A Low Critical Path Delay Structure for Composite Field AES S-Box Based on Constant Matrices Multiplication Merging

Xiaoqiang ZHANG¹,²,a), Xinggan ZHANG¹b), Lan TANG¹c), Xinxing ZHENG⁴, Tianming NI³,³, Ning WU⁵

Abstract In this paper, a low critical path delay (CPD) circuit structure is proposed for composite field S-box circuit. In the low CPD structure, multiplicative inverse over $GF(2^4)$ and multiplicative over $GF(2^8)$ are constructed by AND-XOR-networks. The XOR-networks in the last two multiplications over $GF(2^8)$ are further merged with the following constant matrix multiplication operation to shorten the CPD. Finally, hardware complexities of our designs are compared with previous works. The comparisons indicate that our proposed method is effective. Our design of S-box/InvS-box based on the proposed method has lower CPD.

key words: Advanced Encryption Standard; S-Box; Composite Field; Critical Path Delay; Constant Matrix Multiplication Merging

Classification: Integrated circuits

1. Introduction

The Advanced Encryption Standard (AES) is the latest block cipher standard published by the National Institute of Standards and Technology (NIST) in 2001 [1], and it is widely used in the various systems of information security now. AES encryption process consists of four key operations, namely the SubBytes, ShiftRows, MixColumns and AddRoundKey. And AES decryption process consists of four inverse operations. Among the four operations, the SubBytes transformation, commonly known as the S-box, is the only nonlinear operation in AES. So it consumes the most resources and power in the AES implementations and it is the major bottleneck in both small area applications and high speed applications [2-4]. Over the years, different hardware implementations of AES S-box have been proposed. Among these implementations, the ones based on composite field arithmetic (CFA) technologies have the smallest size [5, 6]. Furthermore, the CFA-based S-box can further improve the running speed through pipeline division technology [7], and further reduce the power consumption through path balancing technology [8-11]. Therefore, hardware implementations of AES S-box based on CFA have caught more attentions in current studies.

Different construction schemes of composite fields have been proposed for AES S-box in previous works [12-23]. Most of these works mainly focus on reducing area cost. However, efficiency of the hardware implementations is not only measured by area cost but also by delay [16, 24]. In this paper, a low critical path delay (CPD) structure is proposed for CFA-based AES S-box. Firstly, in the proposed low CPD structure, multiplication over $GF(2^4)$ and MI over $GF(2^8)$ are constructed by low delay AND-XOR-networks. Secondly, the XOR-networks of last two multiplications over $GF(2^4)$ in multiplicative inverse (MI) over $GF(2^8)$ are further merged with the following constant matrix multiplication (CMM) operation. By the merging, the CPD of CFA-based AES S-box is further shortened. In the last, inverse S-box (InvS-box) are also constructed by the same way, and our best designs of S-box/InvS-box are compared with previous works, the comparisons indicate our designs based on the proposed structure have lower CPD.

2. Low CPD Structure for MI over $GF((2^4)^3)$

2.1 S-Box Base on CFA Technologies

The AES S-box is defined as a MI over Galois field $GF(2^8)$ followed by an affine transformation [1]. The MI over $GF(2^8)$ is a complicated and resource consuming task. To reduce the computational complexities, the MI over $GF(2^8)$ are often mapped into composite field by CFA technologies [3, 4]. The structure of CFA-based S-box is shown in Fig. 1.

An isomorphic mapping matrix $\delta$ is used to map the input vector from finite field $GF(2^8)$ to the composite
field and its inverse matrix $\delta^{-1}$ is used to revert the computing results back to field $GF(2^4)$. Usually, the inverse isomorphic mapping matrix $\delta^{-1}$ is merged with affine matrix $M$ to reduce hardware resource. As shown in Fig. 1(a), the CFA-based S-box is consisted of CMM operation $\delta \times$, MI over composite field $(\alpha)^{-1}$, CMM operation $M \times$, add constant vector operation $+C$, where $M = M \cdot \delta^{-1}$, and operation $M \times$ and operation $+C$ perform affine transform operation together [1].

A specific Galois field is dependent on the selected irreducible polynomial and the basis. Standard basis and normal basis are the two most commonly used bases in Galois field. The hardware structure of MI over $GF((2^4)^2)$ based on the standard basis is shown in Fig.1(b) [13]. The dashed line denotes the critical path of the MI over $GF((2^4)^2)$.

$$\begin{align*}
\delta \times & \quad (a) S-box \ structure; \ (b) \ MI \ over \ GF((2^4)^2) \ structure
\end{align*}$$

All operations in MI over $GF((2^4)^2)$ are implemented over $GF(2^4)$, these operations include multiplication $\Theta$, addition $\Phi$, constant coefficients multiplication (CCM) $\times_B$, MI $(\alpha)^{-1}$, and square $(\gamma)^2$.

Among these operations, addition, CCM, and square are linear operations, which include only XOR operations. And as square and CCM are adjacent to each other, they are often merged into one linear operation to reduce the area cost and CPD in hardware implementations [2]. Multiplication and MI are non-linear operations, which include not only XOR operations but also AND operations.

Only XOR gates and AND gates are used in AES S-box. Therefore, area cost of S-box can be measured by XOR gate counts and AND gate counts, and CPD can also be measured by XOR gate counts and AND gate counts on critical path [24].

In this paper, we use $A_{XOR}$ and $A_{AND}$ to denote area cost of a XOR gate and area cost of a AND gate, respectively. Normally, A XOR gate requires 12 transistors and a AND gate requires 6 transistors [25], therefore, $A_{XOR}$ is about double $A_{AND}$. We use $T_{XOR}$ and $T_{AND}$ to denote delay of a XOR gate and a AND gate, respectively. Normally the $T_{AND}$ is little smaller than $T_{XOR}$. By simulation, we can get $T_{AND}=3/4T_{XOR}$ in SMIC 0.18$\mu$m technologies.

Note that add constant vector operation $+C$ in Fig. 1(a) can also be implemented by logic NOT gates, and a logic NOT gates with a logic XOR gate in the preceding operation can be further replaced by logic XNOR gates. As the area cost and delay of a XNOR gate are the same as the ones of a XOR gate, the area cost and delay of the operation $+C$ can be ignored in hardware implementations.

2.2 Low CPD Structures for Multiplication over $GF(2^4)$

As mentioned before, a specific $GF(2^4)$ is depended on the selected irreducible polynomial and the selected basis for $GF(2^4)$. There are three irreducible polynomials for $GF(2^4)$. They are listed as follows.

$$GF (2^4): \begin{cases} f_1 (x) = x^4 + x^3 + x^0 \ f_2 (x) = x^4 + x^0 \ f_3 (x) = x^4 + x^3 + x^2 + x^1 + x^0 \end{cases} (1)$$

We take the a specific $GF(2^4)$ generated by irreducible polynomial $f_i(x)$ with standard basis to illustrate the design method of low CPD structure. The multiplication over this specific $GF(2^4)$ can be expressed as the following.

$$\gamma = \alpha \beta (\text{mod} \ f_i(x))$$

$$\begin{align*}
\gamma_1 &= \alpha_3 \beta_3 + \alpha_2 \beta_2 + \alpha_1 \beta_1 + \alpha_0 \beta_0 + \alpha_2 \beta_1 + \alpha_3 \beta_3 + \alpha_0 \beta_3 + \alpha_1 \beta_0 \\
\gamma_2 &= \alpha_2 \beta_2 + \alpha_0 \beta_0 + \alpha_3 \beta_3 \\
\gamma_3 &= \alpha_3 \beta_3 + \alpha_1 \beta_1 + \alpha_0 \beta_0 + \alpha_2 \beta_2 \\
\gamma_4 &= \alpha_2 \beta_2 + \alpha_1 \beta_1 + \alpha_0 \beta_0 + \alpha_3 \beta_3
\end{align*} \quad (2)$$

where $\{a, b, \gamma\} \in GF(2^4)$, $\{\alpha_0, \alpha_1, \beta_0, \beta_1, \beta_2, \beta_3, \gamma_0, \gamma_1, \gamma_2, \gamma_3\} \in GF(2)$. According to Eq. (2), the area cost of the multiplication is $22A_{XOR}+26A_{AND}$ in the direct implementation. The structure of the multiplication over $GF(2^4)$ based on $AND-XOR-networks$ is shown in Fig. 2.

As shown in Fig. 2, the circuit is divided into two parts. Part I is consisted of AND gates only and Part II is consisted of XOR gates only. The expressions of Part I and Part II are expressed as following, respectively.
To achieve the shortest CPD, Part I and Part II are constructed by Delay-Driven-Binary-Tree (DDBT) structure, respectively, which was proven that it has the shortest critical path for two-input logical gates networks [26]. According to Eq. (3) and Eq. (4), we can get that the hardware complexities of the structure in Fig. 2 are 22\text{A}$XOR+16\text{A}$AND+4\text{T}\text{XOR}+17\text{T}\text{AND}$. We suppose input delays of multiplication over $GF(2^4)$ can be ignored, Part I and Part II are also constructed by Fastest-Binary-Tree (FBT) structure [27, 28], which is a special case of the DDBT structure and it is only suitable for the same input delays of single gate networks [29, 30].

It is easy to construct Part I, as there is only one layer AND operation in Part I. The delays of all outputs of Part I are the same, and the delays are all $1\text{T}\text{AND}$. The XOR gate counts of Part II can be further reduced by sharing common subexpressions in Eq. (4). But it has been proven that sharing common subexpressions may increase the CPD in hardware implementations [29]. To keep CPD unchanged after sharing common subexpressions, delay-aware common subexpressions elimination (DACSE) algorithm propose in [30], which can search the common subexpressions under delay constrains, is used in this paper. As the delay constrain is set with $4\text{T}\text{XOR}+17\text{T}\text{AND}$ for the XOR-networks, so we can keep CPD unchanged after sharing the common subexpressions. The structure is also constructed by DDBT structure after sharing common subexpressions. And the hardware complexities after sharing common subexpressions are $15\text{A}$XOR+$16\text{A}$AND+$47\text{XOR}+17\text{T}\text{AND}$. Total 7 XOR gates are reduced by DACSE. About 31.82\% XOR gates are reduced.

2.3 Low CPD Structures for MI over $GF(2^4)$

The multiplication over the specific $GF(2^4)$ can be expressed as the following.

$$\alpha^{-1} = \{\alpha_3^{-1}, \alpha_2^{-1}, \alpha_1^{-1}, \alpha_0^{-1}\}$$

where $\alpha^{-1} \in GF(2^4)$, and \{\alpha^{-1}_3, \alpha^{-1}_2, \alpha^{-1}_1, \alpha^{-1}_0\} is $GF(2)$.

According to Eq. (5), the MI over $GF(2^4)$ requires the area cost of 26$A$XOR+32$A$AND in the direct implementation. Eq. (5) can also be divided into two part as following.

$$\alpha^{-1} = \{\alpha_3^{-1}, \alpha_2^{-1}, \alpha_1^{-1}, \alpha_0^{-1}\}$$

The structure of the MI over $GF(2^4)$ based on AND-XOR-networks is the same as multiplication over $GF(2^4)$, except that the delays of AND-networks are different, they varies from $0\text{T}\text{AND}$ to $2\text{T}\text{AND}$. The XOR-networks and AND-networks in MI over $GF(2^4)$ area also constructed by DDBT structure. The hardware complexities for MI over $GF(2^4)$ based on AND-XOR-networks are $(26\text{A}$XOR+$14\text{A}$AND)$@$(3\text{T}\text{XOR}+2\text{T}\text{AND})$. The gates counts in AND-networks and XOR-networks also can be reduced by DACSE algorithm. We set the delay constrains with $2\text{T}\text{AND}$ for AND-networks and $3\text{T}\text{XOR}+2\text{T}\text{AND}$ for XOR-networks. The hardware complexities of MI over $GF(2^4)$ are $(20\text{A}$XOR+$10\text{A}$AND)$@$(3\text{T}\text{XOR}+2\text{T}\text{AND})$ after optimized by DACSE algorithm. Total 6 XOR gates and 4 AND gates are reduced by DACSE. About 23.08\% XOR gates and 28.57\% AND gates are reduced.

2.4 Hardware Complexities Analyses

Except for multiplication over $GF(2^4)$ and MI over $GF(2^4)$, other operations in S-box are linear operations. These operations are also constructed by DDBT and optimized by DACSE algorithm. The hardware complexities of MI over $GF(2^4)$ and the whole S-box are analyzed on Table I. As shown on Table I, the hardware complexities of whole MI over $GF(2^4)$ are $(75\text{A}$XOR+$58\text{A}$AND)$@$(19\text{T}\text{XOR}+4\text{T}\text{AND})$. The hardware complexities of whole S-box are $(100\text{A}$XOR+$58\text{A}$AND)$@$(19\text{T}\text{XOR}+4\text{T}\text{AND})$. 

| Blocks | counts | Area | Path |
|--------|--------|------|------|
| Multiplier | 3 | 13 | 16 | 4 | 1 |
| MI over | \(GF(2^4)\) | \(\text{M}_{\text{MI}}\) | 1 | 20 | 10 | 3 | 2 |
| Adder | 2 | 4 | 4 | 1 | 1 |
| Sum of MI | 75 | 58 | 13 | 4 |
| \(\text{M}_{\text{M}}\) | 1 | 12 | 3 | 3 |
| Sum of S-box | 100 | 58 | 19 | 4 |
3. Further Shortening CPD by Matrices Merging

As shown in Fig. 1, the last operations of MI over $GF(2^4)$ are two multiplications over $GF(2^4)$. The XOR-networks of last two multiplications over $GF(2^4)$ can be further merged with the following CMM operation, as they are also the linear operations. The merged method is presented in the following.

The expressions of XOR-networks in Eq. (4) can be further expressed as a CMM operation as follows.

$$\gamma = M_{\gamma} \Phi$$ (8)

where

$$\gamma = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_4 \end{bmatrix}, \quad \Phi = \begin{bmatrix} \Phi_{15} \\ \vdots \\ \Phi_0 \end{bmatrix},$$

$$M_{\gamma} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix},$$

where $M_{\gamma}$ is a 4×16 bits constant matrix. There are two multiplication over $GF(2^4)$ in the last operations of MI over $GF(2^4)$. As shown in Fig. 3, the CMM operations of last two multiplications over $GF(2^4)$ can be combined into one CMM operation. The combined CMM operation can be expressed as follows.

$$\left[ \begin{array}{c} \gamma_h \\ \gamma_l \end{array} \right] = \left[ \begin{array}{c} M_s \\ 0 \end{array} \right] \left[ \begin{array}{c} \Phi_h \\ 0 \end{array} \right] \Rightarrow \gamma_w = M_{\gamma} \Phi_w$$ (9)

where $\gamma_h$ and $\gamma_l$ are input vectors of multiplication $A_h^{-1}$ and multiplication $A_l^{-1}$, respectively, $\Phi_h$ and $\Phi_l$ are output vectors of multiplication $A_h^{-1}$ and multiplication $A_l^{-1}$, respectively, $M_{\gamma}$ is 8×16 bits combined matrix.

After merging, only AND-networks are left in the last two multiplications over $GF(2^4)$. The hardware complexities of MI over $GF(2^4)$ and whole S-box are optimized by DACSE to optimize the block under constrain with $T_{XOR}$. After optimized by DACSE, the hardware complexities turn into $A_{XOR}$. About 60.09% gates counts are reduced by DACSE.

![Fig. 4 The merging process of CMM operations](image)

As shown in Fig. 4, $M_{\gamma} \times$ operation is followed by $M_{\delta} \times$ operation. As $M_{\delta} \times$ operation is 8×8 bits constant, $M_{\gamma} \times$ operation can be merged with $M_{\delta} \times$ operation as follows.

$$\eta = M_{\eta} \gamma_w = M_{\gamma} M_{\delta} \Phi_w = M_{\delta} \Phi_w$$ (9)

where $M_{\gamma} \times M_{\delta} \times$ is a merged matrix, and it is an 8×16 bits matrix. After merging, we can get the hardware complexities of $M_{\delta} \times$ block are $115 A_{XOR}$ at $5 T_{XOR}$. And the gate counts of $M_{\delta} \times$ block can be further reduced by CSE algorithms. To keep CPD unchanged, we use DACSE to optimize the block under constrain with $T_{XOR}$. After optimized by DACSE, the hardware complexities turn into $A_{XOR}$. About 60.09% gates counts are reduced by DACSE.

![Fig. 3 The combined process of CMM operations](image)

| Blocks | Area | Path |
|--------|------|------|
| Multiplier | 15 | 15 | 4 |
| MI over $GF(2^4)$ | 20 | 10 | 3 |
| Adder | 2 | 4 | 1 |
| AND-Nets | 16 | 16 | 1 |
| Sum of MI | 45 | 58 | 9 |
| $\delta \times$ | 1 | 12 | 3 |
| $M_{\gamma} \times$ | 45 | 58 | 9 |
| Sum of S-box | 102 | 58 | 17 |

4. Best Designs and Comparisons

The low CPD structures of S-box on other specific $GF(2^4)$ are designed in the same way. Total 2 basis for $GF(2^4)$ ×(irreducible polynomial for $GF(2^4)$) ×2(basis for $GF(2^4)$) ×3(irreducible polynomial for $GF(2^4)$) ×8(isomorphic mapping matrices) = 768 structures are check to find the best one, which has the shortest CPD with the minimal area. The specifications of best S-box are list on table III. As shown on Table III, the CPD of best S-box is only (147XOR+47AND).
Low CPD structures of InvS-box are constructed in the same way, and the specifications of best InvS-box are also listed on Table III. And the CPD of best InvS-box is also (14XOR+4AND). The hardware complexities of S-box and InvS-box proposed in this paper are compared with previous works on Table IV.

Note that only standard basis and normal basis are discussed in this paper. The CPD also can be shortened by taking special CFA technologies in [22, 23]. In [22], redundantly represented basis are mixed with standard basis and normal basis. And polynomial ring representation are further added to construct composite basis with low CPD structure to further study the design methods of low CPD structures of AES S-box.

### 5. Conclusions

In this paper, low CPD structure of AES S-box is proposed. The low CPD structure is constructed by low-delay AND-XOR-networks structure. And the delay is further shortened by CMM merging. The comparisons indicate that our designs base on the proposed structure has lower CPD. The low CPD structure of AES S-box proposed in this paper only take structural aspect into consideration. The CPD also can be shortened by take mixed basis [22, 23]. In the future works, we will combine our low CPD structure with low CPD basis to further study the design methods of low CPD structures of AES S-box.

### Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 61976113 and No. 61904001), the Natural Science Foundation of Anhui Province (No. 1908085MF179 and No. 1908085QF272), the Natural Science Foundation of the Anhui Province Higher Education Institutions (No. KJ2019A0983 and No. KJ2019A0163), the Natural Science Research Program of Anhui Province Higher Education Promotion Plan (No. TSJK2017B23), The Scientific Research Starting Foundation for the Introduction of Talents of Anhui Polytechnic University (No. 2017YQQ001 and No. 2018YQQ007).

### References

1. National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES) FIPS Publication 197, http://csrc.nist.gov/publications/fips/fips-197/fips-197.pdf, Nov 2001.
2. X. Zhang, N. Wu, X. Zheng, the Design Method of Compact Composite Field AES S-Box Based on AND-XOR Array Structure. In the IEEE Conference on Industrial Electronics and Applications-ICIEA, Siem Reap, Cambodia, 18-20 June 2017, pp. 1881-1886.
3. M. M. Wong, M. L. D. Wong, A. K. Nandi, I. Hijazin, Composite field $GF((2^4)^2)$ Advanced Encryption Standard (AES) S-box with Algebraic Normal Form Representation in the Subfield Inversion. IET Circuits, Device & Systems. 2011, 5, 471-476.
4. M. M. Wong, M. L. D. Wong, A. K. Nandi, I. Hijazin, Construction of Optimum Composite Field Architecture for Compact High-Throughput AES S-boxes. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2012, 20, 1151–1155.
5. S. Morioka, A. A. Satoh, 10-Gbps Full-AES Crypto Design with a Twisted BDD S-Box Architecture. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2004, 12, 686-691.
6. Y. Chen, X. Zou, Z. Liu, Y. Han, Z. Zheng, Energy-Efficient and Security-Optimized AES Hardware Design for Ubiquitous Computing. Journal of Systems Engineering and Electronics. 2008, 19, 652–658.
7. A. Hodjat and I. Verbauwhede, Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors, IEEE Transactions on Computers. 2006, vol. 55, no. 4, pp. 366–372.
8. Y. H. Zeng, X. C. Zou, Z. L. Liu, J. M. Lei, Low-power clockless hardware implementation of the Rijndael S-box for wireless sensor networks, Journal of China Universities of Posts and Telecommunications, December 2007, vol.14, no. 4, pp. 104–109.
9. A. Dogan, S. B. Ors, G. Saldamli, Analyzing and comparing the AES architectures for their power consumption, Journal of Intelligent Manufacturing, 2014, vol. 25, no. 2, pp. 263–271.
[10] Z. Liu, Y. Zeng, X. Zou, and J. Lei, A Low-power and Compact AES S-box IP in 0.25 μm CMOS for Wireless Sensor Network, *Proceedings of the 2007 IEEE International Conference on Mechatronics and Automation*, 2007, pp. 723–728.

[11] S. Moriya, A. Satoh, An Optimized S-Box Circuit Architecture for Low Power AES Design, *Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002)*, LNCS 2523, 2003, pp. 172–186.

[12] D. Canright, A Very Compact S-Box for AES. In 7th Int. Workshop on Cryptographic Hardware & Embedded Systems-CHES, Edinburgh, Uk, August 29-September 1 J. R. Rao, B. Sunar, Eds. Springer International Publishing: New York, USA, 2005 LNCS, volume 3659, pp. 441-455.

[13] X. Zhang, K. K. Parhi, On the Optimum Constructions of Composite Field for the AES Algorithm. *IEEE Trans. on Circuits and Syst. II: Express Briefs*, 2006, 53, 1153–1157.

[14] Y. Nogami, K. Nekado, T. Toyota, N. Hongo, Y. Morikawa, Mixed Bases for Efficient Inversion in \( F(2^{256}) \) and Conversion Matrices of SubBytes of AES. In 12th Int. Workshop on Cryptographic Hardware and Embedded Systems-CHES 2010, Santa Barbara, USA, August 17-20 Stefan Mangard, François-Xavier Standaert, Eds. Springer International Publishing: New York, USA, 2010 LNCS, volume 6225, pp. 234–247.

[15] Y. Nogami, K. Nekado, T. Toyota, N. Hongo, Y. Morikawa, Mixed Bases for Efficient Inversion in \( F(2^{256}) \) and Conversion Matrices SubBytes of AES. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, 2011, E94-A, 1318–1327.

[16] X. Zhang, N. Wu, F. Zhou, F. Ge, Optimization of Area and Delay for Implementation of the Composite Field Advanced Encryption Standard S-Box. *Journal of Circuits, Systems, and Computers*, 2016, 25, 1-29.

[17] J. Wolkerstorfer, E. Oswald, M. Lamberger, An ASIC Implementation of the AES S-boxes. In *Conference on the Cryptographers' Track at the RSA - CT-RSA*, San Jose, CA, USA, February 18-22 Bart Preneel, Eds. Springer International Publishing: New York, USA, 2010 LNCS, volume 2271, pp. 67–78.

[18] S.-F. Hsiao, M.-C. Chen, C.-S. Tu, Memory-Free Low-Cost Designs of Advanced Encryption Standard Using Common Subexpression Elimination for Subfunctions in Transformations. *IEEE Transactions on Circuits and Systems—I: Regular papers*, 2006, 53, 615-627.

[19] N. Chen, Z. Y. Yan, Compact Designs of Mixcolumns and Subbytes Using a Novel Common Subexpression Elimination Algorithm In 2008 IEEE International Symposium on Circuits and Systems - ISCAS 2008, Seattle, Washington, USA, May 18-21 2008, pp. 1584 – 1587.

[20] N. Chen, Z. Y. Yan, High-Performance Designs of AES Transformations. In 2009 IEEE International Symposium on Circuits and Systems - ISCAS 2009, Taipei, Taiwan, May 24-27 2009, pp. 2906-2909.

[21] Y. Jeon, Y. Kim, D. A. Lee, Compact Memory-Free Architecture for the AES Algorithm Using Resource Sharing Methods. *Journal of Circuits, Systems, and Computers*, 2010, 19, pp.1109-1130.

[22] K. Nekado, Y. Nogami, K. Iokibe, Very Short Critical Path Implementation of AES with Direct Logic Gates. In *7th International Workshop on Security*, IWSEC 2012, Advances in Information and Computer Security; Fukuoka, Japan, November 7-9 Goichi Hakoda, Toru Hiro Yamauchi, Eds. Springer International Publishing: New York, USA, 2012 LNCS, Vol. 7631, pp. 51-68.

[23] R. Ueno, N. Homma, Y. Sugawara, Y. Nogami, T. Aoki, Highly Efficient GF(2^8) Inversion Circuit Based on Redundant GF Arithmetic and Its Application to AES Design. In *17th Int. Workshop on Cryptographic Hardware and Embedded Systems*, CHES 2015, Saint-Malo, France, September 13-16 Tim Güneysu, Helena Handschuh, Eds. Springer International Publishing: New York, USA, 2015 LNCS, volume 9293, pp. 234–247.

[24] J. L. Imaña, J. M. Sánchez, and F. Tirado, Bit-Parallel Finite Field Multipliers for Irreducible Trinomials, *IEEE Transaction on Computers*, vol. 55, no. 5, pp. 520-530.

[25] N. Ahmad, S. M. R. Hasan, Low-power compact composite field AES S-Box/Inv S-Box design in 65 nm CMOS using Novel XOR Gate, *INTEGRATION, the VLSI journal*, 46(2013), pp. 333–344.

[26] N. Petra, D. D. Caro, A. G. M. Strollo, A Novel Architecture for Galois Fields GF(2^n) Multipliers Based on Mastrovito Scheme. *IEEE Transactions on Computers*, 2007, 56, 1470-1483.

[27] A. Hosangadi, F. Fallah, R. Kastner, Simultaneous Optimization of Delay and Number of Operations in Multiplexerless Implementation of Linear Systems. In *14th International Workshop on Logic and Synthesis-IWLS*, Lake Arrowhead, California, USA, June 8-10, 2005 pp. 1-8.

[28] A. Chandrakasan, M. Potkonjak, R. Mehra, J. Rabaey, R. W. Brodersen, Optimizing Power Using Transformations. *IEEE Transactions on Computer-Aided Design Integration Circuits and Systems*. 1995, 14, 12–31.

[29] X. Zhang, N. Wu, F. Zhou, J. Li, Yasir, Low-delay parallel Chien search architecture for RS decoder. *IEICE Electronics Express. 2016, 13, 1-6.*

[30] X. Zhang, N. Wu, F. Zhou, X. Chen, An optimized delay-aware common subexpression elimination algorithm for hardware implementation of binary-field linear transform. *IEICE Electronics Express. 2014, 11, 1-8.*