     |

We have implemented all solutions mentioned above in Verilog HDL, all of which just consist of combinatorial logic. The experimental results of various S-boxes are shown in Table 3. From Table 3 we could easily find out that **DSE** is an ideal candidate for low power AES design for wireless sensor networks among the six structures.

#### 3.2. The improved balanced S-Box architecture

Considering the DSE S-box, the switch unit executes wire permutation without power dissipation. Therefore, the power optimization is translated into the low power en-

coder and decoder design.

Although the decoder module within the DSE structure has been well studied by Bertoni [13] to be power-efficient, the encoder design only considered the maximum reuse of the ORs optimized by synthesis tools. However, aiming at minimizing chip area as a primary goal, we find that the resulting netlist can still be improved to be more power-efficient.

Through the implementation of various S-Boxes we notice that when the circuit structure of the S-Box is changed, the power of the S-Box circuits can vary more than several-fold (see Table 3), due to the changes in the situations creating and propagating dynamic hazards, even though the total circuit size has less effect on the power consumption than expected. In this case, only considering the resource reuse, the number of gates can be cut down, but we would neglect other factors that may further decrease the power consumptions. Inspired by the 3-stage decoder structure, we developed a 4-stage encoder structure that has balanced signal paths to eliminate the dynamic hazards and maximum reuse of the gates.

We first consider a simple sub-encoder with four inputs:  $X_0, X_1, X_2$  and  $X_3$  and two outputs:  $Y_1$  and  $Y_2$ , and the Boolean function becomes

$$\begin{cases} Y_0 = X_1 + X_3 \\ Y_1 = X_2 + X_3 \end{cases} \quad (4)$$

Where the input  $X_0$  is unused. Accordingly, we can arrange the eight outputs of encoder into four pairs with four sub-encoders. As shown in Fig. 2, all 256 inputs ( $I_{0x00} \sim I_{0xff}$ ) are enumerated. Note that  $xxxx\_xx00$  denotes 8-bit binary digits with the last two bits '00', and  $x0$  denotes 8-bit hexadecimal digits with the last four bits '0x0', both of which represent the subscripts of the inputs. The values in dashed frame are unused.

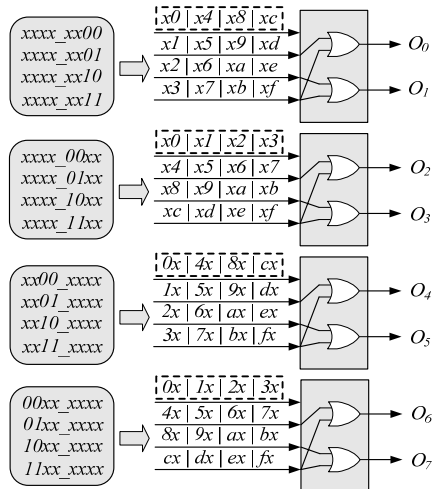


Figure 2. Diagram of the proposed encoder

From Fig.2 we note that many four consecutive inputs can be reused to generate the outputs, for instance,  $I_{0xcc} \sim I_{0xff}$  can be reused to generate  $O_2, O_3, O_6$  and  $O_7$ . Therefore, we try to maximize the reuse of 4-way ORs. On the other hand, in order to eliminate spurious transitions caused by the creation and propagation of dynamic hazards, we build the circuits with balanced signal paths. Adopting the above two methods, the thus built structure is shown in Fig. 3.

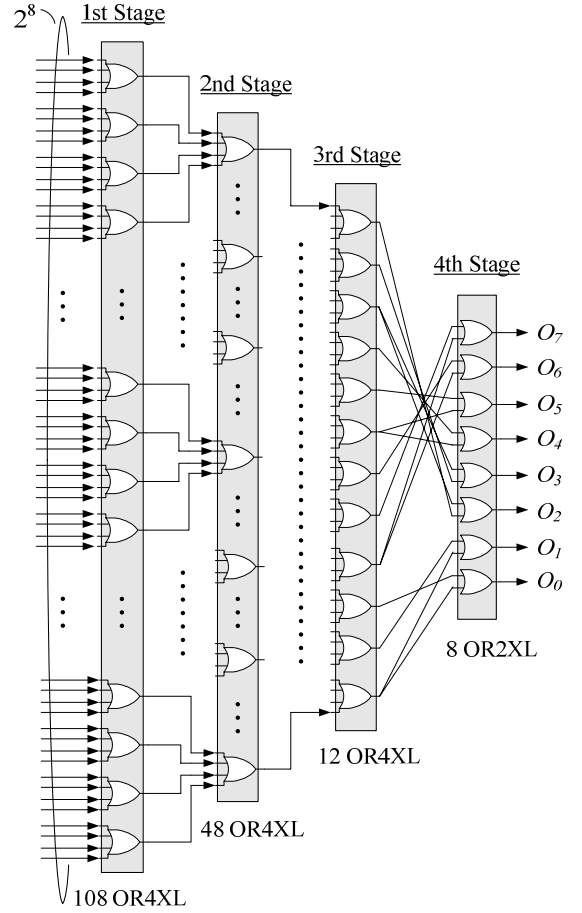


Figure 3. Optimized encoder structure for S-Box

Optimizing the original DSE S-Box by replacing the encoder module generated by synthesis tools with our proposed encoder, the power consumption is reduced by 8% (see Table 4).

So far, our work has optimized the DSE S-Box with power-efficiency as the primary goal; nevertheless, small silicon area for sensor nodes is important as well. Hence, we seek to find a trade off between power and area, and then our work turns to optimize the decoder circuits by decreasing the number of gates at the expense of a little power consumption. Based on the original DSE S-Box implementation, the decoder is almost constructed with 2-way ANDs. Our method is to optimize the silicon area

using smaller cells, and keep the original balanced 3-stage decoder structure. We have devised several structures to improve the 3-stage decoder, and the structure, which meets our requirements to be both compact and power-efficient, are constructed with three stages built by NANDs, ORs and NORs respectively.

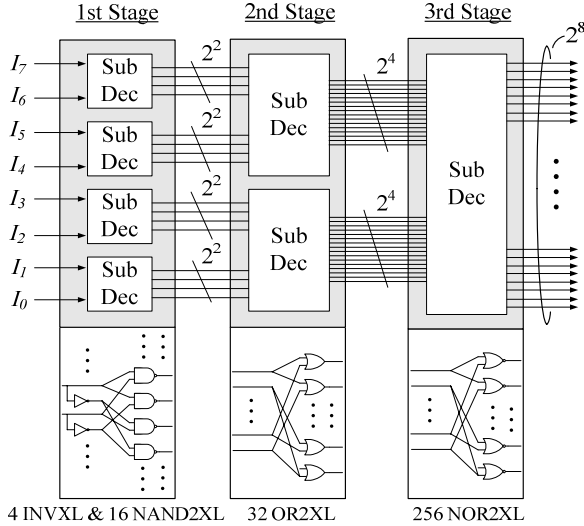


Figure 4. Optimized decoder structure for S-Box

From Fig. 4, keeping the logic function of the decoder module, by substituting the 2-way ANDs with 2-way NANDs, we save about 5 gates in the first stage; in the second stage, the area is unchanged since 2-way ORs and 2-way ANDs have the same size; in the last stage, 85 gates have been saved by replacing the 2-way ANDs with 2-way NORs. In all, the silicon area of the decoder is decreased to only 78% with respect to the original architecture (see Table 4). Combining our proposed decoder and encoder circuits, we obtain a new full-balanced S-Box, characterized as both compact and power-efficient.

### 3.3. Experimental results

Based on above analysis we have obtained several decoder and encoder structures. To further investigate the optimal combination of the decoder and encoder, we have tried all the possible implementations and some of the results are shown in Table 4. The simplest design is using synthesis tools to optimize both decoder and encoder, which is denoted as **DSE I**. The implementation used a 3-stage decoder and a synthesized encoder is called **Bertoni** [13]. We also applied our proposed 4-stage encoder to substitute the encoder module in **Bertoni**. This approach is denoted as **DSE II**. Our proposed full-balanced S-Box is denoted as **Proposed**. From the simulation results, by using our proposed 4-stage encoder, **DSE II** exceeds **Bertoni** in

all aspects. Further, **Proposed** reduces the area and power compared to **DSE II** at the expense of a little more critical path delay. Since area and power factors are more important when applied in the wireless sensor networks, especially to 802.15.4 which is characterized as a low-rate, small, power-efficient solution, **Proposed** is the best choice.

Table 4. Comparison of various DSE S-Boxes (UMC 0.25 $\mu$ m 1.8v CMOS standard cell, 1 gate=NAND2XL)

|          | Area (gate) | Delay (ns) | Average Power (mW@10MHz) |
|----------|-------------|------------|--------------------------|
| DSE I    | 681         | 2.76       | 9.08e-2                  |
| DSE II   | 763         | 3.03       | 6.99e-2                  |
| Bertoni  | 780         | 3.17       | 7.58e-2                  |
| Proposed | 673         | 3.19       | 6.92e-2                  |

Fig. 6 shows our results in terms of the power-area product. All power-area products have been normalized to the product of **LUT**. This metric is particularly relevant for applications which require both small silicon area and low power consumption, e.g. cryptographically enhanced RFID tags or sensor nodes [15]. Due to its high power consumption and large size, **BDD** has much bigger power-area product than the others (see Table 3), and the product is not illustrated in the figure for display convenience. Our proposed full-balanced S-Box gains the smallest power-area product as expected.

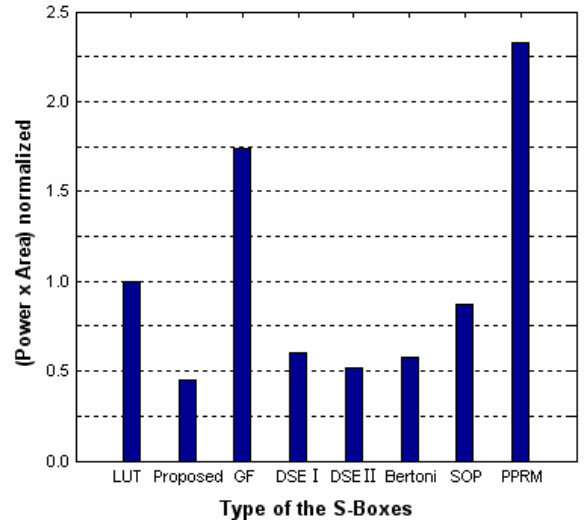


Figure 6. Power-area product of various S-Boxes

## 4. Conclusions

In this paper, we have developed a full-balanced DSE architecture for small size and low-power S-Box circuits.

The designed S-Box for AES crypto module, using optimized balanced architectures of 3-stage decoder and 4-stage encoder, is applicable to security applications which require both compact area and power-efficiency, such as sensor nodes for wireless sensor networks. The power consumption of S-Box circuits can be reduced by avoiding the creation and propagation of dynamic hazards, and the silicon size can be decreased by optimizing the logic at gate level. Simulation results, obtained at 10 MHz using a 0.25 $\mu$ m 1.8v CMOS technology, show that the area and power consumption are reduced by 14% and 9%, respectively, compared to the original DSE S-Box [11]. Moreover, we have analyzed and compared various cost metrics of selected nine S-Box implementations, and our proposed full-balanced S-Box achieves the smallest power-area product.

#### Acknowledgements

The research described in this paper has been supported by the Natural Science Foundation of Hubei, China under grant 2006ABA080.

#### References

- [1] M. T. Thai, F. Wang, and D. Z. Du, "Coverage Problems in Wireless Sensor Networks: Designs and Analysis", *International Journal of Sensor Networks*, Special Issue on Coverage Problems in Sensor Networks, 2005.
- [2] M. Kim, J. Kim, and Y. Choi, "Low Power Circuit Architecture of AES Crypto Module for Wireless Sensor Network", *Transactions on Engineering, Computing and Technology V8* October 2005, <http://www.enformatika.org/data/v8/v8-28.pdf>
- [3] "Advanced Encryption Standard (AES)", *Federal Information Processing Standards Publication 197*, Nov. 2001.
- [4] *Wireless medium access control and physical layer specifications for low-rate wireless personal area networks*. IEEE Standard, 802.15.4-2003, May. 2003. ISBN 0-7381-3677-5.
- [5] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "Spins: Security protocols for sensor networks", *Wireless Networks*, Vol. 8, pp. 521-534, 2002.
- [6] I. Verbauwhede, P. Schaumont, and H. Kuo, "Design and Performance Testing of A 2.29-GB/s Rijndael Processor", *IEEE Journal of Solid-State Circuits*, Vol. 38, No. 3, pp. 569-572, Mar. 2003.
- [7] S. Morioka and A. Satoh, "A 10 Gbps Full-AES Crypto Design with a Twisted-BDD SBox Architecture," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* archive, Vol. 12, No. 7, pp. 686-691, Jul. 2004.
- [8] V. Fischer and M. Drutarovsky, "Two Methods of Rijndael Implementation in Reconfiguration Hardware", *Proceeding of CHES 2001*, Paris, pp. 77-92, May 2001.
- [9] J. Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC Implementation of the AES S-boxes", *The Cryptographer's Track at the RSA Conference, CT-RSA 2002*, LNCS 2271, pp. 67-78, 2002.
- [10] S. Morioka and A. Satoh, "An optimized S-box circuit architecture for low power AES design", *CHES 2002*, LNCS 2523, pp.172-186, 2003.
- [11] J. M. Rabaey, A. Chandrakasan, and B. Nikolic, "Digital Integrated Circuits, A Design Perspective", Second Edition, Prentice-Hall, Upper Saddle River, NJ, 2003.
- [12] R. E. Bryant, "Graph-Based Algorithms for Boolean Function Manipulation", *IEEE Trans. on Computer*, Vol.C-35, No.8, pp.677-691, 1986.
- [13] G. Bertoni, M. Macchetti, L. Negri, and P. Frangneto, "Power-efficient ASIC Synthesis of Cryptographic Sboxes", In *Proceedings of the 14th ACM Great Lakes symposium on VLSI (GLSVLSI 2004)*, pp. 277-281, ACM Press, 2004.
- [14] S. Morioka, and A. Satoh, "An optimized S-box circuit architecture for low power AES design", *CHES 2002*, LNCS 2523, pp.172-186, 2003.
- [15] T. Stefan, M. Feldhofer, and J. Großschädl, "Area, Delay, and Power Characteristics of Standard-Cell Implementations of the AES S-Box", In *Proceedings of 6th Work Shop on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS 2006)*, LNCS 4017, pp. 457-466, Jul. 2006.