An Area Optimized Implementation of AES S-Box Based on Composite Field and Evolutionary Algorithm

Yaoping Liu, Ning Wu, Xiaoqiang Zhang, LilingDong, and Lidong Lan

***Abstract*—In this paper, in order to reduce the hardware complexity, the S-Box based on composite field arithmetic (CFA) technology is optimized by using Genetic Algorithm (GA) and Cartesian Genetic Programming (CGP) model. Firstly, the multiplicative inverse (MI) over GF(2^8) is mapped into composite field GF((2^4)^2) by using the CFA technique. Secondly, the compact circuit of MI over GF(2^4) is selected from 100 evolved circuits, and same design method is applied to the compact circuit of multiplication over GF(2^2). Compared with the direct implementations, the areas of optimized circuits of MI over GF(2^4) and multiplication over GF((2^2)^2) are reduced by 66% and 57.69%, respectively. Moreover, the area reductions for MI over GF(2^8) and the whole of S-Box are up to 59.23% and 56.14%, respectively.**

***Index Terms*—Advanced Encryption Standard (AES), composite field arithmetic (CFA), S-Box, Evolutionary Algorithm (EA)**

I. Introduction

THE Advanced Encryption Standard (AES) is the smart-of-the-art symmetric block data encryption algorithm which was established by the National Institute of Standards and Technology (NIST) to replace the Data Encryption Standard (DES) in 2001. The AES algorithm consists of four transformations, namely SubBytes (SB), ShiftRows (SR), MixColumns (MC) and AddRoundKey (ARK). Nowadays, it has been widely used in various fields of information security, such as wireless local area network (WLAN), wireless personal network (WPAN), wireless sensor network (WSN) and the smart card system[1,2]. With the wide application of AES algorithm, it is very necessary to design and implement compact circuit of AES. However, the implementation of S-Box is the most expensive part in terms of the required hardware. Therefore, the design and implementation of compact S-Box is the key component of the AES algorithm [3] [4].

AES S-box is defined as a multiplicative inverse (MI) over the Galois field GF(2^8) followed by an affine transformation. The affine transformation is relatively simple to achieve, so the difficulty in design of AES S-Box is how to implement MI over GF(2^8) in the specific hardware implementation. Different circuit architectures have been proposed by many papers for design and implementation of AES S-Box, such as CFA technology, look up table (LUT), positive polarity reed-muller (PPRM), decoder-switch-encoder (DSE), sum of products (SOP), binary decision diagram (BDD) and twisted-BDD. Among these implementations, S-Box implemented with CFA has the smallest area [5] [6]. Therefore, in order to reduce the hardware complexity, the MI over GF(2^8) can be decomposed into composite filed GF((2^4)^2) or GF(((2^2)^2)^2) by using the CFA technology.

Circuit optimization method is adopted to design a compact S-Box because there are still many redundant gates in the implementation of CFA S-Box. Different common sub-expression elimination (CSE) methods have been proposed by many papers to optimize the circuit of CFA S-Box. In [3] [4], the MI over GF(2^8) is decomposed into composite filed GF((2^4)^2). According to different irreducible polynomials with normal basis representations, the MI over GF(2^4) is expressed by logic expressions directly and optimized by CSE algorithm, which is an important part in MI over GF((2^4)^2). In [7], the MI and multiplication over GF(2^4) are decomposed into GF((2^2)^2) and optimized by sharing common sub-expressions (CSs), and matrix multiplication is optimized by CSE algorithm. The implementation of S-Box proposed in [7] has the smallest area [4].

Evolutionary algorithm is an intelligent optimization algorithm based on population search. And people pay more and more attentions to it in recent years. Using EA to design circuit can reduce the resources of gates and the areas of circuits effectively and can also improve the utilization efficiency of the circuit. What is more, it can find novel circuit structure which is difficult for people to think of. Therefore, in this paper, Genetic Algorithm (GA) is adopted to further optimize the circuit of CFA S-Box.

The main works of this paper are as follows: Firstly, using CFA technology, the MI over GF(2^8) is decomposed into composite filed GF((2^4)^2), and the multiplication over GF(2^4)

Manuscript received July 10, 2015. This work was supported by the National Natural Science Foundation of China (No. 61376025, No. 61106018), the Industry-academic Joint Technological Innovations Fund Project of Jiangsu (No. BY2013003-11), the Funding of Jiangsu Innovation Program for Graduate Education (No. KYLX_0273), and the Fundamental Research Funds for the Central Universities.

Yaoping Liu is with College of Electrical and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing 210016, China (e-mail: liuyaoping91@163.com).

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

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

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).

Lidong Lan is with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing 210016, China (e-mail: lanlidongdt@126.com).

is further mapped into composite filed GF((2^2)^2). Secondly, the MI over GF(2^4) and the multiplication over GF(2^2) are optimized with by GA respectively. Finally, the implementation of CFA S-Box optimized by GA has smaller area cost than the one proposed in [7] which has the minimal area cost [4].

II. The Implementation of CFA S-Box Optimized by GA

A. The design process of AES S-Box

In this paper, in order to reduce the hardware complexity, GA is adopted to optimize the circuit of CFA S-Box because the circuit designed by EA has small area cost. Fig. 1 shows the whole design process of AES S-Box.

Firstly, the MI over GF(2^8) is decomposed into composite field GF((2^4)^2). Secondly, the MI over GF(2^4) is optimized by GA, and at the same time the multiplication over GF(2^4) is further mapped into GF((2^2)^2), and then the multiplication over GF(2^2) is optimized by GA. Thirdly, the multiplications over GF(2^4) in MI over GF((2^4)^2) are optimized by CSE algorithm. Finally, the MI over GF((2^4)^2) is mapped into GF(2^8) to implement the circuit of S-Box.

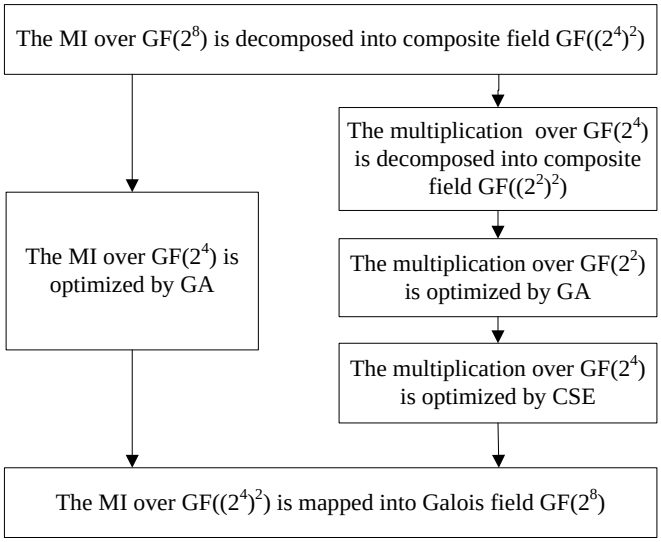

Fig. 1. The design process of AES S-Box.

B. The implementation of S-Box based on CFA technology

AES S-Box is defined as the MI over the finite field GF(2^8) followed by an affine transformation. The MI over GF(2^8) can be mapped into composite field GF(((2^2)^2)^2) to reduce the hardware complexity by adopting CFA technology, since direct calculation of the MI over GF(2^8) is a complicated and difficult task. In this paper, the CFA technology proposed in [7] is adopted to illustrate the optimization of CFA S-Box by GA.

In CFA technology, an isomorphic mapping matrix is demanded to map the input vector from the finite field GF(2^8) to the composite field GF(((2^2)^2)^2), and its inverse matrix is required to revert the computing results to GF(2^8). So the S-Box based on CFA technique can be expressed as:

$$S(X) = M(\mathrm{T}^{-1}(\mathrm{T}X)^{-1}) + V \tag{1}$$

where T is the isomorphic mapping matrix and T^{-1} is inverse matrix of T. Generally, matrix T^{-1} and matrix M are merged into a single matrix to reduce the hardware resources. The architecture of S-Box using the CFA technique is shown in Fig. 2.

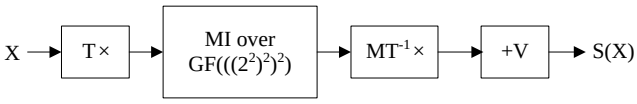

Fig.2. Architecture of S-Box using the CFA technique.

In CFA technology, the MI over GF(2^8) is built iteratively from GF(2) by using the following irreducible polynomials:

$$\begin{cases} GF((2^4)^2): f_1(z) = z^2 + z + \gamma \\ GF((2^2)^2): f_2(y) = y^2 + y + \lambda \\ GF((2)^2): f_3(w) = w^2 + w + 1 \end{cases} \tag{2}$$

In [7], it indicates that the circuit constructed under coefficients {$\gamma=(0001)_2$, $\lambda=(10)_2$} needs the least number of gates. So coefficients {$\gamma=(0001)_2$, $\lambda=(10)_2$} are also used in this paper.

According to the first irreducible polynomial in (2), the MI over GF(2^8) is decomposed into GF((2^4)^2) as (3) [7]:

$$B(Z) = A^{-1}(Z) = ((A_h + A_l)^2\gamma + A_h A_l)^{-1} \times (A_l Z^{16} + A_h Z) \tag{3}$$

where A(Z) can be expressed as $A(Z)=A_hZ^{16}+ A_lZ$, {A_h, A_l } $\in$ GF(2^4). B(Z) can be represented in the same way. The architecture of MI over GF((2^4)^2) is shown in Fig. 3.

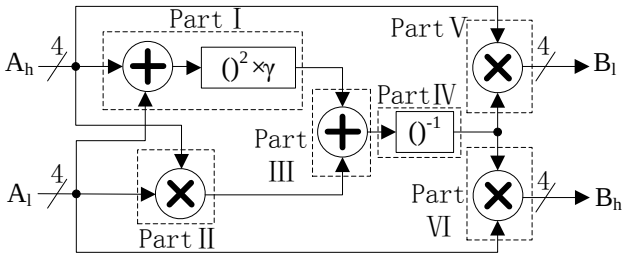

Fig. 3. The architecture of the MI over GF((2^4)^2).

As shown in Fig. 3, the MI over GF((2^4)^2) includes two additions, a MI, a square, a constant multiplication and three multiplications. All the operations are over GF(2^4). The addition over GF(2^k) is defined as bitwise XOR operations. The square and constant multiplication over GF(2^4) can be deduced from multiplication over GF(2^4), and they are usually joint into a single block to reduce the number of gates. The MI and multiplication over GF(2^4) are further mapped into GF(2^2)^2) by using the second irreducible polynomial in (2). They are expressed as (4) and (5) respectively:

$$E(Y) = C^{-1}(Y) = ((C_h + C_l)^2\lambda + C_h C_l)^{-1} \times (C_l Y^4 + C_h Y) \tag{4}$$

$$\begin{aligned} F(Y) = C(Y)D(Y) = &\left[C_h D_h + (C_l + C_h)(D_l + D_h)\lambda\right]Y^4 \\ &+ \left[C_l D_l + (C_l + C_h)(D_l + D_h)\lambda\right]Y \end{aligned} \tag{5}$$

where C(Y) can be expressed as $C(Y)=C_hY^4+ C_lY$, {C_h, C_l} $\in$ GF(2^2). D(Y), E(Y) and F(Y) can be represented in the same way. By using the third irreducible polynomial in (2), the MI and multiplication over GF(2^2) are further

decomposed into GF((2)^2) as (6) and (7) respectively:

$$H(W) = G^{-1}(W) = (g_0 W^2 + g_1 W) \quad (6)$$

$$L(W) = G(W)K(W) = (g_0k_0 + g_1k_0 + g_0k_1)W^2 + (g_1k_0 + g_0k_1 + g_1k_1)W \quad (7)$$

where G(W)=g_1W^2+g_0W, { g_1 ,g_0}$\in$GF(2), K(W), H(W) and L(W) are expressed in the same way. According to (4) to (7), the logic expressions of each part in Fig. 3 can be derived.

C. Genetic Algorithm and Evolvable Hardware

GA is an adaptive optimization algorithm of probability search which simulates heredity and evolution of biology in environment, and uses some mechanisms inspired by biological evolution: selection, crossover and mutation [9] [10]. It is usually used to search exact or approximate solutions to optimize and solve problems.

GA will be constantly for evolutionary computation until find the best design. After several iterations, under the survival of the fittest algorithm, the bad design will be abandoned on the basis of competitive selection strategy. Therefore, the number of excellent individuals will increase continually and the best design will be find finally.

In this paper, the circuit model is based on Cartesian Genetic Programming (CGP) [11]. Each candidate circuit is encoded in the chromosome. The chromosome is a string of integers where each three continuous genes embody a gate. Each triplet in the chromosome encodes the two inputs and the type of a gate respectively. So each chromosome represents a candidate circuit topology. The type, function and the quantity of transistors of logic gates [8] and their corresponding numbers are listed in TABLE I.

TABLE I
THE TYPE, FUNCTION AND THE NUMBER OF TRANSISTORS OF LOGIC GATES AND THEIR CORRESPONDING NUMBERS

Number	Type	Function	Transistors
0	AND	A&&B	6
1	OR	A‖B	6
2	XNOR	A⊙B	14
3	NOT1	!A	2
4	NOT2	!B	2
5	NAND	! (A&&B)	4
6	NOR	!(A‖B)	4
7	XOR	A⊕B	12

D. The optimization of MI over composite field GF((2^4)^2)

In this paper, the circuit of MI over composite field GF(2^4) which is based on CGP model, is optimized by GA. The basic parameters of GA are set as follows: the population size is 500, the size of initial population is 200, the crossover probability is 0.8, and the mutation probability is 0.03. The optimization of each part in Fig. 3 is in the following.

The optimization of MI over composite field GF(2^4)

According to the derivation in section B, the logic expressions of MI over GF(2^4) are represented as (8):

$$Q = P^{-1} = \begin{cases} q_3 = p_2p_1p_0 + p_3p_1 + p_2p_1 + p_1 + p_0 \\ q_2 = p_3p_1p_0 + p_3p_1 + p_2p_1 + p_2p_0 + p_0 \\ q_1 = p_3p_2p_0 + p_3p_1 + p_3p_0 + p_3 + p_2 \\ q_0 = p_3p_2p_1 + p_3p_1 + p_3p_0 + p_2p_0 + p_2 \end{cases} \quad (8)$$

In this paper, it is optimized by GA on the basis of logical relations shown in (8). The compact circuit of the 100 evolutionary circuits is shown in Fig. 4.

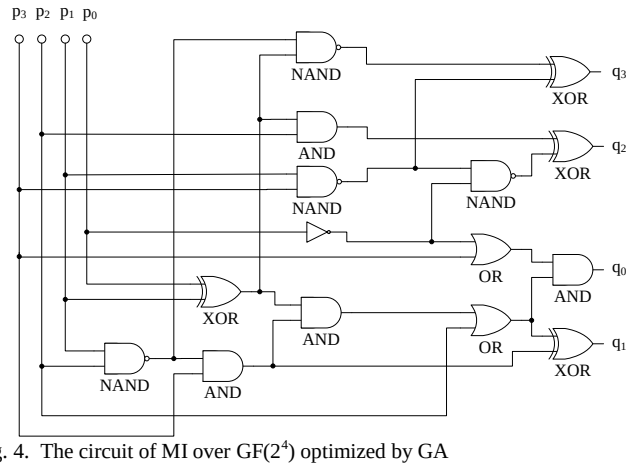

Fig. 4. The circuit of MI over GF(2^4) optimized by GA

The optimization of multiplication over composite field GF(2^4)

The multiplication over GF(2^4) is mapped into composite field GF((2^2)^2) in this paper. According to (7), the direct implementation of multiplication over GF(2^2) needs three XORs and four ANDs. The circuit optimized by GA includes three XORs and four NANDs, which requires 52 transistors, with a reduction of 13.33% in terms of the total area occupancy. The circuit of multiplication over GF(2^2) optimized by GA is shown in Fig. 5.

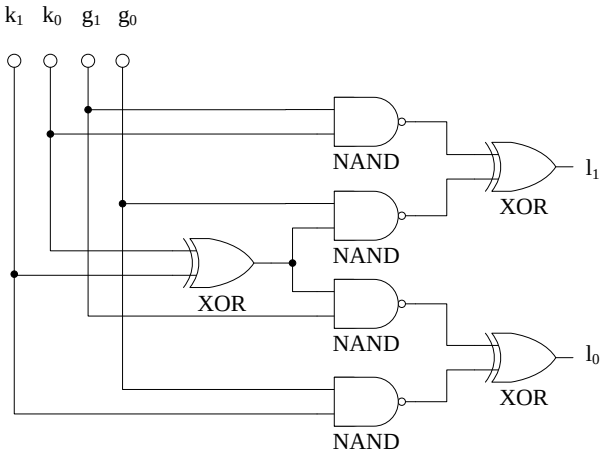

Fig. 5. The circuit of multiplication over GF(2^2) optimized by GA

According to (6), it can be get that:

$$G(W) \times \lambda = (g_0W^2 + (g_0 + g_1)W) \quad (9)$$

where $\lambda=(10)_2$. The block () $\times\lambda$ in (7) requires one XOR gates by using the computation in (9)

So the optimized circuit of multiplication over GF(2^4)

demands 18 XORs and 12 NANDs, which contains 264 transistors. Compared to the quantity of transistors in direct implementation, which requires 44 XORs and 16 ANDs, it gives 360(57.69%) transistors reduction in total area cost.

Hardware performances of optimized implementations

Substitute (7), (9), and $\gamma=(0001)_2$ into (5) to obtain that:

$$S = C^2 \times \gamma = \begin{cases} s_3 = c_2 + c_0 \\ s_2 = c_3 + c_3 \\ s_1 = c_1 + c_0 \\ s_0 = c_0 \end{cases} \quad (10)$$

where $c=(c_3c_2c_1c_0) \in GF(2^4)$, $\{c_3,c_2,c_1,c_0\} \in GF(2)$. According to (10), the block $()^2\times\gamma$ in Fig. 3 needs three XORs.

Six XORs are eliminated by sharing common sub-expressions among Part II, Part V and Part VI in Fig. 3. Therefore, The three multiplications over $GF(2^4)$ requires 48 XORs and 36 NANDs.

The total area of MI over composite field $GF((2^4)^2)$ is computed as:

$$\begin{aligned} A_{MI} &= A_I + A_{III} + A_{IV} + A_{II} + A_{V+}A_{VI} \\ &= (4A_{XOR} + 3A_{XOR}) + 4A_{XOR} \\ &\quad + (A_{NOT} + 4A_{XOR} + 4A_{NAND} + 4A_{AND} + 2A_{OR}) \\ &\quad + (48A_{XOR} + 36A_{NAND}) \\ &= A_{NOT} + 40\,A_{NAND} + 4A_{AND} + 2A_{OR} + 63A_{XOR} \end{aligned} \quad (11)$$

However, in the direct implementation, 162 XORs and 66 ANDs are required, and the number of transistors is 2340. The area reduction is up to 954(59.23%).

In this paper, the isomorphic mapping matrix T and matrix MT^{-1} are adopted as same as those in [7]. So the implementation of isomorphic mapping matrix multiplication requires 13 XORs and the multiplication of matrix MT^{-1} needs 11 XORs. The total number of gates in S-Box is computed as:

$$\begin{aligned} A_{S\_Box} &= A_T + A_{MT^{-1}} + A_{MI} \\ &= 13A_{XOR} + 11\,A_{XOR} \\ &\quad + (A_{NOT} + 40\,A_{NAND} + 4A_{AND} + 2A_{OR} + 63A_{XOR}) \\ &= A_{NOT} + 40\,A_{NAND} + 4A_{AND} + 2A_{OR} + 87A_{XOR} \end{aligned} \quad (12)$$

Compared with the direct implementation, which includes 203 XORs and 66 ANDs, the quantity of transistors of optimized S-Box is 1242 with a reduction of 56.14% in terms of the total area cost.

III. Comparisons and Results

In this paper, the implementation of CFA S-Box is optimized by GA. The type and quantity of logic gates as well as the total number of transistors in the direct implementation and optimization by GA are listed in TABLE II, respectively.

As shown in TABLE II, compared to the direct implementation, the optimized circuit of MI over $GF((2^4)^2)$ is reduced by 59.23%. The area reduction for S-Box is up to 56.14%.

In TABLE III, the multiplication and MI over $GF(2^4)$ proposed in this paper is compared to the implementations in the previous works. It can be known that, the multiplication over $GF(2^4)$ is further decomposed into composite field $GF((2^2)^2)$, and the implementation in this paper has the minimal area. The MI over $GF(2^4)$ is directly implemented in [3,4] and this paper, whereas it is further mapped into $GF((2^2)^2)$ in [7]. The best implementations in [3] and [4], which proposed four and three implementations respectively, are listed in TABLE III. As shown in TABLE III, the MI over $GF(2^4)$ proposed in this paper achieves the minimal area cost.

The comparisons of the whole of implementation of S-Box are listed in TABLE IV. As shown in table 4, the S-Box achieved with CFA technology is more compact than those with other methods. The optimized implementation of S-Box proposed in this paper has the minimal hardware requirement.

TABLE II
The area cost required by each part of the CFA S-box that is optimized by GA

Modules	Direct			Optimized by GA					
	XOR	AND	Transistors	NOT	NAND	AND	OR	XOR	Transistors(Reduction)
Multiplication Over$GF(2^4)$	44	16	624	—	12	—	—	18	264(57.69%)
MI over $GF(2^4)$	16	18	300	1	4	4	2	4	102(66%)
$(A_h+A_l)^2\times\gamma$	10	—	120	—	—	—	—	7	84(30%)
Adder Over $GF(2^4)$	4	—	48	—	—	—	—	4	48(0%)
MI Over $GF((2^4)^2)$	162	66	2340	1	40	4	2	63	954(59.23%)
T×	24	—	288	—	—	—	—	13	156(45.83%)
MT^{-1}×	17	—	204	—	—	—	—	11	132(35.29%)
S-Box	203	66	2832	1	40	4	2	87	1242(56.14%)

TABLE III
Comparisons of multiplication over $GF(2^4)$ and the MI over $GF(2^4)$ proposed in the works

Works	Multiplication over $GF(2^4)$					MI over $GF(2^4)$						
	Realization	XOR	AND	NAND	Transistors	Realization	XOR	AND	NOT	NAND	OR	Transistors
[3]	$GF((2^2)^2)$	21	9	—	306	$GF(2^4)$	13	8	—	—	—	204
[4]	$GF((2^2)^2)$	20	9	—	294	$GF(2^4)$	13	9	—	—	—	210
[7]	$GF((2^2)^2)$	18	12	—	288	$GF((2^2)^2)$	14	12	—	—	—	240
Ours	$GF((2^2)^2)$	12	—	18	264	$GF(2^4)$	4	4	1	4	2	102

ISBN: 978-988-19253-6-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE IV
THE COMPARISONS OF THE WHOLE OF IMPLEMENTATIONS OF S-BOX

Works	Realization	Transistors
[5]	Twisted BDD	11260
[6]	PPRM	2308
[6]	DSE	2788
[3]	CFA	1614
[4]	CFA	1368
[7]	CFA	1308
ours	CFA	1242

IV. CONCLUSION

The circuit generated by using EA has the compact and novel structure that is hard for people to come up with. Therefore, in this paper, the S-Box with CFA technology is optimized by adopting GA and the implementation has the minimal area occupancy. Firstly, the MI over $GF(2^8)$ is decomposed into composite field $GF((2^4)^2)$, and then the MI over $GF(2^4)$ and the multiplication over $GF((2^2)^2)$ are optimized with using GA. Compared with the direct implementation, the number of transistors in the optimized circuit of MI over $GF(2^4)$ and multiplication over $GF((2^2)^2)$ are reduced by 66% and 57.69%, respectively. Secondly, the common sub-expressions among three multiplications over $GF(2^4)$ in MI over $GF((2^4)^2)$ are eliminated by CSE algorithm. The area reduction of MI over $GF((2^4)^2)$ and S-Box is up to 59.23% and 56.14% respectively compared to the direct implementation. In previous works, the implementation of S-Box proposed in [7] has the minimal area cost [4], which consists of 91 XORs and 36 ANDs, i.e.1308 transistors. Compared with the implementation in [7], the optimization proposed in this paper includes a NOT, 40 NANDs, four ANDs, two ORs and 87 XORs, i.e.1242 transistors, with a reduction of 13.33% in terms of the total area occupancy. Therefore, the implementation of S-Box proposed in this paper has the minimal area cost at present.

REFERENCES

[1] O. Song, and J. Kim, "Compact Design of the Advanced Encryption Standard Algorithm for IEEE 802.15.4 Devices," *Journal of Electrical Engineering & Technology*, Vol. 6, No. 3, pp. 418–422, 2011.

[2] L. Fu, X. Shen, L. Zhu, J. Wang, "A Low-Cost UHF RFID Tag Chip with AES Cryptography Engine," *Security and Communication Networks*, Vol. 7, No. 2, pp. 365–375, February 2014.

[3] M. M. Wong, M. L. D. Wong, A. K. Nandi, and I. Hijazin, "Composite field $GF(((2^2)^2)^2)$ Advanced Encryption Standard (AES) S-box with algebraic normal form representation in the subfield inversion," *IET Circuits, Devices & System*, Vol. 5, No. 6, pp. 471–476, 2011.

[4] M. M. Wong, M. L. D. Wong, A. K. Nandi, and I. Hijazin, "Construction of Optimum Composite Field Architecture for Compact High-Throughput AES S-boxes," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 20, No. 6, pp. 1151–1155, 2012.

[5] S. Morioka, A. Satoh, "A 10-Gbps Full-AES Crypto Design with a Twisted BDD S-Box Architecture," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 12, No. 7. pp. 686-691, July 2004.

[6] Y. Chen, X. Zou, Z. Liu, Y. Han, and Z. Zheng, "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.

[7] D. Canright, "A Very Compact S-Box for AES," *7th International Workshop on CHES*, Springer-Verlag, LNCS, vol. 3659, pp. 441–455, 2005.

[8] X. Zhang, and K. K. Parhi, "On the optimum constructions of composite field for the AES algorithm," *IEEE Transaction on Circuits and systems–II: Express Briefs*, Vol. 53, No. 10, pp. 1153–1157, Oct. 2006.

[9] Z. G. Bao, and T.Watanabe, "A Novel Genetic Algorithm with Cell Crossover for Circuit Design Optimization," *Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on*, Taipei, Taiwan, May 24-27, 2009, pp.2982 – 2985, 2009.

[10] Z. G. Bao, and T. Watanabe, "A novel genetic algorithm with different structure selection for circuit design optimization," *the 14th International Symposium on Artificial Life and Robotics*, Oita, Japan, February 5–7, 2009, pp.266-270, 2009.

[11] J. F. Miller, and P. Thomson, " Cartesian genetic programming," *Proceedings of the Third European Conference on Genetic Programming Published as Lecture Notes in Computer Science*, vol. 1802, pp. 121–132 , 2000.

ISBN: 978-988-19253-6-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)