# 3D Design for Lightweight S-Box

**Conference Paper** · February 2022

DOI: 10.1109/ICISET54810.2022.9775854



**3 authors:**

Tasnuva Ali
Daffodil International University
**7** PUBLICATIONS **23** CITATIONS
SEE PROFILE

Azni Halim
USIM | Universiti Sains Islam Malaysia
**54** PUBLICATIONS **287** CITATIONS
SEE PROFILE

Nur hafiza Zakaria
USIM | Universiti Sains Islam Malaysia
**18** PUBLICATIONS **71** CITATIONS
SEE PROFILE

# 3D Design for Lightweight S-Box

Tasnuva Ali
*Department of Electronics and Telecommunication Engineering*
*Daffodil International University*
Dhaka, Bangladesh
tasnuva@daffodilvarsity.edu.bd

A. H Azni
*Faculty of Science and Technology*
*Universiti Sains Islam Malaysia*
Nilai, Malaysia
ahazni@usim.edu.my

Nur Hafiza Zakaria
*Faculty of Science and Technology*
*Universiti Sains Islam Malaysia*
Nilai, Malaysia
mzhafiza@usim.edu.my

***Abstract*— The Internet of Things (IoT) applications are considered as smart device applications because of its remote monitoring/ controlling access. The vast quantity of devices is linked with heterogeneous IoT infrastructures which increases various attacks in IoT applications. Therefore, the security analysis should be evaluated to find out the best secured encryption process before implementing IoT applications. Moreover, lightweight algorithms are suitable for small power and high speed IoT devices. In this paper, lightweight algorithm is chosen because of its faster speed among other algorithms. However, the security of lightweight algorithms is not satisfactory for IoT/mHealth applications. To enhance the security of lightweight algorithms, we have designed a 4x4 composite S-Box rather than Look Up Table (LUT) method. Additionally, the composite S-Box value is again secured using 3D cipher for confusion and diffusion process to improve its security. Thus, we have proposed a lightweight 3D Composite S-Box which will give more security compared to other existing S-Boxes.**

***Keywords—S-Box, 3D, Security.***

## I. INTRODUCTION

The wide-ranging IoT applications are becoming potential and popular because of its easily data collection process from real world and transfer data in different domains. The most common challenge of handling IoT devices is limited resources such as memory , power and physical space [1]. Thus, the resource constrained IoT devices are facing high security issues to transfer data over network. The embedded IoT devices are also arranged at various locations but facing physical security problem [2]. These devices are mandatory to enhance the security compared to existing design although offering less memory, energy and power aspects. The lightweight algorithms are suitable for power constrained devices which provide definite solutions to exact problems by designers [3]. The design of algorithms is based on two specific requirements: identify all possible cryptanalysis attacks and a set of specific guidelines that function on a step-by-step [4]. The difficult task is to merge these two goals together to get the better performance like security, less power, less memory of any lightweight algorithms.

To meet the above targets, many lightweight block ciphers have been designed over last two decades. Many of these designs meet one or two targets but fail to give security properly. Moreover, many articles have worked on enhancing security of proposed algorithms but couldn't meet all security criterions recommended by NIST. In this paper, different lightweight algorithms are studied thoroughly by addressing secured transmission of signal in medium. Among them SIMECK [5], SPECK [6], GIFT [7], Midori64 [8], RoadRunneR [9], LRBC [10], SKINNY [11], RECTANGLE [12], BORON [13], SPARX [14] are the popular SPN and Feistel networks lightweight algorithms to meet the different performance criterions.

In this paper, lightweight S-Box has been chosen because of its better performance regarding Figure of Merit (FOM) and security aspects [15]. Besides, the 2D S-Box security is improved increasing round numbers or confusion diffusion properties that enhanced delay time. Thus, it is mandatory to design the algorithm with optimized confusion and diffusion steps with minimized mentioned attacks [16]. The confusion property of S-Box can be upgraded by designing different types of ideal S-Boxes [17] and diffusion properties can be modified by upgrading key schedule algorithm [18]. Therefore, the new design can be focused on 3D S-Box design to improve the mentioned limitations in future IoT/ mHealth applications.

Therefore, we have proposed a composite 3D S-Box for lightweight algorithms. The confusion/substitution step is done by designing composite S-Box and diffusion step which is equal to shift rows and mix columns, is ended by 3D rotation to get the final cipher text. The proposed round is reduced because the composite S-Box has already encrypted the data compared to other 2D designs. The composite S-Box is designed for 4X4 block size using Galois field sub-pipelining structure which reduces number of gates as areas compared to [19-20]. Then the shift rows and mix column operation are achieved by 3D rotation which uses 64 bits block size and 128 bits key with proposed 16 rounds which is less than other 3D designs. Hence, the paper is organized as follows: section 2 describes composite lightweight S-Box Design, Section 3 explains 3D design for S-Box and section 4 concludes the work.

## II. COMPOSITE LIGHTWEIGHT S-BOX DESIGN

The finite field S-Box {GF $(2^4)$} and GF $\{((2^2))^2\}$ is a combinational and sub-pipelining structure which improves linear and differential cryptanalysis compared to Look Up Table (LUT) S-Box and also reduced number of gates [21]. The lightweight ciphers designed in papers [22-27] are LUT based which have their security limitations in hardware implementation. Therefore, we have to design a 4X4 composite field S-Box that steps are:

- First, find out the irreducible polynomials of 4X4 square matrix. We get 3 irreducible polynomials such as $x^4+x+1$, $x^4+x^3+1$, $x^4+ x^3+x^2+x+1$ among 16

combinations. We consider $x^4+x+1$ irreducible polynomial for further calculation in this paper.

- Then Isomorphic Mapping(δ) from {GF ($2^4$)} to {GF $((2^2))^2$} composite field is required for Conversion Matrix. This isomorphic mapping involves two steps. Firstly, generate a conversion matrix between {GF ($2^4$) and GF $((2^2))^2$} and secondly conversion matrix selection is calculated based on polynomials.
- After that, find out Multiplication Inverse (MI) Matrix from Conversion Matrix.
- The Multiplicative inverse output is feed to Inverse Isomorphic($\delta^{-1}$) from GF $\{((2^2))^2\}$ to {GF($2^4$)} composite field.
- Final step is completed by Affine Transformation (AT) to get the final composite S-Box value which is ready for diffusion process.

### A. *Minimal Polynomials for Composite Field*

The minimal polynomial calculation for 4X4 Matrix is:

$$m_\alpha(x) = (x+\alpha)\,(x+\alpha^2 m) \quad (1)$$

For 4X4 matrix pipelining, we use here n=2 and m=2

Thus, $m_\alpha(x) = (x+\alpha)\,(x+\alpha^4)$

$$= x^2 + x\alpha + x\alpha^4 + \alpha^5 \quad (2)$$

Consider, one of the irreducible polynomials that is

$P(x) = x^4+x+1$

After calculation, $x^4 = x+1$, $\alpha^4 = \alpha+1$

### B. *Conversion Matrix Calculation (CM)*

The conversion matrix equation {GF ($2^4$)} to {GF $((2^2))^2$} can be expressed as:

$$A= \overline{a_{00}} + ( \overline{a_{10}} + \overline{a_{11}} )\alpha + ( \overline{a_{01}} + \overline{a_{10}} + \overline{a_{11}} )\,\alpha^2 + \overline{a_{11}}\,\alpha^3 \quad (3)$$

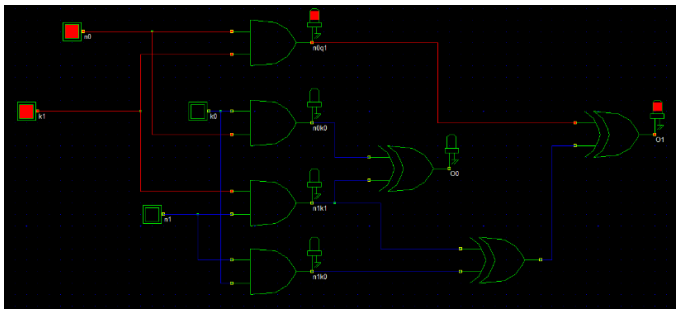
Hence, {GF ($2^4$)} to GF $\{((2^2))^2\}$ CM is

$$\delta \times a = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (4)$$

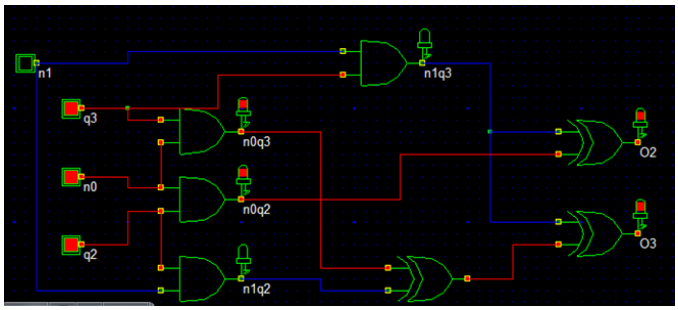
where "a" is the 4 bits input message.

### C. *MI Calculation*

The Multiplicative Inverse (MI) can be found after Isomorphic Function calculation. The MI module is designed using dsch2 software to get the final $O_1$, $O_2$, $O_3$, $O_4$ output. All the add operations are considered as XOR operation. To design the Multiplicative Inverse module, we need 18 XOR gates and 12 AND gates for 4X4 square matrix. The final result from dsch2 software is given below where we take input as 1111 and get the final output 1110 from MI calculations.



Step 1: $O_1$ and $O_0$ Output




Step 2: $O_3$ and $O_2$ Output

Fig. 1. Composite S-Box Output using dsch2 Software

### D. *Inverse Isomorphic ($\delta^{-1}$)*

The inverse isomorphic ($\delta^{-1}$) function converts GF $\{((2^2))^2\}$ to {GF ($2^4$)} using the following equation:

$$A= \overline{a_{00}} + ( \overline{a_{01}} + \overline{a_{10}} )\alpha + ( \overline{a_{01}} + \overline{a_{11}} )\,\alpha^2 + \overline{a_{11}}\,\alpha^3 \quad (5)$$

Here, GF $\{((2^2))^2\}$ to GF ($2^4$) CM is

$$\delta^{-1} \times a = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (6)$$

The isomorphic inverse function output is applied to Affine Transformation (AT) block to get the final Composite S-Box output.

### E. *Affine Transformation (AT):*

The equation of Affine Transformation and Inverse Affine Transformation can be expressed as:

$$AT = Ax + C \quad (7)$$

$$AT^{-1} = A^{-1}x + C \quad (8)$$

Here, A and $A^{-1}$ are 4x4 Affine Matrixes, x is 4-bit inputs which comes from Inverse Isomorphic Function ($\delta^{-1}$), '+' is XOR operation and C is the Affine Constant. Therefore,

$$\text{Affine Transformation} = \begin{bmatrix}1 & 0 & 0 & 0\\ 1 & 0 & 1 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix} \text{x} \begin{bmatrix}a3\\ a2\\ a1\\ a0\end{bmatrix} + \begin{bmatrix}c3\\ c2\\ c1\\ c0\end{bmatrix} \quad (9)$$

$$\text{Inverse Affine} = \begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\end{bmatrix} \text{x} \begin{bmatrix}a3\\ a2\\ a1\\ a0\end{bmatrix} + \begin{bmatrix}\overline{c3}\\ \overline{c2}\\ \overline{c1}\\ \overline{c0}\end{bmatrix} \quad (10)$$

Here, $a_0$, $a_1$, $a_2$, $a_3$ are $\delta^{-1}$ outputs for Affine Transformation and $\delta$ for Inverse affine Transformation, $c_0$, $c_1$, $c_2$, $c_3$ are Affine Constants which can be 16 possible combinations. In this paper, we take 0110 constant to calculate further equations. We need 16 XOR gates and 16 AND gates for Affine Transformation module.

## III. 3D S-BOX DESIGN

The diffusion can be done of the algorithm on the text using 3D rotation of the composite S-Box values depending on 4x4 inputs. In previous works, 3D rotation can be done by slice rotation [28], particular axis rotation [29] or lateral shift rotation [30] which needs 512 bits key length. The large block and key size are not appropriate for designing IoT/mHealth devices. Therefore, we propose a 3D axis or shift rotations of the rows with 128 bits key and 64 bits block size. The 3D transformation process can be divided into 3 sub sections:

- Axis wise plate arrangement
- Key Bits distribution
- Rotation Policy depending on key

### A. Axis Wise Plate Arrangement

The length of the key is considered as 8 bits for each round with 16 number of rounds. The 4X4 or 64 bits array data first divided into 4 blocks and each axis is divided into 4 Plates. The 64 bits data block can be distributed 4 plates like X Axis:

| | | | |
|---|---|---|---|
| $a_{15}$ | $a_{14}$ | $a_{13}$ | $a_{12}$ |
| $a_{11}$ | $a_{10}$ | $a_9$ | $a_8$ |
| $a_7$ | $a_6$ | $a_5$ | $a_4$ |
| $a_3$ | $a_2$ | $a_1$ | $a_0$ |

| | | | |
|---|---|---|---|
| $a_{14}$ | $a_{30}$ | $a_{46}$ | $a_{62}$ |
| $a_{10}$ | $a_{26}$ | $a_{42}$ | $a_{58}$ |
| $a_6$ | $a_{22}$ | $a_{38}$ | $a_{54}$ |
| $a_2$ | $a_{18}$ | $a_{34}$ | $a_{50}$ |

| | | | |
|---|---|---|---|
| $a_{13}$ | $a_{29}$ | $a_{45}$ | $a_{61}$ |
| $a_9$ | $a_{25}$ | $a_{41}$ | $a_{57}$ |
| $a_5$ | $a_{21}$ | $a_{37}$ | $a_{53}$ |
| $a_1$ | $a_{17}$ | $a_{33}$ | $a_{49}$ |

| | | | |
|---|---|---|---|
| $a_{63}$ | $a_{62}$ | $a_{61}$ | $a_{60}$ |
| $a_{59}$ | $a_{58}$ | $a_{57}$ | $a_{56}$ |
| $a_{55}$ | $a_{54}$ | $a_{53}$ | $a_{52}$ |
| $a_{51}$ | $a_{50}$ | $a_{49}$ | $a_{48}$ |

Along Y axis Plates Distribution,

| | | | |
|---|---|---|---|
| $a_{15}$ | $a_{31}$ | $a_{47}$ | $a_{63}$ |
| $a_{14}$ | $a_{30}$ | $a_{46}$ | $a_{62}$ |
| $a_{13}$ | $a_{29}$ | $a_{45}$ | $a_{61}$ |
| $a_{63}$ | $a_{62}$ | $a_{61}$ | $a_{60}$ |

| | | | |
|---|---|---|---|
| $a_{11}$ | $a_{27}$ | $a_{43}$ | $a_{59}$ |
| $a_{10}$ | $a_{26}$ | $a_{42}$ | $a_{58}$ |
| $a_9$ | $a_{25}$ | $a_{41}$ | $a_{57}$ |
| $a_{59}$ | $a_{58}$ | $a_{57}$ | $a_{56}$ |

| | | | |
|---|---|---|---|
| $a_7$ | $a_{23}$ | $a_{39}$ | $a_{55}$ |
| $a_6$ | $a_{22}$ | $a_{38}$ | $a_{54}$ |
| $a_5$ | $a_{21}$ | $a_{37}$ | $a_{53}$ |
| $a_{55}$ | $a_{54}$ | $a_{53}$ | $a_{52}$ |

| | | | |
|---|---|---|---|
| $a_3$ | $a_{19}$ | $a_{35}$ | $a_{51}$ |
| $a_2$ | $a_{18}$ | $a_{34}$ | $a_{50}$ |
| $a_1$ | $a_{17}$ | $a_{33}$ | $a_{49}$ |
| $a_{51}$ | $a_{50}$ | $a_{49}$ | $a_{48}$ |

Along Z Axis 4 plates Distribution,

| | | | |
|---|---|---|---|
| $a_{15}$ | $a_{31}$ | $a_{47}$ | $a_{63}$ |
| $a_{11}$ | $a_{27}$ | $a_{43}$ | $a_{59}$ |
| $a_7$ | $a_{23}$ | $a_{39}$ | $a_{55}$ |
| $a_3$ | $a_{19}$ | $a_{35}$ | $a_{51}$ |

| | | | |
|---|---|---|---|
| $a_{14}$ | $a_{30}$ | $a_{46}$ | $a_{62}$ |
| $a_{10}$ | $a_{26}$ | $a_{42}$ | $a_{58}$ |
| $a_6$ | $a_{22}$ | $a_{38}$ | $a_{54}$ |
| $a_2$ | $a_{18}$ | $a_{34}$ | $a_{50}$ |

| | | | |
|---|---|---|---|
| $a_{13}$ | $a_{29}$ | $a_{45}$ | $a_{61}$ |
| $a_9$ | $a_{25}$ | $a_{41}$ | $a_{57}$ |
| $a_5$ | $a_{21}$ | $a_{37}$ | $a_{53}$ |
| $a_1$ | $a_{17}$ | $a_{33}$ | $a_{49}$ |

| | | | |
|---|---|---|---|
| $a_{63}$ | $a_{62}$ | $a_{61}$ | $a_{60}$ |
| $a_{59}$ | $a_{58}$ | $a_{57}$ | $a_{56}$ |
| $a_{55}$ | $a_{54}$ | $a_{53}$ | $a_{52}$ |
| $a_{51}$ | $a_{50}$ | $a_{49}$ | $a_{48}$ |

Fig. 2. Axis Wise Plate Arrangement

Therefore, diffusion of the text can be done using rotation or shifting of elements of the above plates or original plates specified by the 8 bits key to get the cipher text.

### B. Key Bits Distribution

The diffusion of the text can be done using rotation 90, 180 or 270 degree or shifting of elements of the above plates or original plates specified by the 8 bits key to get the cipher text. Each round key is 8 bits long where 2 bits define axis, 4 bits define plate number and last 2 bits express types of rotation of the plate.

TABLE I.

KEY 8 BITS DISTRIBUTION

| **Rotation Degree (2 bits)** | | **Plate Number selection (4 bits)** | | | | **Axis (2 Bits)** | |
|---|---|---|---|---|---|---|---|
| $R_1$ | $R_0$ | $P_3$ | $P_2$ | $P_1$ | $P_0$ | $A_1$ | $A_0$ |

### C. Rotation Policy Depending on Key Bits

The rotation policy is defined as following table:

TABLE II.

ROTATION POLICY

| ***Rotation (2 bits)*** | | | ***Plate Number (4 bits)*** | | | | ***Axis (2 bits)*** | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | ***Plate Row no*** | ***Plate No*** | | | | | |
| 0 | 0 | $90^0$ clockwise | After selecting any plate, 4 rows are counted as 00,01,10, 11 | 0 | 0 | Plate 1 | 0 | 0 | X axis |
| 0 | 1 | $180^0$ clockwise | | 0 | 1 | Plate 2 | 0 | 1 | Y axis |
| 1 | 0 | $270^0$ Clockwise | | 1 | 0 | Plate 3 | 1 | 0 | Z axis |
| 1 | 1 | 1, 2 or 3 bits circular shifts rotation determined by Axis bits | | 1 | 1 | Plate 4 | 1 | 1 | X to Z shift |

The rotation and axis can be determined by subkey to get the final value of S-Box. Therefore, the encryption process is completed to a finite number of rounds to rotate the specific plane by 90, 180 or 270 degree along X, Y and Z axis. The decryption process is similarly done in the reverse way of the encryption technique.

TABLE III.

THE PROPOSED 3D S-BOX

| IN | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OUT | 6 | E | F | 1 | D | B | 8 | 0 | 9 | 2 | 5 | C | 3 | 4 | A | 7 |

## IV. CONCLUSION

The work has been proposed to design a composite 3D S-Box where we use 3D shift rotation to enhance the security of lightweight algorithm. The composite field S-Box is a pipelining design which reduced the number of gates as well as area with security. The security is further enhanced using 3D shift rotation which gives better result compared to 2D S-Box. Moreover, the proposed 4X4 S-Box provides less gate area compared to 8x8 designs which is suitable for IoT / mHealth applications. The future work will be done on testing different performance analysis like linear cryptanalysis, differential cryptanalysis, key sensitivity test, bit error test and randomness test as per NIST recommendation.

## REFERENCES


[1] V. A. Thakor, M. A. Razzaque, M.R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," IEEE, vol. 9, 2021.

[2] S. Kubler, J. Robert, A. Hefnawy, K. Framling, C. Cherifi, and A. Bouras, "Open IoT ecosystem for sporting event management," IEEE Access, vol. 5, pp. 7064-7079, 2017

[3] M. Marjani, F. Nasaruddin, A. Gani, and A. Karim, "Big IoT Data analytics: Architecture, opportunities, and open research challenges," IEEE Access, vol. 5, pp. 5247-5261, 2017.

[4] A. A. Zakaria, A. H. Azni, F. Ridzuan, N. H. Zakaria, M. Daud, "Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT," IEEE Access, 2020

[5] G. Yang, B. Zu, V. Suder, M. D. Aagaard and G. Gong," The Simeck Family of Lightweight Block Ciphers," International Workshop on Cryptographic Hardware and Embedded Systems, 2015.

[6] R. A. F. Lustro, A. M. Sison and R. P. Medina," Performance Analysis of Enhanced SPECK Algorithm," Proceedings of the 4th International Conference on Industrial and Business Engineering, 2018.

[7] P. T. An, N. D. Hoang, and N. K. Linh, "An efficient improvement of gift wrapping algorithm for computing the convex hull of a finite set of points in ℝn$\mathbb {R}^{n}," Springer, 2020.

[8] X. Dong and Y. Shen, "Cryptanalysis of Reduced-Round Midori64 Block Cipher," Computer Science, Simentic Scholar, 2015.

[9] A. Baysel, and S. Sahin, "RoadRunneR: A Small and Fast Bitslice Block Cipher for Low Cost 8-Bit Processors," LightSec Conference , Germany, 2015.

[10] W. Fang, Q. Zang, M. Liu, Q. Liu, and P. Xia, "Earning Maximization with Quality of Charging Service Guarantee for IoT Devices," IEEE Internet of Things Journal, 2018.

[11] C. Beierle, J. Jean, S. Kolbl, G. Leander, and A. Moradi, "The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS," Annual International Cryptology Conference, Springer, 2016.

[12] M. A. Philip, V. Vaithiyanathan, and K. Jain, "Implementation analysis of rectangle cipher and its variant," in Proc. 3rd IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT), May 2018, pp. 474-479.

[13] H. Liang and M. Wang, "Cryptanalysis of the Lightweight Block Cipher BORON," Security and Communication Networks, 2019.

[14] D. Dinu, L. Perrin, " SPARX: a group of arx-based absolutely light-weight rectangular figures provably comfortable in the direction of right away and differential assaults," strategies of Asiacrypt16,2017.

[15] J. Wang, C. Jiang, T. Q. S. Quek, X. Wang, and Y. Ren, "The value strength aided information diffusion in socially-aware mobile networks," IEEE Access, vol. 4, pp. 3907-3919, 2016.

[16] W. Zhang, Z. Bao, V. Rijmen, and M. Liu, "A new classification of 4-bit optimal S-boxes and its application to PRESENT, RECTANGLE and SPONGENT," in Proc. Int. Workshop Fast Softw. Encryption, 2015, pp. 494-515.

[17] H. Yan, Y. Luo, M. Chen, and X. Lai, "New observation on the key schedule of RECTANGLE," Sci. China Inf. Sci., vol. 62, no. 3, Mar. 2019, Art. no. 032108.

[18] A. Satoh, S. Morioka, K. Takano, S. Munetoh,"A compact Rijndael hardware architecture with S-box optimization," Asiacrypt 2001, 2248, 239-254.

[19] A. Satoh, S. Morioka, "Hardware-focused performance comparison for the standard block ciphers AES, CAMELIA, and Triple-DES," in International Conference on Information Security; Springer: Berlin/Heidelberg, Germany, 2003; pp. 252-266.

[20] M. F. Mushtaq, S. Jamel, S. Radhiah, U. Akram, and M. Mat, "Keyschedule algorithm using 3-Dimensional hybrid cubes for block cipher,"Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 8, pp. 427-442, 2019.

[21] A. Prathiba, V. S. K. Bhaaskaran,," Lightweight S-Box Architecture for Secure Internet of Things," MDPI, Information., vol. 9, 2018.

[22] L. Z. Rong, Z. Yiqi , Z. Chao, J. Gang," Low-power and area-optimized VLSI implementation of AES coprocessor for Zigbee system," J. China Univ. Posts Telecommun. 2009, 16, 89-94.

[23] T. Good, M. Benaissa, "692-nW Advanced Encryption Standard (AES) on a 0.13-µm CMOS," IEEE Trans. VeryLarge Scale Integr. Syst. 2010, 18, 1753–1757.

[24] 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 Trans. Very Large Scale Integr. Syst. 2012, 20, 1151–1155.

[25] X. Zhang, K.K. Parhi," High-speed VLSI architectures for the AES algorithm. IEEE Trans," Very Large Scale Integr. Syst. 2004, 12, 957–967.

[26] D. Canright, "A very compact S-box for AES," in International Workshop on Cryptographic Hardware and Embedded Systems," Springer: Berlin/Heidelberg, Germany, 2005; pp. 441–455.

[27] A. Rudra, P.K. Dubey, C.S. Jutla, V. Kumar, J.R. Rao, P. Rohatgi, "Efficient Rijndael encryption implementation with composite field arithmetic," CHES 2001, 2162, 171–184.

[28] J. Nakahara, ''3D: A three-dimensional block cipher,'' in Proc. Int. Conf. Cryptol. Netw. Secur. Berlin, Germany: Springer, 2008, pp. 252–267.

[29] P. R. Suri and S. S. Deora, ''A Cipher based on 3D Array Block Rotation,'' IJCSNS International Journal of Computer Science and Network Security., vol. 10, 2010.

[30] P. R. Suri and S. S. Deora, ''3D array block rotation cipher: An improvement using lateral shift,'' Global J. Comput. Sci. Technol., vol. 11, no. 19,pp. 17–23, 2011.