ELectronics EXpress

LETTER

IEICE Electronics Express, Vol.14, No.11, 1–6

A new compact hardware architecture of S-Box for block ciphers AES and SM4

Yaoping Liu[1a)], **Ning Wu**[1b)], **Xiaoqiang Zhang**[2], **and Fang Zhou**[1]

[1] *College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China*

[2] *College of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000, China*

a) *liuyaoping91@163.com*

b) *wunee@nuaa.edu.cn*

Abstract: In this paper, a new compact implementation of S-Box based on composite field arithmetic (CFA) is proposed for block ciphers AES and SM4. Firstly, using CFA technology, the multiplicative inverse (MI) over GF(2^8) is mapped into GF((2^4)^2) and the new architecture of S-Box is designed. Secondly, the MI over GF(2^4) is optimized by Genetic algorithm (GA), and the multiplication over GF(2^4) and the constant matrix multiplications are optimized by delay-aware common sub-expression elimination (DACSE) algorithm. Finally, compared with the direct implementation, the area reduction of MI over GF((2^4)^2) and the new S-Box are up to 49.29% and 43.80%, severally. In 180 nm 1.8 V COMS technology, compared to the synthesized results of AES S-Box and SM4 S-Box, the area and power consumption of the new S-Box are reduced by 24.76% and 38.54%, respectively.

Keywords: advanced encryption standard (AES), SM4, S-Box, composite field arithmetic (CFA)

Classification: Integrated circuits

References

[1] L. Fu, *et al.*: "A low-cost UHF RFID tag chip with AES cryptography engine," Secur. Commun. Netw. **7** (2014) 365 (DOI: 10.1002/sec.723).

[2] C. Wang, *et al.*: "Low complexity implementation of block cipher SM4 algorithm," Comput. Eng. **39** (2013) 177 (DOI: 10.3969/j.issn.1000-3428.2013.07.040).

[3] W. Shan, *et al.*: "VLSI design of a reconfigurable S-box based on memory sharing method," IEICE Electron. Express **11** (2014) 20130872 (DOI: 10.1587/elex.10.20130872).

[4] J. Yang, *et al.*: "An area-efficient design of reconfigurable S-box for parallel implementation of block ciphers," IEICE Electron. Express **13** (2016) 20160138 (DOI: 10.1587/elex.13.20160138).

[5] Yasir, *et al.*: "Highly optimised reconfigurable hardware architecture of 64 bit block ciphers MISTY1 and KASUMI," IET (2016).

[6] Y. Chen, *et al.*: "Energy-efficient and security-optimized AES hardware design

DOI: 10.1587/elex.14.20170358
Received April 10, 2017
Accepted April 27, 2017
Publicized May 15, 2017
Copyedited June 10, 2017

for ubiquitous computing," J. Syst. Eng. Electron. **19** (2008) 652 (DOI: 10.1016/S1004-4132(08)60134-6).
[7] M. M. Wong, *et al.*: "Construction of optimum composite field architecture for compact high-throughput AES S-boxes," IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **20** (2012) 1151 (DOI: 10.1109/TVLSI.2011.2141693).
[8] D. Canright: "A Very Compact S-Box for AES," *7th International Workshop on CHES*, LNCS vol. 3659 (Springer-Verlag, Heidelberg, 2005) 441.
[9] Y. Xu, *et al.*: "A new algorithm of S-box for hardware implementation of SMS4," J. Univ. Sci. Technol. China **39** (2009) 1164.
[10] H. Liang, *et al.*: "Design and implementation of SM4 block cipher based on composite field," Microelectron. Comput. **32** (2015) 16.
[11] X. Zhang, *et al.*: "An optimized delay-aware common subexpression elimination algorithm for hardware implementation of binary-field linear transform," IEICE Electron. Express **11** (2014) 20140934 (DOI: 10.1587/elex.11.20140934).
[12] Z. Bao and T. Watanabe: "A novel genetic algorithm with cell crossover for circuit design optimization," IEEE International Symposium on Circuits and Systems, 2009. ISCAS 2009 (2009) 2982 (DOI: 10.1109/ISCAS.2009.5118429).

1 Introduction

The Advanced Encryption Standard (AES) is the latest international block cipher standard, which is widely used in various fields of information security [1]. SM4 is the first block cipher algorithm released by the Chinese government, and mainly used to protect the security of wireless local area network (WLAN) products [2]. Nowadays, in order to accommodate different applications, most of the cipher chips produced in China integrate AES and SM4 IP cores, but they are independent, so those chips cover a larger area and are not conducive to be used in the wireless sensor network and radio frequency identification and other resources limited applications. Therefore, it is important to design a new AES/SM4 IP core with small area and low power consumption for cipher chips by sharing the same computing unit in the AES and SM4 encryption circuits.

S-Box is the unique nonlinear component and the main computing unit of AES and SM4 algorithm, which occupies most of the area and power consumption of the circuits. And S-Box as the similar computing unit in the AES and SM4 encryption circuits, focusing on its design is the key for the implementation of new AES/SM4 encryption circuit. In [3, 4], the reconfigurable S-Box based on look up table (LUT) with memory-sharing are designed, which use a sharing memory to achieve different S-Box operations for different block cipher algorithms and have the advantage of high flexibility. However, these implementations not only cover a huge area but also reduce the circuit performance.

In order to reduce the hardware complexity, one of the effective implementations of the new S-Box is to reuse the same computing unit [5]. AES S-Box is defined as the multiplicative inverse (MI) over GF(2^8) followed by an affine transformation, and SM4 S-Box has a similar design to AES S-Box. The MIs over GF(2^8) are the similar computing unit and the key component of the AES/SM4

DOI: 10.1587/elex.14.20170358
Received April 10, 2017
Accepted April 27, 2017
Publicized May 15, 2017
Copyedited June 10, 2017

S-Boxes. So the implementation of new AES/SM4 S-Box by multiplexing the MIs over GF(2^8) will greatly reduce the hardware resources. But the MIs in these two ciphers are defined on different GF(2^8), respectively. In this paper, the MIs over GF(2^8) are mapped into the same composite filed GF((2^4)^2), and a new S-Box is constructed through multiplexing the MI over GF((2^4)^2). Among different implementations of S-Box proposed in previous works, S-Box based on composite field arithmetic (CFA) covers the smallest area [6]. Therefore, it will greatly reduce the area of the new AES/SM4 S-Box by mapping the MIs over GF(2^8) into the same composite filed GF((2^4)^2) and reusing the MI over GF((2^4)^2).

The main works of this paper are as follows: Firstly, the new architecture of the CFA-Based AES/SM4 S-Box is proposed. Secondly, the MI over GF(2^8) is decomposed into GF((2^4)^2), and then the MI over GF((2^4)^2) is optimized by Genetic algorithm (GA) [12] and delay-aware common sub-expression elimination (DACSE) algorithm [11]. Finally, compared with independent AES S-Box and SM4 S-Box, the new S-Box has smaller area cost.

2 The new implementation of S-Box based on CFA

2.1 The new design of CFA-based S-Box

In CFA technology, the MI over GF(2^8) is decomposed into composite field GF((2^4)^2) using the following irreducible polynomials.

$$\begin{cases} GF((2^4)^2) : f_1(y) = y^2 + y + v \\ GF(2^4) : f_2(x) = x^4 + x^3 + x^2 + x + 1 \end{cases} \tag{1}$$

Where $v = \{0010\}_2$. The AES S-Box and SM4 S-Box based on CFA technique can be expressed as (2) and (3) respectively.

$$Z = M(\delta^{-1}(\delta X)^{-1}) + V \tag{2}$$

$$Y = A(T^{-1}(T(AX + C))^{-1}) + C \tag{3}$$

Where $\delta = [0xE7, 0xB6, 0x57, 0xB4, 0x64, 0x6C, 0xA0, 0x01]$ and $T = [0x68, 0x8F, 0xBF, 0x84, 0xF0, 0xF6, 0x4B, 0x01]$, δ and T are the isomorphic mapping matrix of AES S-Box and SM4 S-Box respectively. Generally for reducing the hardware resources, matrix M and matrix δ^{-1} are merged into a single matrix, i.e., $M_i = M \times \delta^{-1} = [0x5E, 0x05, 0x60, 0x52, 0x84, 0x9D, 0x36, 0x1F]$. In the same way, matrix $A_i = A \times T^{-1} = [0x0C, 0xD9, 0x78, 0xF3, 0x44, 0xB0, 0xC1, 0xCB]$.

According to (2) and (3), the new architecture of S-Box based on CFA is shown in Fig. 1. The MI over GF((2^4)^2) is shared between the two S-Boxes by using 2:1 selectors. When the select signal is 0, these blocks, which are the mapping matrix multiplication $\delta\times$, the combined matrix multiplication $M_i\times$, the addition $+V$ and the MI over GF((2^4)^2), are selected, and the circuit of AES S-Box is achieved. If the select signal is 1, the circuit of new S-Box is rearranged, the operations $T\times$, $A\times$, $A_i\times$, $+C$ and the MI over GF((2^4)^2) are functional and the functionality for SM4 S-Box is implemented.

2.2 The optimized implementation of new S-Box

2.2.1 The implementation of the MI over GF((2^4)^2)

Polynomial basis is used to represent field elements in each level composite field.

DOI: 10.1587/elex.14.20170358
Received April 10, 2017
Accepted April 27, 2017
Publicized May 15, 2017
Copyedited June 10, 2017

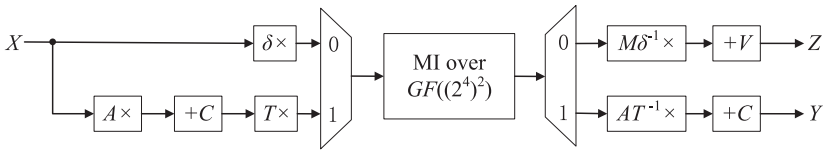

Fig. 1. The new architecture of S-Box using the CFA technique

Suppose A is an element over GF($(2^4)^2$), then it can be represented by polynomial basis as $A = A_hX + A_l$, where $\{A_h, A_l\} \in$ GF(2^4). The MI of A can be expressed as (4) by using the first irreducible polynomial in (1).

$$B = A^{-1} = (A_h{}^2 v + (A_h + A_l)A_l)^{-1}(A_h\gamma + (A_h + A_l)) \tag{4}$$

Where $B = B_hX + B_l$. According to (4), the MI over GF($(2^4)^2$) is completed by two additions, three multiplications, a square, a constant multiplication and a MI. All the operations are over GF(2^4). The addition over GF(2^4) can be implemented by bit-XOR operations. The square and constant multiplication over GF(2^4) are usually joint into a single block to reduce the number of gates.

Suppose a and b are elements over GF(2^4), then they can be represented as $a = a_3\omega_3 + a_2\omega_2 + a_1\omega + a_0, b = b_3\omega_3 + b_2\omega_2 + b_1\omega + b_0$, where $\{a_3, a_2, a_1, a_0, b_3, b_2, b_1, b_0\} \in$ GF(2). According to the second irreducible polynomial in (1), the multiplication $a \times b$ and the MI a^{-1} over GF(2^4) can be expressed as (5) and (6), respectively.

$$c = a \times b = \begin{cases} c_3 = (a_3b_1 + a_1b_3) + (a_3b_0 + a_0b_3) + (a_2b_1 + a_1b_2) + a_2b_2 \\ c_2 = (a_3b_1 + a_1b_3) + (a_2b_0 + a_0b_2) + a_2b_2 + a_1b_1 \\ c_1 = (a_3b_1 + a_1b_3) + (a_1b_0 + a_0b_1) + a_3b_3 + a_2b_2 \\ c_0 = (a_3b_2 + a_2b_3) + (a_3b_1 + a_1b_3) + a_2b_2 + a_0b_0 \end{cases} \tag{5}$$

$$f = a^{-1} = \begin{cases} f_3 = a_3a_2a_0 + a_3a_1a_0 + a_3a_1 + a_2a_0 + a_2 + a_1 \\ f_2 = a_3a_2a_0 + a_2a_1a_0 + a_2a_0 + a_1a_0 + a_3 + a_1 \\ f_1 = a_3a_2a_1 + a_3a_1a_0 + a_2a_1a_0 + a_3a_0 + a_2a_1 + a_2a_0 + a_1 \\ f_0 = a_3a_2a_1 + a_3a_2a_0 + a_3a_2 + a_2a_0 + a_1 + a_0 \end{cases} \tag{6}$$

Where $c = c_3\omega_3 + c_2\omega_2 + c_1\omega + c$, and $f = f_3\omega_3 + f_2\omega_2 + f_1\omega + f_0$. Substitute $v = (0010)_2$ into (5), we can know that the block $()^2 \times v$ does not consume hardware resources.

According to (5) and (6), there are many redundant gates in the direct implementations. For reducing the hardware complexity, based on GA [12] and DACSE algorithm [11], a joint optimization method is proposed to optimize the new S-Box based on CFA in this paper.

The multiplication over GF(2^4) is optimized by the DACSE algorithm, and the optimized result includes 15XORs and 16ANDs, which needs 69 equivalent gates, with a reduction of 31.34% in terms of the total area occupancy compared with the direct implementation.

GA is adopted to optimize the MI over GF(2^4), and the optimized circuit require 37.5 equivalent gates. Compared with the direct implementation, which needs 21 XORs and 27 ANDs, it gives 66(63.77%) gates reduction in total area cost.

DOI: 10.1587/elex.14.20170358
Received April 10, 2017
Accepted April 27, 2017
Publicized May 15, 2017
Copyedited June 10, 2017

2.2.2 The optimization of matrix multiplication

Using AES isomorphic mapping matrix $\delta\times$ as an example, multiplication of matrix δ is expressed as (7). The matrix multiplication $T\times$, $A\times$, $M_i\times$ and $A_i\times$ can be expressed as the same form.

$$Y=\delta X=\begin{bmatrix}1&1&0&1&0&0&1&0\\1&0&1&0&1&1&0&0\\1&1&0&1&1&1&1&0\\0&1&1&1&0&0&0&0\\0&0&0&0&0&1&0&0\\1&1&1&1&1&1&0&0\\1&1&1&0&0&0&0&0\\1&0&1&0&0&0&0&1\end{bmatrix}\begin{bmatrix}x_7\\x_6\\x_5\\x_4\\x_3\\x_2\\x_1\\x_0\end{bmatrix}=\begin{cases}y_7=x_7+x_6+x_4+x_1\\y_6=x_7+x_5+x_3+x_2\\y_5=x_7+x_6+x_4+x_3+x_2+x_1\\y_4=x_6+x_5+x_4\\y_3=x_2\\y_2=x_7+x_6+x_5+x_4+x_3+x_2\\y_1=x_7+x_6+x_5\\y_0=x_7+x_5+x_0\end{cases}\tag{7}$$

The matrix multiplications optimized by DACSE algorithm needs 255gates with a reduction of 36.57% compared to the direct implementation, as shown in Table I.

2.3 Hardware performances of the new S-Box

The type and quantity of logic gates as well as the number of equivalent gates in the direct implementation and optimization in this paper are listed in Table I.

Table I. The area cost required by each part of the CFA-Based S-Box

Modules	Direct			Optimized by GA and DACSE						
	XOR	AND	Gates	NAND	NOR	AND	OR	XOR	XNOR	Gates (Reduction)
MI Over GF($(2^4)^2$)	113	127	529.5	7	2	51	4	57	2	268.5 (49.29%)
$\delta\times$	22	—	66	—	—	—	—	11	—	33 (50%)
$M\delta^{-1}\times$	20	—	60	—	—	—	—	13	—	39 (35%)
$A\times$	32	—	96	—	—	—	—	21	—	63 (34.38%)
$T\times$	24	—	72	—	—	—	—	13	—	39 (45.83%)
$AT^{-1}\times$	22	—	66	—	—	—	—	13	—	39 (40.91%)
S-Box	247	127	931.5	7	2	51	4	142	2	523.5 (43.80%)

As shown in Table I, the optimized S-Box needs 523.5 gates, and the area reduction is up to 408 (43.80%) gates compared to the direct implementation, which requires 931.5 equivalent gates.

3 Comparisons and results

In Table II, the new S-Box proposed in this paper is compared with the implementations in previous works. In [7], the MI over GF(2^8) is mapped into GF($(2^4)^2$), and CSE algorithm is used to optimize the MI over GF(2^4). In [8, 9, 10], the MI over GF(2^8) is decomposed into GF($(((2^2)^2)^2$), and the MI and multiplication over GF($(2^2)^2$) and matrix multiplication are optimized by CSE algorithm.

As shown in Table II, the implementations of AES S-Box and SM4 S-Box proposed in [8] and [9] has the smallest area respectively. And the total number of

DOI: 10.1587/elex.14.20170358
Received April 10, 2017
Accepted April 27, 2017
Publicized May 15, 2017
Copyedited June 10, 2017

Table II. The comparisons of the whole of implementations of S-Box

Works	Implementation	Gates
[7]	AES S-Box	342
[8]	AES S-Box	327
[9]	SM4 S-Box	402
[10]	SM4 S-Box	474
Ours	The new AES/SM4 S-Box	523.5

equivalent gates in the two S-Boxes is 729 gates. However, the new AES/SM4 S-Box implemented in this paper needs 523.5 gates with a reduction of 28.19% in terms of the total area occupancy. In other words, the optimized implementation of the new S-Box proposed in this paper has the minimal hardware requirement.

In the SMIC 0.18 µm 1.8 V cell library, the implementations of AES S-Box, SM4 S-Box and the new AES/SM4 S-Box are synthesized. The synthesized results are listed in Table III.

Table III. The synthesized results of the implementations

Implementations	Area (μm^2)	Delay (ns)	Power (µW)
AES S-Box	2844.0720	7.64	75.65
SM4 S-Box	3496.0465	8.60	110.58
The new AES/SM4 S-Box	4770.0577	9.03	114.45

As shown in Table III, at 7.64 ns and 8.60 ns delay target, the design of AES S-Box and SM4 S-Box achieve the minimum area and power, respectively. The total area and power of the two S-Boxes are severally 6340.1185 μm^2 and 186.23 µW. At 9.03 ns delay target, the implementation of the new AES/SM4 S-Box covers an area of 4770.0577 μm^2 and the power consumption is 114.45 µW, whose area and power consumption has a better performance with 24.76% and 38.54% less than the independent designs of AES S-Box and SM4 S-Box.

4 Conclusions

S-Box as the similar computing unit in the AES and SM4 encryption circuits, studying on its design can effectively reduce the hardware complexity. Therefore, a new compact implementation of CFA-Based AES/SM4 S-Box is proposed in this paper. Compared to the implementations in [8] and [9], which need 729 gates, the new AES/SM4 S-Box includes 523.5 gates with a reduction of 28.19%. Consequently, the new AES/SM4 S-Box proposed in this paper has a better performance in area occupancy.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61376025), and the Natural Science Foundation of Jiangsu Province (No. BK20160806).

DOI: 10.1587/elex.14.20170358
Received April 10, 2017
Accepted April 27, 2017
Publicized May 15, 2017
Copyedited June 10, 2017