An S-box Design Using Irreducible Polynomial with Affine Transformation for Lightweight Cipher

Muhammad Rana(✉), Quazi Mamun, and Rafiqul Islam

Charles Sturt University, Bathurst, NSW 2678, Australia
{mrana,qmamun,mislam}@csu.edu.au

Abstract. Traditional cryptographic block cipher algorithms are often unsuitable for low-resource profiled IoT (Internet of Things) devices. A lightweight cryptographic algorithm is thus mandated. The S boxes are often called the heart of a cryptographic protocol, as a considerable amount of resource and time complexities are associated with the design of an S box. A lightweight S box will consume less memory, less power and less time, ensuring a high-level Shanon's property of confusion. This paper proposes a lightweight S box design to meet all the requirements of lightweight cryptographic ciphers. The proposed method applies a couple of transformations- the multiplicative inverse in the Galois field (2^4) and affine transformations on selected irreducible polynomials to create 4×4 S-boxes. Several cryptanalyses such as balance test, bijection property, difference distribution table test, and Boomerang Connectivity were performed to demonstrate the robust characteristics of the proposed method.

Keywords: Block cipher · Cryptanalysis · Internet of Things (IoT) · Irreducible polynomial · S-box

1 Introduction

Block cipher is one of the most popular symmetric algorithms use to encrypt the plaintext to ensure secure data transfer by providing confusion and diffusion properties. The substitution box (S-box) provide Shanon's confusion property to hide the relationship between plaintext, ciphertext and key [1]. Henceforth, designing a robust S-box is essential for a reliable and robust cipher [2]. However, for example, the Advanced Encryption System (AES) S-box consume more time and memory. Subsequently, an S-box needs to design for low resource IoT devices.

An S-box can be split into two categories such as dynamic and static. In the case of dynamic, the S-box changes regularly in each session, making the cipher harder to break. However, the same S-box uses in every session in the static state, which is less secure but require less memory and computational power [3]. Latin Square S-box method [4] provide the increased level of security of the block cipher and requires more memory which IoT devices cannot effort. On the contrary, it is easy to identify the

X. Yuan et al. (Eds.): QShine 2021, LNICST 402, pp. 214–227, 2021.
https://doi.org/10.1007/978-3-030-91424-0_13

relationship between plaintext, key, and ciphertext from a static S-box cipher; thus, data communication is less secure.

Therefore, it is challenging to trade-off between security and memory consumption of S-box to secure communication between the resource-constrained IoT devices. This paper considers constructing an S-box using the algebraic method according to specific techniques, likewise Boolean functions, affine transformations, and nonlinear equations. This method involves an S-box generation is based on the selected irreducible polynomial. In this technique, S-box production includes a 4-bit multiplicative inverse from a four-degree irreducible polynomial followed by 4×4 binary affine transformations.

Several approaches have been initiated to generate an S-box such as Algebraic techniques [5], Analytical approach [6], Chaos-based [7], Cellular Automata [8], Dynamic key-dependent [9], the Heuristic method [10], Neural networks [11] Pomaranch [12], and Zhongtang system [13]. Atani et al. [14] describe the Cellular automata-based S-boxes., In [15], the Hyperchaotic system describes generating the S-box. Chaotic maps and cuckoo search algorithm based S-box propose by Wang et al. [16]. However, most methods are energy-consuming and may not be appropriate for low resourced IoT devices. This paper demonstrates the S-boxes generation applying an algebraic method that uses nonlinear irreducible polynomials $m_1(x) = 1 + x + x^4$, $m_2(x) = 1 + x^3 + x^4$, and $m_3(x) = 1 + x + x^2 + x^3 + x^4$. Based on these polynomials, multiplicative inverse tables are created. Nonlinear based block cipher algorithms secure the round transformation [17]. An affine transformation is applied to each component in the multiplicative inverse table to produce a robust S-box. This method introduces a compact S-box derived from the algebraic design and shows strong defiance against linear and dynamic analysis.

Sahoo et al. [19] use the affine matrix and reduce the time complexity of AES. Likewise, Affine matrix transformation decreases the time complexity of the S-box of AES cipher [3]. AES hardware requirement is significantly high, which resource-constrained devices may not effort, implemented in an 8-bit S-box as a 6*16 table. Unfortunately, an 8-bit S-box necessitates a relatively larger hardware area and memory than 4-bit S-box. Therefore 8-bit S-box is impractical for the lightweight block cipher [18]. The 4-bit S-box has typically used a much more cost-effective hardware area than an 8-bit S-box. Consequently, most lightweight block ciphers use a 4-bit substitution box such as RECTANGLE, PRESENT, LED, and GiFT [19].

In this paper, we design an S-box which will be suitable for resource-constrained devices. We suggested an S-box creation process based on 4×4 bits to fit the best in a lightweight cipher. We use the irreducible polynomial equation and affine matrix in this construction method. Three steps are involved in this process. Firstly, find out the irreducible polynomial equation from the four-degree polynomial and create S-box from them. Secondly, take the best affine matrix. Finally, crate the S-boxes with the combination of multiplicative inverse and affine matrix. Empirical results show the suggested S-box offers robust defiance to statical and differential cryptanalysis.

Rest of the paper is arranged as follows: Sect. 2 explains the proposed method with detailed descriptions and the steps of the design process. In Sect. 3, we discuss the efficiency of the proposed S-box design with balanced, bijection, difference distribution tables and boomerang connectivity table. Finally, the conclusion is illustrated in Sect. 4.

2 The Proposed S-box

This section demonstrates the proposed technique to create a cryptographically strong S-box with nominated irreducible polynomials. The three steps involved in the method:

1. Create a multiplicative inverse table from a hexadecimal table.
2. Generate S-box by transforming the affine matrix.
3. Select irreducible polynomial equation and generate the hexadecimal table.

2.1 Select Irreducible Polynomial Equation and Generate the Hexadecimal Table

Figure 1 indicates the selection technique of the irreducible polynomials. The irreducible polynomial has a diffusion property and makes a nonlinear premutation function. This system allocates input bits to output bits in a nonlinear way.

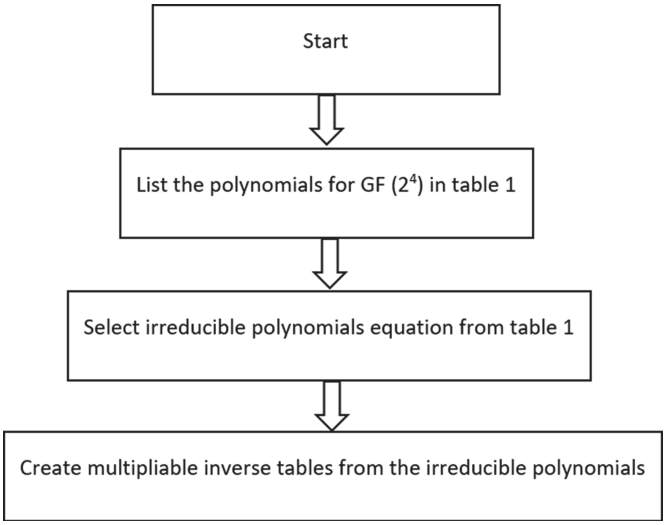

Fig. 1. Flowchart to create a multiplicative inverse table

We found three irreducible polynomials from $GF(2^4)$ such as $m_1(x) = x^4 + 1, m_2(x) = x^4 + x^3 + 1,$ and $m_3(x) = x^4 + x^3 + x^2 + x + 1$. Galois field $GF(2^4)$, also noted as F_2^4 contains $2^4 = 16$ elements. F_2^4 is the quotient ring $F_2[X]/(x^4 = x + 1)$ of the polynomial ring generated by $(x^4 = x + 1)$ in the field of order 2^4. $GF(2^4)$ elements list can be produced on the polynomial with the defining primitive polynomial.

$a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$, where $a_i \in$ for $i = 0, 1, 2, 3$ and α is the primitive root of this field.

Table 1. The elements for $x^4 + x + 1$ irreducible polynomial of Galois field $GF(2^4)$

GF (2^4) elements for $x^4 + x + 1$				
$\alpha^4 + \alpha + 1 = 0$	$\alpha^4 = \alpha + 1$			
$\alpha^5 = \alpha^4.\alpha$	$\alpha^5 = (\alpha + 1).\ \alpha$	$\alpha^5 = \alpha^2 + \alpha$		
$\alpha^6 = \alpha^5.\alpha$	$\alpha^6 = (\alpha^2 + \alpha).\ \alpha$	$\alpha^6 = \alpha^3 + \alpha^2$		
$\alpha^7 = \alpha^6.\alpha$	$\alpha^7 = (\alpha^3 + \alpha^2).\ \alpha$	$\alpha^7 = \alpha^4 + \alpha^3$	$\alpha^7 = \alpha^3 + \alpha + 1$	
$\alpha^8 = \alpha^7.\alpha$	$\alpha^8 = (\alpha^3 + \alpha + 1).\ \alpha$	$\alpha^8 = \alpha^4 + \alpha^2 + \alpha$	$\alpha^8 = \alpha + 1 + \alpha^2 + \alpha$	$\alpha^8 = \alpha^2 + 1$
$\alpha^9 = \alpha^8.\alpha$	$\alpha^9 = (\alpha^2 + 1).\ \alpha$	$\alpha^9 = \alpha^3 + \alpha$		
$\alpha^{10} = \alpha^9.\alpha$	$\alpha^{10} = (\alpha^3 + \alpha).\ \alpha$	$\alpha^{10} = \alpha^4 + \alpha^2$	$\alpha^{10} = (\alpha + 1) + \alpha^2$	$\alpha^{10} = \alpha^2 + \alpha + 1$
$\alpha^{11} = \alpha^{10}.\alpha$	$\alpha^{11} = (\alpha^2 + \alpha + 1).\ \alpha$	$\alpha^{11} = (\alpha^2 + \alpha + 1).\ A$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$	
$\alpha^{12} = \alpha^{11}.\ \alpha$	$\alpha^{12} = (\alpha^3 + \alpha^2 + \alpha).\ \alpha$	$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha^2$	$\alpha^{12} = \alpha + 1 + \alpha^3 + \alpha^2$	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^{13} = \alpha^{12}.\ \alpha$	$\alpha^{13} = (\alpha^3 + \alpha^2 + \alpha + 1).\ \alpha$	$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	$\alpha^{13} = \alpha + 1 + \alpha^3 + \alpha^2 + \alpha$	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^{14} = \alpha^{13}.\ \alpha$	$\alpha^{14} = (\alpha^3 + \alpha^2 + 1).\ \alpha$	$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha$	$\alpha^{14} = \alpha + 1 + \alpha^3 + \alpha$	$\alpha^{14} = \alpha^3 + 1$
$\alpha^{15} = \alpha^{14}.\ \alpha$	$\alpha^{15} = (\alpha^3 + 1).\ \alpha$	$\alpha^{15} = \alpha^4 + \alpha$	$\alpha^{15} = \alpha + 1 + \alpha$	$\alpha^{15} = 1$

$GF(2^4)$ is a field; therefore, every component has a unique multiplicative inverse, except the zero. Based on these chosen irreducible polynomials, their elements, binary representation, and multiplicative inverse tables are created and are given in Tables 1, 2, and 3.

The non-zero elements of the field are typically denoted by adding a star sign on the upper right $F^*_{2^4} = F_{2^4} - \{0\}$ form a multiplicative cycle group. $F^*_{2^4}$ can be generated by x i.e. $F^*_{2^4} = (x)$.

2.2 Generating the Multiplicative Inverse Table

The S-Box is considered with the multiplicative inverse over the Galois Field $GF\left(2^4\right)$ using an irreducible polynomial. The multiplicative inverses m_1, m_2 and m_3 are created from irreducible polynomials $m_1(x)$, $m_3(x)$, and $m_3(x)$. Three S-boxes have been produced from the multiplicative inverse of four-degree irreducible polynomials presented in Tables 4, 5 and 6.() 10, 11 and 12.

Table 2. Binary and hexadecimal representation of $m_1(x) = x^4 + x + 1$ irreducible polynomial

Power representation	Polynomial representation				4-Tuple representation				Hexadecimal
	α^3	α^2	α	1	α^3	α^2	α	1	
0					0	0	0	0	0
1				1	0	0	0	1	1
α			α		0	0	1	0	2
α^2		α^2			0	1	0	0	4
α^3	α^3				1	0	0	0	8
α^4			α	1	0	0	1	1	3
α^5		α^2	α		0	1	1	0	6
α^6	α^3	α^2			1	1	0	0	C
α^7	α^3		α	1	1	0	1	1	B
α^8		α^2		1	0	1	0	1	5
α^9	α^3		α		1	0	1	0	A
α^{10}		α^2	α	1	0	1	1	1	7
α^{11}	α^3	α^2	α		1	1	1	0	E
α^{12}	α^3	α^2	α	1	1	1	1	1	F
α^{13}	α^3	α^2		1	1	1	0	1	D
α^{14}	α^3			1	1	0	0	1	9

2.3 Affine Transformation and S-box Creation

An affine transformation is used to obtain a robust S-box. This transformation relocates the elements of the S-box. However, the resultant S-box properties remain unchanged. This technique improves the complexity of the algebraic expression of an S-box, which transform the S-box stronger against interpolation attacks and foundation for the protection against differential attacks [20].

Affine mapping is defined in $GF(2^4)$ as $\beta_i = \alpha\, \beta_i^{'} + \gamma_{\,\mathrm{I}}$, where, $\gamma_{\,\mathrm{I}}$ is the addition of a 4-bit vector constant, α is an invertible 4×4 (nxn) matrix [21]. Here$(\beta_3^{'}, \beta_2^{'}, \ldots\ldots, \beta_0^{'})$ are the multiplicative inverse of the byte at the input of the S-box and $(\beta_3, \beta_2, \ldots\ldots, \beta_0)$ are the byte at the output of the S-box. In a matrix, an affine matrix is formulated in Eq. 1.

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{bmatrix} = \begin{bmatrix} 0\,1\,1\,1 \\ 1\,0\,1\,1 \\ 1\,1\,0\,1 \\ 1\,1\,1\,0 \end{bmatrix} \begin{bmatrix} \beta_0' \\ \beta_1' \\ \beta_2' \\ \beta_3' \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \tag{1}$$

The following three affine transformations to assemble in $GF(2^4)$ [22].

Table 3. The power generator and proposed multiplicative inverse for $\boldsymbol{m}_1(\boldsymbol{x}) = \boldsymbol{x}^4 + \boldsymbol{x} + 1$ irreducible polynomial

I	$P(\alpha) \in GF(2^4)$	$P(\alpha) \in GF\left(2^4\right)$ bin	Multiplicative Inverse	Multiplicative Inv. bin	Hexadecimal
α^0	1	0001	1	0001	1
α^1	α	0010	$\alpha^3 + 1$	1001	9
α^2	α^2	0100	$\alpha^3 + \alpha^2 + 1$	1101	D
α^3	α^3	1000	$\alpha^3 + \alpha^2 + \alpha + 1$	1111	F
α^4	$\alpha + 1$	0011	$\alpha^3 + \alpha^2 + \alpha$	1110	E
α^5	$\alpha^2 + \alpha$	0110	$\alpha^2 + \alpha + 1$	0111	7
α^6	$\alpha^3 + \alpha^2$	1100	$\alpha^3 + \alpha$	1010	A
α^7	$\alpha^3 + \alpha + 1$	1011	$\alpha^2 + 1$	0101	5
α^8	$\alpha^2 + 1$	0101	$\alpha^3 + \alpha + 1$	1011	B
α^9	$\alpha^3 + \alpha$	1010	$\alpha^3 + \alpha^2$	1100	C
α^{10}	$\alpha^2 + \alpha + 1$	0111	$\alpha^2 + \alpha$	0110	6
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110	$\alpha + 1$	0011	3
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111	α^3	1000	8
α^{13}	$\alpha^3 + \alpha^2 + 1$	1101	α^2	0100	4
α^{14}	$\alpha^3 + 1$	1001	α	0010	2

Affine matrix 1 **Affine matrix 2**

$$\begin{bmatrix}\beta_0\\ \beta_1\\ \beta_2\\ \beta_3\end{bmatrix} = \begin{bmatrix}0&1&1&1\\ 1&0&1&1\\ 1&1&0&1\\ 1&1&1&0\end{bmatrix}\begin{bmatrix}\beta_0'\\ \beta_1'\\ \beta_2'\\ \beta_3'\end{bmatrix} + \begin{bmatrix}1\\ 1\\ 0\\ 0\end{bmatrix} \quad \begin{bmatrix}\beta_0\\ \beta_1\\ \beta_2\\ \beta_3\end{bmatrix} = \begin{bmatrix}1&0&1&1\\ 1&1&0&1\\ 1&1&1&0\\ 0&1&1&1\end{bmatrix}\begin{bmatrix}\beta_0'\\ \beta_1'\\ \beta_2'\\ \beta_3'\end{bmatrix} + \begin{bmatrix}1\\ 0\\ 0\\ 1\end{bmatrix}$$

Affine matrix 3

$$\begin{bmatrix}\beta_0\\ \beta_1\\ \beta_2\\ \beta_3\end{bmatrix} = \begin{bmatrix}1&1&0&1\\ 1&1&1&0\\ 0&1&1&1\\ 1&0&1&1\end{bmatrix}\begin{bmatrix}\beta_0'\\ \beta_1'\\ \beta_2'\\ \beta_3'\end{bmatrix} + \begin{bmatrix}0\\ 0\\ 1\\ 1\end{bmatrix}$$

We are transforming irreducible polynomial $x^4 + x + 1$ using affine matrix 1, irreducible polynomial $x^4 + x^3 + 1$ using affine matrix 2 and irreducible polynomial

Table 4. S-Box created from $x^4 + x + 1$ multiplicative inverse at $GF(2^4)$

4-bit value at $GF\left(2^4\right)$	Multiplicative inverse	x	$m_1(x)$
0000	0000	0	0
0001	0001	1	1
0010	1001	2	9
0011	1110	3	E
0100	1101	4	D
0101	1011	5	B
0110	0111	6	7
0111	0110	7	6
1000	1111	8	F
1001	0010	9	2
1010	1100	A	C
1011	0101	B	5
1100	1010	C	A
1101	0100	D	4
1110	0011	E	3
1111	1000	F	8

$x^4 + x^3 + x^2 + x + 1$ using affine matrix 3. Table 7 shows the three new S-boxes using three affine matrixes by three irreducible polynomials.

3 Performance Analysis of Proposed S-box

The nonlinear transformation is an essential criterion in modern cipher. It should provide a robust cryptographic character against different cryptanalyses such as Balance, Bijection, Difference Distribution Table (DDT), and Boomerang Connectivity Table (BCT), which will be discussed in this chapter.

3.1 Balance and Bijective

A Boolean function $S : GF(2^n) \rightarrow GF(2)$ is called balanced when the number of ones and zeros are equal in the output set in the corresponding truth table. Two Boolean functions *XOR* and *AND* defined as follows:

$$S_1 = \oplus : GF\left(2^2\right) \rightarrow GF(2)$$

$$S_2 = . : GF\left(2^2\right) \rightarrow GF(2)$$

Table 5. S-box created from $x^4 + x^3 + 1$ multiplicative inverse at $GF\left(2^4\right)$

4-bit value at $GF\left(2^4\right)$	Multiplicative inverse	x	$m_2(x)$
0000	0000	0	0
0001	0001	1	1
0010	1100	2	C
0011	1000	3	8
0100	0110	4	6
0101	1111	5	F
0110	0100	6	4
0111	1110	7	E
1000	0011	8	3
1001	1101	9	D
1010	1011	A	B
1011	1010	B	A
1100	0010	C	2
1101	1001	D	9
1110	0111	E	7
1111	0101	F	5

The following truth table with two variables x_1 and x_2 can define this (Table 8)

The *XOR* function has an equal number of zeros and ones; thus, this is balanced. On the other hand, the fourth column denotes *AND* function, which is not balanced.

If all linear combinations of columns are balanced, then a Boolean function $S : GF\left(2^2\right) \rightarrow GF(2)$ is called bijective. According to Tang et al. [23], the bijective property is satisfied with an (nxn) S-box if the Boolean functions f_i(for $1 \leq i \leq n$) of S-box can be represented, where $c_i \in \{0.1\}$ for $(c_1, c_2, ...c_3) \neq (0, 0, \ldots.., 0)$ and the Hamming weight is *Hwt* [24]

$$Hwt\left(\sum_{i=1}^{n} c_i f_i\right) = 2^{n-1}$$

According to the above calculation, sage math [25], a free and open-source mathematics software, can calculate the balance for different S-boxes by the following command. The analysis shows the S-box$_1$, S-box$_2$, and S-box$_3$ are balanced and bijective.

Table 6. S-box created from $x^4 + x^3 + x^2 + x + 1$ multiplicative inverse at $GF\left(2^4\right)$

4-bit value at $GF\left(2^4\right)$	Multiplicative inverse	x	$m_3(x)$
0000	0000	0	0
0001	0001	1	1
0010	1111	2	F
0011	1010	3	A
0100	1000	4	8
0101	0110	5	6
0110	0101	6	5
0111	1001	7	9
1000	0100	8	4
1001	0111	9	7
1010	0011	A	3
1011	1110	B	E
1100	1101	C	D
1101	1100	D	C
1110	1011	E	B
1111	0010	F	2

```
sage: S1 = SBox(3,0xd,0xa,2,1,7,0xb,5,0xc,0xe,0xf,6,9,8,0,4)
sage: S1.is_balanced()
True

sage: S2 = SBox(9,0xe,0xf,2,0xa,6,4,1,0,8,0xb,0xc,7,5,0xd,3)
sage: S2.is_balanced()
True
sage: S3 = SBox(0xc,7,3,6,1,5,9,0xa,2,0xe,0,8,4,0xf,0xd,0xb)
sage: S3.is_balanced()
True
```

3.2 Difference Distribution Table and Boomerang Connectivity Table

Differential cryptanalysis is one of the essential cryptographical methods for evaluating the security of block ciphers. The defiance against differential cryptanalysis is highly reliant on the non-linearity structures of the predefined S-box.

$S : \{0, 1\}^n \rightarrow \{0, 1\}^n$, n-bit S-box, the differential propagations of S are typically represented in the $2^n x 2^n$ Difference Distribution table (DDT)τ, value for any pair (Δ_i, Δ_0)

Table 7. Three S-boxes after an affine transformation

4-bit value at $GF\left(2^4\right)$	S-box$_1$ binary	**S**-box$_1$ hex	S-box$_2$ binary	S-box$_2$ hex	S-box$_3$ binary	S-box$_3$ hex
0000	0011	**3**	1001	**9**	1100	**C**
0001	1101	**D**	1110	**E**	0111	**7**
0010	1010	**A**	1111	**F**	0011	**3**
0011	0010	**2**	0010	**2**	0110	**6**
0100	0001	**1**	1010	**A**	0001	**1**
0101	0111	**7**	0110	**6**	0101	**5**
0110	1011	**B**	0100	**4**	1001	**9**
0111	0101	**5**	0001	**1**	1010	**A**
1000	1100	**C**	0000	**0**	0010	**2**
1001	1110	**E**	1000	**8**	1110	**E**
1010	1111	**F**	1011	**B**	0000	**0**
1011	0110	**6**	1100	**C**	1000	**8**
1100	1001	**9**	0111	**7**	0100	**4**
1101	1000	**8**	0101	**5**	1111	**F**
1110	0000	**0**	1101	**D**	1101	**D**
1111	0100	**4**	0011	**3**	1011	**B**

Table 8. The truth table shows *XOR*, *AND*

x_1	x_2	$x_1 \oplus x_2$	$x_1 \cdot x_2$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

is stored in the corresponding entry $\tau(\Delta_i, \Delta_0)$ of DDT, which denotes the input difference Δ_i propagates to the output difference Δ_0 with the likelihood, the highest entry in the table is named the differential uniformity of S [26].

$$\#\left\{x \in \{0, 1\}^n \middle| S_{(x)}S(x\Delta_i) = \Delta_0\right.$$

$$\tau(\Delta_i, \Delta_o)\backslash 2^n$$

The DDT for S-box$_1$ is shown in Table 9; We can observe the differential uniformity of the S-box is 4. The Boomerang Connectivity table may exploit the differential properties of diverse sections of the cipher. In the boomerang attack, E is the target cipher

Table 9. Difference Distribution Table (DDT) of S-box$_1$

Output Difference S-box$_1$																
Input Difference S-box$_1$		**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	2	2	0	2	0	2	0	2	2	0	0	0	0	4	0
	2	0	0	2	2	0	0	0	0	2	4	2	0	2	0	0	2
	3	0	4	0	0	2	0	0	2	2	0	2	0	2	2	0	0
	4	0	2	4	0	0	2	2	2	0	0	2	0	0	0	0	2
	5	0	0	0	0	4	0	2	2	0	2	0	2	2	0	0	2
	6	0	0	0	0	0	2	2	0	4	0	2	2	2	0	2	0
	7	0	0	0	2	0	0	4	2	2	0	0	0	0	2	2	2
	8	0	2	0	2	2	2	0	0	2	0	0	2	0	0	0	4
	9	0	2	0	0	0	2	0	0	0	2	0	0	2	4	2	2
	A	0	2	2	2	0	0	2	0	0	0	0	2	4	2	0	0
	B	0	0	2	2	2	4	0	2	0	0	0	0	2	0	2	0
	C	0	0	0	2	2	2	2	0	0	2	4	0	0	2	0	0
	D	0	0	2	0	2	0	0	0	0	0	2	4	0	2	2	2
	E	0	2	0	4	0	0	0	2	0	2	2	2	0	0	2	0
	F	0	0	2	0	0	2	0	4	2	2	0	2	0	2	0	0

compare to two sub-ciphers E_0 and E_1. So, $E = E_1 o E_0$. If the input difference α is propagated to the difference β by E_0 with the probability p. Then, with the probability p, the difference γ is propagated to δ by E_1. The boomerang attack can exploit the following difference with expected probability [27],

$$Pr\Big[E^{-1}(E(x) \oplus \delta) \oplus E^{-1}(E(x \oplus \alpha) \oplus \delta) = \alpha\Big] = q^2 p^2$$

E can be distinguished from a model cipher, on making around $(qp)^{-2}$ adaptive selected cipher/plain text requests.

The boomerang connectivity tale (BCT) is two-dimensional denoted by S can be represented by

$$BCT(\alpha, \beta) = \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus \beta) \oplus S^{-1}(S(x \oplus \alpha) \oplus \beta) = \alpha\}$$

Where $\alpha, \beta \in \mathbb{F}_2^n$. The S, the boomerang uniformity, is the highest value in the BCT except for the first row and the first column.

S-box$_1$ DDT and BCT are provided in Tables 9 and 10, respectively. The differential uniformity is 4, and boomerang uniformity is 16.

Table 10 shows the difference distribution table of our proposed S-box$_1$. The DDT has 16 rows, 16 columns, and 265 cells. The row and column represent the output

Table 10. Boomerang Connectivity Table (BCT) of S-box$_1$

∇_0 S-box$_1$																
Δ_i S-box$_1$		**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
	0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
	1	16	0	6	0	0	6	0	4	2	0	0	0	2	2	2	0
	2	16	0	0	0	2	0	4	2	0	0	6	2	6	0	2	0
	3	16	2	2	6	2	0	0	0	6	0	0	4	2	0	0	0
	4	16	0	0	4	0	0	2	2	6	0	0	6	0	2	0	2
	5	16	6	0	0	2	2	2	0	2	0	0	0	0	0	6	4
	6	16	0	0	0	6	2	0	0	0	6	0	2	2	4	0	2
	7	16	0	0	6	0	2	0	0	4	2	2	6	0	0	2	0
	8	16	0	2	2	6	0	2	0	0	4	0	0	0	6	2	0
	9	16	4	0	2	0	0	0	2	0	2	0	0	2	0	6	6
	A	16	0	4	2	2	6	0	6	0	0	2	0	0	0	0	2
	B	16	2	6	0	0	4	2	6	0	2	0	2	0	0	0	0
	C	16	6	2	0	0	0	0	0	0	0	2	2	0	2	4	6
	D	16	0	2	0	0	0	6	0	2	2	6	0	4	0	0	2
	E	16	2	0	0	4	0	0	2	2	6	2	0	0	6	0	0
	F	16	2	0	2	0	2	6	0	0	0	4	0	6	2	0	0

difference from 0 to F for each input difference. Zero represents the absence of that output difference for the following input difference. Too high or too low zero discloses more information concerning output difference [28]. S-box$_1$ difference distribution table indicates that it has three values 0, 2, and 4. Only one 4 find in each row and column. Consequently, S-box$_1$ can offer robust defiance alongside differential cryptoanalysis.

4 Conclusion

In this paper, we proposed a lightweight S-box design that uses algebraic methods to fulfil all of the requirements of lightweight cryptographic ciphers. This algebraic technique employs three irreducible polynomials from the Galois field $GF(2^4)$. Three multiplicative matrices, $m_1(x)$, $m_2(x)$, and $m_3(x)$ give rise to three multiplicative inverses, m_1, m_2, and m_3. Then, using affine transformations, three S-boxes, S-boxe1, S-box2, and S-box3, are constructed. The cryptographic analysis demonstrates strong resistance to differential and boomerang cryptanalysis. In the future, produced S-boxes should be subjected to further testing and utilized for lightweight block ciphers to protect network interactions between IoT resource-constrained devices. This approach creates S-boxes that are suitable for resource end devices. S-boxes can also be used to provide a lightweight block cipher for IoT network communications.

References

1. Gao, W., et al.: Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF(28)). IEEE Access **8**, 136736–136749 (2020)
2. Wang, X., et al.: A chaotic system with infinite equilibria and its S-Box constructing application. Appl. Sci. **8**(11), 2132 (2018)
3. Ibrahim, S., Abbas, A.M.: A novel optimization method for constructing cryptographically strong dynamic s-boxes. IEEE Access **8**, 225004–225017 (2020)
4. Mohamed, K., et al.: Study of S-box Properties in Block Cipher. In: International Conference on Computer, Communications, and Control Technology (I4CT) (2014)
5. Jamal, S.S., Shah, T.: A novel algebraic technique for the construction of strong substitution box. Wireless Pers. Commun. **99**(1), 213–226 (2018)
6. Radhakrishnan, S.V., Subramanian, S.: An analytical approach to S-Box generation. Comput. Electr. Eng. **39**(3), 1006–1015 (2013)
7. Özkaynak, F.: On the effect of a chaotic system in performance characteristics of chaos based s-box designs. Physica A: Stat. Mech. Appl. **550**, 124072 (2020)
8. Mariot, L., et al.: Cellular automata based S-boxes. Crypt. Commun. **11**, 41–62 (2018)
9. Partheeban, P., Kavitha, V.: Dynamic key dependent AES S-box generation with optimized quality analysis. Clust. Comput. **22**(6), 14731–14741 (2018). https://doi.org/10.1007/s10586-018-2386-6
10. Lineham, A., Gulliver, T.A.: Heuristic S-box Design. Contemporary. Eng. Sci. **1**, 147–168 (2008)
11. Noughabi, M.N.A., Sadeghiyan, B.:Design of S-boxes based on neural networks. In: 2010 International Conference on Electronics and Information Engineering (2010)
12. Isa, H., Jamil, N., Z'aba, M.R.: S-box construction from non-permutation power functions. In: 6th International Conference on Security of Information and Networks (2013)
13. Çavu¸so˘glu, Ü., et al.: A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear Dyn. **87**(2), 1081–1094 (2017)
14. Atani, R.E., Mirzakuchaki, S., Atani, S.E.:Low cost implementation of Pomaranch S-Box. In: 1st International Conference on Wireless Communication. (2009)
15. Islam, F.U., Liu, G.: Designing S-Box Based on 4D-4Wing Hyperchaotic System (2017)
16. Alhadawi, H.S., Majid, M.A., Lambić, D., Ahmad, M.: A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm. Multimedia Tools Appl. **80**(5), 7333–7350 (2020). https://doi.org/10.1007/s11042-020-10048-8
17. Dey, S., Ghosh, R.: A Review of Cryptographic Properties of 4-Bit S-Boxes with Generation and Analysis of Crypto Secure S-Boxes. Taylor & Francis Group (2019)
18. Wong, M.M., Wong, M.L.D.: New lightweight AES S-box using LFSR. In: International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Kuching, Malaysia (2014)
19. Zhang, W., Bao, Z., Rijmen, V., Liu, M.: A New Classification of 4-bit Optimal S-boxes and Its Application to PRESENT, RECTANGLE and SPONGENT. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 494–515. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48116-5_24
20. Dawood, O.A., et al.: Design a compact non-linear S-Box with multiple-affine transformations. In: Khalaf, M., Al-Jumeily, D., Lisitsa, A. (eds.) Applied Computing to Support Industry: Innovation and Technology, ACRIT 2019, Communications in Computer and Information Science, vol 1174. Springer, Cham (2020)
21. Waqas, U., et al.: Generation of AES-Like S-Boxes by Replacing Affine Matrix. In: 12th International Conference on Frontiers of Information Technology (2014)

22. Zhang, X., et al.: Hardware Implementation of Compact AES S-box. Int. J. Comput. Sci. **42**, 125–131 (2015)
23. Tang, G., Liao, X., Chen, Y.: A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons Fractals **23**(2), 413–419 (2005)
24. Song, L., Qin, X., Hu, L.: Boomerang connectivity table revisited. application to SKINNY and AES. IACR Trans. Symmetric Crypt. **1**, 118–141 (2019)
25. Stein, W.A.: *S*-Boxes and their algebraic representations. Sage 9.3 Reference Manual: Cryptography (2021)
26. Cid, C., et al.: Boomerang Connectivity Table: A New Cryptanalysis Tool. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques (2018)
27. Boura, C., Canteaut, A.: On the Boomerang Uniformityof Cryptographic Sboxes. IACR Trans. Symmetric Crypt. **3**, 290–310 (2018)
28. Dey, S., Ghosh, R.: A review of existing 4-bit crypto S-Box cryptanalysis techniques and two new techniques with 4-bit boolean functions for cryptanalysis of 4-bit crypto S-Boxes. Adv. Pure Math. **8**(3), 273 (2018)