Journal of Zhejiang University SCIENCE A
ISSN 1673-565X (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

A low-power Rijndael S-Box based on pass transmission gate and composite field arithmetic*

ZENG Yong-hong†, ZOU Xue-cheng, LIU Zheng-lin, LEI Jian-ming

(*Research Center for VLSI and Systems, Department of Electronic Science & Technology, Huazhong University of Science & Technology, Wuhan 430074, China*)

†E-mail: zyher1974@126.com

Received Mar. 9, 2007; revision accepted Apr. 27, 2007

Abstract: Using composite field arithmetic in Galois field can result in the compact Rijndael S-Box. However, the power consumption of this solution is too large to be used in resource-limited embedded systems. A full-custom hardware implementation of composite field S-Box is proposed for these targeted domains in this paper. The minimization of power consumption is implemented by optimizing the architecture of the composite field S-Box and using the pass transmission gate (PTG) to realize the logic functions of S-Box. Power simulations were performed using the netlist extracted from the layout. HSPICE simulation results indicated that the proposed S-Box achieves low power consumption of about 130 μW at 10 MHz using 0.25 μm/2.5 V technology, while the consumptions of the positive polarity reed-muller (PPRM) based S-Box and composite field S-Box based on the conventional CMOS logic style are about 240 μW and 420 μW, respectively. The simulations also showed that the presented S-Box obtains better low-voltage operating property, which is clearly relevant for applications like sensor nodes, smart cards and radio frequency identification (RFID) tags.

Key words: Composite field, Rijndael S-Box, Full-custom, Pass transmission gate (PTG), Low power consumption, Low-voltage
doi:10.1631/jzus.2007.A1553 **Document code:** A **CLC number:** TN4; TP309

INTRODUCTION

The National Institute for Standard and Technology (NIST) selected the Rijndael block as the Advanced Encryption Standard (AES) algorithm in 2000. Federal Information Processing Standards 197 (FIPS-197) was issued by the NIST in 2001 (Kuorilehto *et al*., 2005). The Rijndael algorithm offers higher levels of security as compared with the Data Encryption Standard (DES) and is currently replacing the DES as the worldwide standard symmetric encryption algorithm (Mentens *et al*., 2005).

As the only nonlinear structure in Rijndael algorithm, the S-Box dominates the hardware complexity of the Rijndael cryptographic module. The hardware implementation efficiency of Rijndael algorithm in terms of size, speed, and power consumption depends largely on the number and style of S-Boxes implementation (Wolkerstorfer *et al*., 2002). Since there are many hardware design options for the S-Box, it is challenging to find an optimal implementation for a particular purpose. Many implementations for S-Box have been proposed recently, and their performances have been evaluated by using standard CMOS libraries (Satoh *et al*., 2001; Morioka and Satoh, 2002; Wolkerstorfer *et al*., 2002; Macchetti and Bertoni, 2002; Bertoni *et al*., 2004; Canright, 2005; Mentens *et al*., 2005). However, there is no report using the full-custom design methodology, as far as we know. In fact, S-Box is a small module and does not require the excessive driving capability offered by standard cells. Moreover, output transistors of gates can be dimensioned smaller and this will in

* Project supported by the Hi-Tech Research and Development Program (863) of China (No. 2006AA01Z226) and the Scientific Research Foundation of Huazhong University of Science and Technology (No. 2006Z001B), China

turn make it possible to scale all transistors down without deteriorating performance. So we assume that the required chip's area and power consumption can be reduced if we use full-custom design methodology.

In this paper, the research focuses on the full-custom hardware implementation of the S-Box for resource-limited embedded applications, where both low power and small silicon area are mandatory. Having the possibility to deal with a wide supply voltage range, the low power enables the design of flexible and efficient power management strategies, especially valuable in the following application domains: sensor nodes, smart cards, and radio frequency identification (RFID) tags (Tillich *et al*., 2006).

Rudra *et al*.(2001) proposed the use of composite field arithmetic to reduce the computation cost of the S-Box. This solution can result in a very compact hardware implementation. In the S-Box of (Satoh *et al*., 2001), the finite field $GF(2^8)$ is represented as the composite field $GF(((2^2)^2)^2)$. In this paper, it is optimized for the reduction of the total power consumption. In addition, the pass transmission gate (PTG) was used to implement the logic functions of the S-Box, which results in an even more compact S-Box design and the reduction of power consumption. In our experimental comparison, the resulting circuit using 0.25 μm/2.5 V CMOS technology achieves lower power consumption than that using the positive polarity reed-muller (PPRM) based S-Box presented in (Morioka and Satoh, 2002), which is to our knowledge the lowest power implementation over composite field so far. The simulation results also showed that our implementation exhibits good low-voltage operating property.

COMPOSITE FIELD S-BOX

The two pairs $\{GF(2^n), Q(y)\}$ and $\{GF((2^n)^m), P(x)\}$ constitute a composite field if $GF(2^n)$ is constructed from $GF(2)$ by $Q(y)$ and $GF((2^n)^m)$ is constructed from $GF(2^n)$ by $P(x)$, where $Q(y)$ and $P(x)$ are polynomials of degree n and m, respectively. The fields $GF((2^n)^m)$ and $GF(2^k)$ ($k=nm$) are isomorphic to each other (Rudra *et al*., 2001). Since the complexity of various arithmetic operations varies with the fields, we assume that the computation cost reduction in a given underlying field $GF(2^k)$ exploiting the isomorphism to map a computation from one field to the other is possible. In the Rijndael S-Box, a multiplicative inverse transformation over Galois field $GF(2^8)$ determines the overall complexity of the Rijndael arithmetic. The composite field arithmetic mentioned above can be used to create compact S-Box circuit, and is far better suited for hardware implementation. Satoh *et al*.(2001) introduced a composite field $GF(((2^2)^2)^2)$ and presented the involved hardware implementation. Another area efficient implementation is presented in (Wolkerstorfer *et al*., 2002), where the field $GF(2^8)$ is represented as an extension of its subfield $GF(2^4)$.

In this paper we represent $GF(2^8)$ as the composite field $GF(((2^2)^2)^2)$. In this case, $GF(((2^2)^2)^2)$ is the field extension of degree 2 over $GF((2^2)^2)$ constructed using the irreducible polynomial $R(y)=y^2+y+\lambda$, with y a root of the polynomial and $\lambda=\{1100\}_2$. $GF((2^2)^2)$ is the field extension of degree 2 over $GF(2^2)$ constructed using the irreducible polynomial $Q(z)=z^2+z+\eta$, where z is a root of the polynomial and $\eta=\{10\}_2$. $GF(2^2)$ is the field extension of degree 2 over $GF(2)$ constructed using the irreducible polynomial $P(w)=w^2+w+1$, with root w. Thus, we can use the following operation to compute the inverse transformation over $GF(2^8)$ in the Rijndael S-Box:

Given $a\in GF(2^8)$, $a=(a_\mathrm{l}, a_\mathrm{h})$, where a_l, $a_\mathrm{h}\in GF((2^2)^2)$, we want to find an element $b\in GF(2^8)$, $b=(b_\mathrm{l}, b_\mathrm{h})$, where $b_\mathrm{l}, b_\mathrm{h}\in GF((2^2)^2)$ such that

$$ab=(1, 0). \tag{1}$$

Directly carrying out this multiplication yields

$$\begin{aligned} ab &= (a_\mathrm{h}y + a_\mathrm{l})(b_\mathrm{h}y + b_\mathrm{l}) \\ &= a_\mathrm{l}b_\mathrm{l} + (a_\mathrm{h}b_\mathrm{l} + a_\mathrm{l}b_\mathrm{h})y + a_\mathrm{h}b_\mathrm{h}y^2 \mod R(y) \\ &= (a_\mathrm{l}b_\mathrm{l} + \{\lambda\}a_\mathrm{h}b_\mathrm{h}) + (a_\mathrm{l}b_\mathrm{h} + a_\mathrm{h}b_\mathrm{l} + a_\mathrm{h}b_\mathrm{h})y \mod R(y). \end{aligned} \tag{2}$$

Substituting Eq.(2) into Eq.(1) gives two linear equations with the solution

$$\begin{cases} b_\mathrm{h} = \dfrac{a_\mathrm{h}}{a_\mathrm{l}^2 + a_\mathrm{l}a_\mathrm{h} + \{\lambda\}a_\mathrm{h}^2}, \\ b_\mathrm{l} = b_\mathrm{h} + \dfrac{a_\mathrm{l}}{a_\mathrm{l}^2 + a_\mathrm{l}a_\mathrm{h} + \{\lambda\}a_\mathrm{h}^2}. \end{cases} \tag{3}$$

So we can see that inversion of an element in $GF(2^8)$ can be accomplished by 1 inversion, 3 general multiplications, 3 additions, 1 constant multiplication and 2 squarings, where again all operations are over $GF((2^2)^2)$. Our implementation of S-Box shown in Fig.1 can be applied to both encryption and decryption. It consists of affine transformations (affine and affine^{-1} block), isomorphism functions (map and map^{-1} block), the inverter over $GF(((2^2)^2)^2)$ block and selectors.

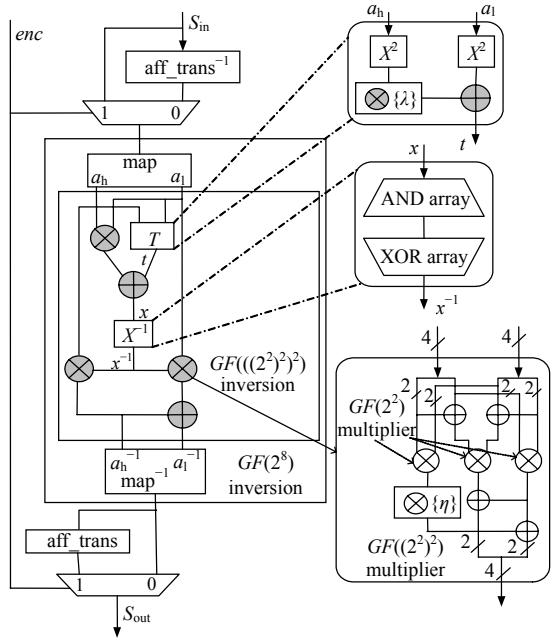


Fig.1 Our proposed S-Box structure based on $GF(((2^2)^2)^2)$

The multiplication in $GF((2^2)^2)$ can be done by multiplication of polynomial with a modular reduction step. The processing is as follows: with q, c, $d \in GF((2^2)^2)$, $c=(c_l, c_h)$, $d=(d_l, d_h)$, where c_l, c_h, d_l, $d_h \in GF(2^2)$,

$$\begin{aligned} q &= cd = (c_h z + c_l)(d_h z + d_l) \\ &= c_l d_l + (c_h d_l + c_l d_h) z + c_h d_h z^2 \mod Q(z) \\ &= (c_l d_l + \{\eta\} c_h d_h) + [(c_l + c_h)(d_l + d_h) + c_l d_l] z \mod Q(z). \end{aligned} \tag{4}$$

Deriving the formula for multiplication in $GF(2^2)$ is similar to multiplication in $GF((2^2)^2)$, with e, $f \in GF(2^2)$, $e=(e_l, e_h)$, $f=(f_l, f_h)$, where e_l, e_h, f_l, $f_h \in GF(2)$,

$$\begin{aligned} ef &= (e_h w + e_l)(f_h w + f_l) \\ &= e_l f_l + (e_h f_l + e_l f_h) w + e_h f_h w^2 \mod P(w) \\ &= (e_l e_l + e_h f_h) + (e_l f_h + e_h f_l + e_h f_h) w \mod P(w). \end{aligned} \tag{5}$$

Since the multiplication of an element in $GF(2^2)$ with the constant $\{\eta\}$ is a special case of multiplication over $GF(2^2)$, its formula can be obtained with $f=\{\eta\}=\{10\}_2$.

$$\{\eta\} e = e_h + (e_l + e_h) w \mod P(w). \tag{6}$$

Substituting Eqs.(5) and (6) into Eq.(4), the multiplication in $GF((2^2)^2)$ can be obtained by

$$\begin{cases} q_0 = c_{l0} d_{l0} \oplus c_{l1} d_{l1} \oplus c_{h0} d_{h1} \oplus c_{h1} d_{h0} \oplus c_{h1} d_{h1}, \\ q_1 = c_{l0} d_{l1} \oplus c_{l1} d_{l0} \oplus c_{l1} d_{l1} \oplus c_{h0} d_{h0} \oplus c_{h0} d_{h1} \oplus c_{h1} d_{h0}, \\ q_2 = c_{l0} d_{l0} \oplus c_{l1} d_{l1} \oplus (c_{l0} \oplus c_{h0})(d_{l0} \oplus d_{h0}) \oplus \\ \quad (c_{l1} \oplus c_{h1})(d_{l1} \oplus d_{h1}), \\ q_3 = (c_{l0} \oplus c_{h0})(d_{l1} \oplus d_{h1}) \oplus (c_{l1} \oplus c_{h1})(d_{l0} \oplus d_{h0}) \oplus \\ \quad c_{l0} d_{l1} \oplus c_{l1} d_{l0} \oplus c_{l1} d_{l1} \oplus (c_{l1} \oplus c_{h1})(d_{l1} \oplus d_{h1}). \end{cases} \tag{7}$$

Squaring and multiplication with the constant $\{\lambda\}$ in $GF((2^2)^2)$ are the special case of the general multiplication and are respectively given by

$$\begin{cases} q_0 = x_{l0} \oplus x_{l1} \oplus x_{h1}, \quad q_1 = x_{l1} \oplus x_{h0}, \\ q_2 = x_{h0} \oplus x_{h1}, \quad q_3 = x_{h1}, \end{cases} \tag{8}$$

$$\begin{cases} q_0 = y_{h0}, \quad q_1 = y_{h1}, \\ q_2 = y_{l0} \oplus y_{l1} \oplus y_{h0} \oplus y_{h1}, \; q_3 = y_{l0} \oplus y_{h0}, \end{cases} \tag{9}$$

where, $\{c_{h1}, c_{h0}, c_{l1}, c_{l0}\}$ and $\{d_{h1}, d_{h0}, d_{l1}, d_{l0}\}$ denote the inputs of the general multiplication, $\{x_{h1}, x_{h0}, x_{l1}, x_{l0}\}$ and $\{y_{h1}, y_{h0}, y_{l1}, y_{l0}\}$ respectively denote the input of the squaring and the constant multiplication, and variable $\{q_3, q_2, q_1, q_0\}$ denotes the output.

Actually, the power consumption for an S-Box is strongly influenced by the number of dynamic hazards. The main reasons for propagating dynamic hazards lie in two characteristics: the difference of signal arrival time at each gate and the propagation probability of signal transitions. To reduce the power consumption of the S-Box, we optimized the architecture of (Satoh *et al*., 2001). In our implementation (Fig.1): (1) An optimized circuit architecture of

PPRM (Sasao, 1993) proposed in (Morioka and Satoh, 2002) is used to implement the $GF((2^2)^2)$ inversion. In the PPRM-based inversion denoted with X^{-1} in Fig.1, the hazard-transparent XOR gates are located after the other gates to block the hazards. The detailed formula of the X^{-1} block can be found in Appendix A-2 of (Morioka and Satoh, 2002). (2) To minimize the critical path of the complete S-Box, we adopted the structure of (Wolkerstorfer *et al*., 2002), where the affine transformation and the isomorphism map are done separately. In the corresponding architecture of (Satoh *et al*., 2001), however, those two are combined into a single optimized operation to minimize the overall gate count. We have analyzed the power consumption of the above-mentioned two S-Boxes implementation. The power-simulation results showed that the S-Box of (Wolkerstorfer *et al*., 2002) (about 350 μW at 10 MHz) is better than that of (Satoh *et al*., 2001) (about 420 μW at 10 MHz) in the power property.

IMPLEMENTATION

Our implementation is a full-custom circuit on a 0.25 μm logic 2.5 V/5.0 V 1P5M process using three metal layers, based on the structure described in the previous section. The computing of the composite field S-Box can be mathematically broken into operations in $GF(2)$ of the bitwise operations XOR and AND. However, in order to reduce the area of our implementation, we consider other logical operations and implement the logic optimizations for the S-Box. Since logic styles have a good power and area efficiency potential in the full-custom design, it is advantageous to choose the logic style for the targeted applications.

Logic optimization

For standard cell library considered, the NAND gate is smaller than the AND gate. The logic formulas $[ab \oplus cd]$ is equivalent to $[\overline{ab} \oplus \overline{cd}]$, the fact that AND output bits combined by pairs in a following XOR of the $GF(((2^2)^2)^2)$ inversion can be replaced by NAND gates can result in a slight size saving. Generally, the XOR gate has the same size as XNOR gate, and using the XNOR to replace the XOR does not increase the area. The logic formula $[a \oplus \overline{b}]$ is equivalent to $[a \odot b]$, then it is useful in the affine transformation of the S-Box, where the addition of the constant {0x63} means applying a NOT to several output bits. It is also valuable for the general multiplication in $GF((2^2)^2)$ and the $GF((2^2)^2)$ inversion, where all the AND operations are replaced by NAND gates.

Then, the functionality of the S-Box can be implemented by 2-1 multiplexers denoted MUX-, NAND-, XOR- and XNOR-gates. Table 1 lists the gates distribution of all blocks. It is noted that T-block denoted in Table 1 consists of two $GF((2^2)^2)$ squarings, one constant $\{\lambda\}$ multiplication and one $GF((2^2)^2)$ addition.

Table 1 Gates distribution of the S-Box

Block	Gate			
	XOR	XNOR	NAND	MUX
aff_trans	12	4	–	–
aff_trans^{-1}	10	2	–	–
map	15	–	–	–
map^{-1}	13	–	–	–
T-block	10	–	–	–
$GF((2^2)^2)$ multiplication	17	1	12	–
$GF((2^2)^2)$ inversion	9	6	9	–
$GF((2^2)^2)$ addition	4	–	–	–
Selector	–	–	–	8

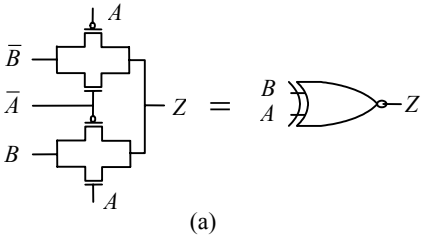
PTG-based circuit design

Most functionality of the S-Box on $GF(((2^2)^2)^2)$ can be implemented with XOR-gates, therefore, it is possible to reduce the total power of S-Box by using a low-power logic style to implement XOR-gates. In the full-custom S-Box circuit design, we use the pass transistor logic to design XOR-gates.

The basic difference of pass transistor logic (PTL) compared to the CMOS logic is that the source side of the logic transistor networks is connected to some input signals instead of the power lines. The advantage is that one p ass transistor network (either NMOS or PMOS) is sufficient for performing the logic operation, which results in a smaller number of transistors and smaller input loads. So PTL is a promising alternative to conventional CMOS for low-power high-performance fields due to the decreased node capacitance and reduced transistor count it offers.

Suntiamorntut (2005) analyzed the performance of some pass transistor logic styles such as SRPL (swing restored pass transistor logic), PPL (push-pull pass transistor logic), SPL (single-ended pass transistor logic) and PTG. From the energy and EDP (energy-delay product) results, PTG-based XOR offers the best energy performance and occupies less than half the area of CMOS. Moreover, PTG-based gates have NMOS and PMOS pass transistors. For any input combination there are always two current paths driving the outputs, which accelerates the charge/discharge process.

An example of the effective use of PTG is the popular XNOR circuit shown in Fig.2. In this PTG-based XNOR, input B is passed to the output when input A is high. Otherwise, $\overline{B}$ is passed to the output. The layout of the PTG-based XNOR gate is also shown in Fig.2, its silicon area is 6.0×5.5 μm^2 in 0.25 μm technology. It is noted that PTG-based XOR shown in Fig.3 can be realized in a similar way as the presented XNOR circuit. Moreover, the XNOR circuits in Fig.2 can also be viewed as different implementations of the 2-1 multiplexer denoted MUX in Fig.3. In our implementation, we select the above-mentioned three PTG-based gates for our full-custom circuit design.



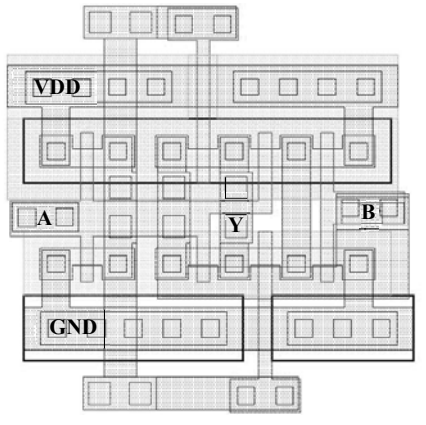


Fig.2 Circuit diagram (a) and layout (b) of PTG-based XNOR

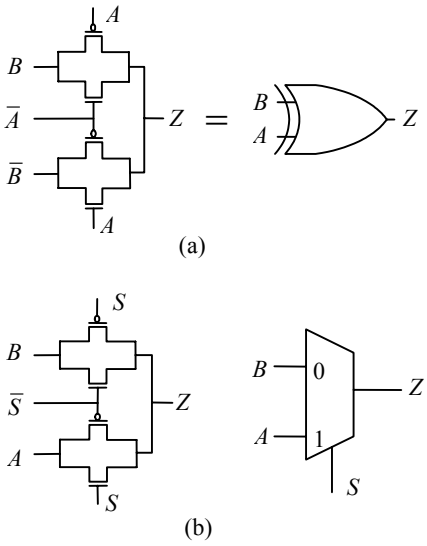


Fig.3 Circuit diagram of PTG-based XOR (a) and PTG-based MUX (b)

SIMULATION AND RESULTS

As the power consumption is strongly data dependent, datasets from real applications display correlations between successive values, which can strongly affect power consumption due to reduced number of changing bits, and can also have sections of low level signals which exhibit frequent signal changes, possibly increasing power consumption. The extracted SPICE netlists of different designs are imported into Synopsys VCS/Nanosim using 0.25 μm CMOS technology operating with 1 ps resolution at 2.5 V and 25 °C. The input sequence of 1000 random datum, at the rate of one byte per 100 ns, is used to activate the tested circuits. The average power dissipation and the worst case delay are used to calculate the EDP and PAP (power-area product). The parameter of PAP is particularly relevant for applications which require both small silicon area and low power consumption. The EDP is used to valuate the energy efficiency of the circuit and the EDP value of differentials is important in the resistance against differential cryptanalysis (Daemen and Rijmen, 2006). For comparison, the same power simulations have also been conducted on the solutions presented in (Satoh *et al*., 2001; Morioka and Satoh, 2002) based on standard 0.25 μm CMOS cell library.

The testing results are presented in Table 2. It is clear that our design has the best PAP and better EDP

although it has longer delay time. Moreover, our design consumes less power than PPRM, where the signal arrival time of gates is as close as possible if the depths of the gates from the primary inputs are the same. Therefore, two delay chains matching the timing of the inversion block are inserted between Stage 1 and Stage 3 of the S-Box. However, since the parasitic effects introduced by interconnecting wires start to dominate the speed of the CMOS circuit, with the development of deep submicron semiconductor technologies, it is difficult to match these timing delays.

Table 2 Performance comparisons of the three S-Boxes

Parameters		S-Boxes		
		Satoh *et al.* (2001)	PPRM	Ours
Area (μm^2)		8150	15282	8560
Delay (ns)		7.0	5.0	7.0
Average-power at 10 MHz (μW)	S-Box	416	232	122
	$S\text{-}Box^{-1}$	433	258	134
EDP (pJ·ns)	S-Box	20.4	5.8	6.0
	$S\text{-}Box^{-1}$	21.2	6.5	6.6
PAP ($W\cdot\mu m^2$)	S-Box	3.39	3.55	1.04
	$S\text{-}Box^{-1}$	3.53	3.94	1.15
EDP comparison	S-Box	0	−72%	−71%
	$S\text{-}Box^{-1}$	0	−69%	−69%
PAP comparison	S-Box	0	+5%	−69%
	$S\text{-}Box^{-1}$	0	+12%	−67%

The lowest possible voltage consistent with the desired performance is normally applied because the power consumption is proportional to the square of the supply voltage. Seven lower levels of voltage below the regular supply voltage have also been evaluated for the EDP and PAP for three S-Boxes (ours, Satoh's, and PPRM). The analysis used the same input sequence of 100 random data. The variations of power consumption of the tested S-Boxes versus voltage are depicted in Fig.4a. Our S-Box consumes the lowest power and its power consumption is reduced by a factor 18 (from about 123.3 μW at 10 MHz/2.5 V to about 6.5 μW at 10 MHz/0.8 V). Fig.4b shows the operating time versus voltage. According to Fig.4b, the lower the voltage is, the longer is the operating time. For our design, when the circuit is supplied 0.8 V, the operating time is multiplied by 10 (from about 7 ns at 2.5 V to about 78 ns at 0.8 V). Figs.4c and 4d present the EDP and PAP versus voltage, respectively. These figures show that the presented S-Box exhibits the best low-voltage property. Therefore, the presented S-Box is the most promising approach for embedded systems.

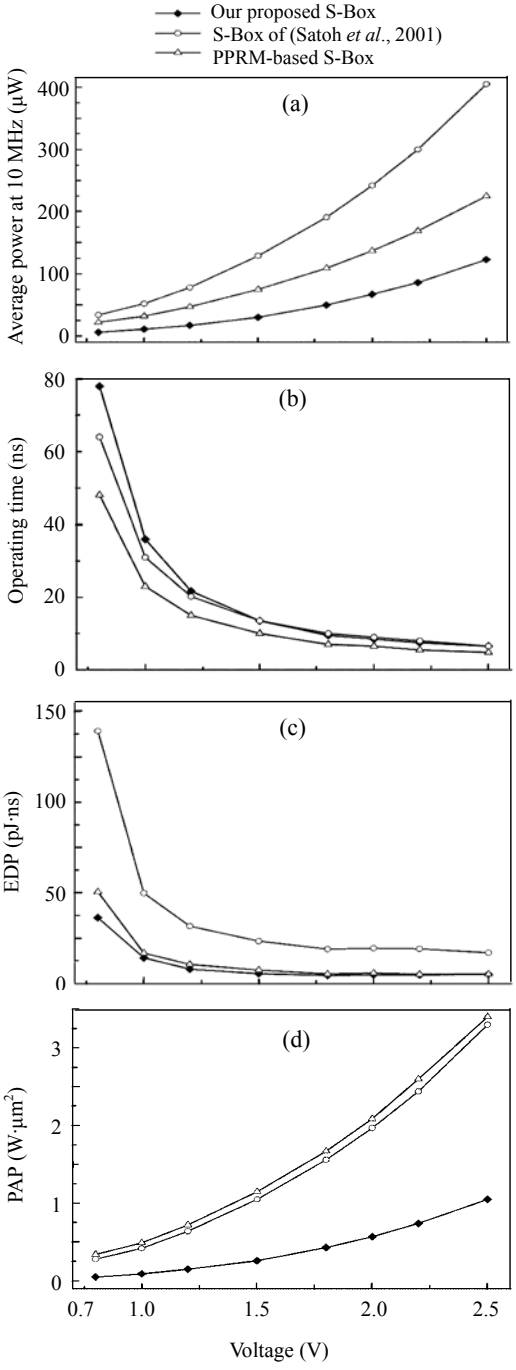


Fig.4 The related parameters versus voltage. (a) Average power at 10 MHz; (b) Operating time; (c) EDP; (d) PAP

CONCLUSION

This paper presents a full-custom hardware implementation of the S-Box. It is based on finite field arithmetic and pass transmission gate (PTG). The proposed S-Box is very compact and has low power dissipation. We optimized the S-Box architecture of (Satoh *et al*., 2001) by using a PPRM-based architecture to design the inversion circuit, which results in the reduction of the power consumption. In the power simulation using HSPICE in a 0.25 μm technology, we compared the performance of the designs in terms of PAP and EDP with the Satoh S-Box and PPRM-based S-Box. The results showed that our design is the best choice for applications requiring both small silicon area and low-power dissipation, such as RFID tags and sensor nodes chip.

References

Bertoni, G., Macchetti, M., Negri, L., Fragneto, P., 2004. Power-efficient ASIC Synthesis of Cryptographic Sboxes. Proc. GLSVLSI, p.277-281. [doi:10.1145/988952.989019]

Canright, D., 2005. A very compact S-Box for AES. *LNCS*, **3659**:441-455. [doi:10.1007/11545262_32]

Daemen, J., Rijmen, V., 2006. Understanding two-round differentials in AES. *LNCS*, **4116**:78-94. [doi:10.1007/11832072_6]

Kuorilehto, M., Hannikainen, M., Hamalainen, T.D., 2005. A survey of application in wireless sensor networks. *EURASIP J. Wirel. Commun. Networking*, (5):774-788. [doi:10.1155/WCN.2005.774]

Macchetti, M., Bertoni, G., 2002. Hardware implementation of the Rijndael S-BOX: a case study. *ST J. Syst. Res.*, p.84-91.

Mentens, N., Batina, L., Preneel, B., Verbauwhede, I., 2005. A systematic evaluation of compact hardware implementations for the Rijndael S-Box. *LNCS*, **3376**:323-333. [doi:10.1007/b105222]

Morioka, S., Satoh, A., 2002. An optimized S-box circuit architecture for low power AES design. *LNCS*, **2523**: 172-186.

Rudra, A., Dubey, P.K., Julta, C.S., Kumar, V., Rao, J.R., Rohatgi, P., 2001. Efficient Rijndael encryption implementation with composite field arithmetic. *LNCS*, **2162**: 171-184.

Sasao, T., 1993. AND-EXOR Expressions and Their Optimization. Logic Synthesis and Optimization. Kluwer Academic Publishers, p.287-312.

Satoh, A., Morioka, S., Takano, K., Munetoh, S., 2001. A compact Rijndael hardware architecture with S-Box optimization. *LNCS*, **2248**:239-254.

Suntiamorntut, W., 2005. Energy Efficient Functional Unit for a Parallel Asynchronous DSP. Ph.D Thesis, The University of Manchester, Manchester, UK.

Tillich, S., Feldhofer, M., Großschädl, J., 2006. Area, delay, and power characteristics of standard-cell implementations of the AES S-Box. *LNCS*, **4017**:457-466. [doi:10.1007/11796435_46]

Wolkerstorfer, J., Oswald, E., Lamberger, M., 2002. An ASIC implementation of the AES S-Boxes. *LNCS*, **2271**:67-78.