Article

Constructing 8×8 S-Boxes with Optimal Boolean Function Nonlinearity

Phuc-Phan Duong * and Cong-Kha Pham

Posted Date: 3 September 2025

doi: 10.20944/preprints202509.0311.v1

Keywords: S-box; Boolean function; nonlinearity; cryptography; block ciphers

 doi:10.20944/preprints202509.0311.v1

Article

Constructing 8 × 8 S-Boxes with Optimal Boolean Function Nonlinearity

Phuc-Phan Duong * and Cong-Kha Pham

University of Electro-Communications (UEC), Department of Computer and Network Engineering, 1-5-1 Chofugaoka, Chofu-shi 182-8585, Tokyo, Japan

* Correspondence: duongphucphan@vlsilab.ee.uec.ac.jp

Abstract

Substitution boxes (S-Boxes) are the core components of modern block ciphers, responsible for introducing the essential nonlinearity that protects against attacks like linear and differential cryptanalysis. For an 8-bit S-Box, the highest possible nonlinearity for a balanced Boolean function is 116. The best results previously reported in the literature were only able to achieve a nonlinearity of 114.5. Our new method surpasses this prior record, generating 8×8 S-Boxes with a nonlinearity of 116. This is a significant achievement as it reaches the highest known bound for balanced functions and sets the new standard for this criterion. The approach is also highly effective, capable of producing a large number of S-Boxes, all with these optimal cryptographic properties. This ensures they are exceptionally resistant to cryptanalysis. Our S-Box construction is not only superior in nonlinearity but also performs well when evaluated against other standard cryptographic metrics, making it a leading solution for secure cipher design.

Keywords: S-box; boolean function; nonlinearity; cryptography; block ciphers

1. Introduction

In modern block cipher algorithms, the substitution box (S-Box) is the fundamental nonlinear component that provides confusion and protects against classical cryptanalytic methods such as linear cryptanalysis and differential cryptanalysis. Formally, an S-Box can be represented as a vectorial Boolean function. The cryptographic strength of an S-Box is therefore determined by the properties of these functions. Nonlinearity (NL) is the most fundamental indicator, as it measures the distance from affine functions and directly reflects resistance to linear approximation attacks.

For 8-variable Boolean functions, corresponding to 8 × 8 S-Boxes, the highest nonlinearity mathematically discovered so far for balanced functions is 116 [1–3]. However, constructing balanced S-Boxes that reach this bound has long been considered a major challenge in cryptography. Previous works based on algebraic transformations [4–16], chaotic systems [17–27], and hybrid approaches [28–37] have achieved significant progress, yet the highest reported nonlinearity has remainsed at 114.5 [29], still below the theoretical maximum.

In addition to nonlinearity, other research directions have focused on optimizing different cryptographic aspects. Several studies aim to maximize the Strict Avalanche Criterion (SAC) [38–40], while others emphasize efficiency in hardware implementation [41–47]. Research on S-Boxes has also focused on optimizing parameters related to side-channel resistance [30,48,49], while other studies target optimization against advanced cryptanalytic techniques such as the Boomerang attack [50] or Differential and Linear Branch Numbers [51].

Although previous studies have made important progress in the design of S-Boxes, the fundamental challenge of attaining the maximum possible nonlinearity for balanced 8 × 8 S-Boxes remains unresolved. In this paper, we focus on bridging these gaps by optimizing nonlinearity in conjunction with hardware efficiency. The main contributions of this work are summarized as follows:

 doi:10.20944/preprints202509.0311.v1

- A novel construction method: We developed a systematic approach for building 8×8 S-Boxes from smaller 4×4 component S-Boxes, which allows for a modular and efficient design.
- Optimal nonlinearity: The S-Boxes we constructed successfully achieve a nonlinearity of 116, reaching the theoretical maximum for 8-variable balanced Boolean functions.
- Comprehensive security analysis: Our analysis confirms that these new S-Boxes meet other critical security criteria, including the Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), Differential Avalanche Probability (DAP), and Linear Avalanche Probability (LAP).
- Practical robustness: Side-channel attack experiments show that our S-Boxes offer resistance comparable to the Advanced Encryption Standard (AES) S-Box, proving their real-world applicability.
- Efficient hardware implementation: Our S-Boxes are designed for efficient hardware resource utilization, making them ideal for systems with limited resources.

The remainder of this paper is organized as follows. Section 2 reviews related work. Section 3 presents the theoretical background of Boolean functions and S-Box design criteria. Section 4 introduces the proposed construction method. Section 5 reports the cryptographic security analysis of the generated S-Boxes and presents experimental results of side-channel attack. Section 6 evaluates the hardware performance in terms of resource efficiency. Finally, Section 7 concludes the paper.

2. Related Works

A wide range of approaches have been proposed for the construction of S-Boxes, which can broadly be categorized into algebraic-based, chaotic-based, hybrid techniques, and composition methods using smaller substitution components. Below, we present some of the most recent studies in this field.

Several studies exploit algebraic structures and mathematical transformations for S-Box construction. In [8], Möbius transformation combined with permutations was applied to design S-Boxes that enhance IoT multimedia security. The study in [9] proposed constructing S-Boxes based on power associative loops, later applied to text encryption. The work in [20] employed Delannoy-derived sequences to generate a new chaotic S-Box. Dimitrov and Baicheva [52] analyzed the classification of 8-bit to 8-bit power mappings defined by pentanomials for S-Box generation. Waheed et al. [29] introduced S-Boxes constructed through a combination of linear fractional transformation and multilayer perceptrons, achieving the best reported nonlinearity of 114.5.

Chaotic dynamical systems have also been widely adopted for constructing S-Boxes. Boobalan et al. [18] proposed dynamic S-Boxes derived from Lorenz and Chua chaotic systems for efficient image encryption. A dynamic scheme based on Mordell elliptic curves over Galois fields was presented in [7]. Group-action-based S-Box generation was described in [6]. The approach in [32] combined chaotic maps with bit-level permutations to construct S-Boxes for medical data security. Furthermore, Zhang Lijun et al. [53] introduced S-Boxes generated via quantum random walks controlled by a hyper-chaotic map. These methods provide advantages in randomness and applicability to image encryption, but the achieved nonlinearity typically remains at medium–high levels, in most cases below 112, and still far from the theoretical optimum.

Other studies combine multiple methods or apply heuristic algorithms to strengthen S-Box properties. A cost-function-based approach for efficient S-Box construction was proposed in [5], while [31] employed a hybrid population-based hill climbing algorithm, where the nonlinearity stopped at 104. The work in [30] utilized rotation symmetry combined with heuristic search to generate S-Boxes. Malik et al. [33] constructed nonlinear components in the form of S-Boxes using hybrid pseudo-random binary sequences. In addition, Song and Zhao [17] focused on S-Box designs for secure image encryption, emphasizing a balance between robustness and efficiency.

Some works explored the construction of larger S-Boxes from smaller substitution components to achieve lightweight and efficient designs. The study in [45] introduced a Feistel-based composition method, while [47] extended the analysis to both Feistel and MISTY networks, highlighting their potential for systematic generation of lightweight substitution layers. High differential and linear branch

 doi:10.20944/preprints202509.0311.v1

numbers were targeted in [51] to improve diffusion, whereas [46] investigated hardware-oriented S-Box constructions combined with masking techniques to resist side-channel attacks. More recently, Yan et al. [48] developed substitution layers based on small S-Boxes that are resilient to differential power analysis, confirming the practicality of this direction. Collectively, these contributions underline that the primary motivation of composition-based methods lies in hardware efficiency and deployability rather than maximizing theoretical cryptographic metrics.

In summary, recent research has significantly expanded the design space of S-Boxes through diverse approaches. However, the gap between the best known result (114.5) and the theoretical maximum (116) persists, leaving an open challenge that the present study aims to address.

3. Background

3.1. Boolean Functions and Nonlinearity

Boolean functions [54] are at the heart of symmetric cryptography, where they provide the nonlinearity required to secure block ciphers against algebraic and statistical attacks. An n-variable Boolean function is formally defined as a mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$, where $\mathbb{F}_2$ denotes the binary field. For an input vector $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, the function outputs a single bit $f(x) \in \{0, 1\}$. One of the most important cryptographic indicators of a Boolean function is its nonlinearity, which quantifies the minimum Hamming distance between f and the set of all affine functions. Formally, the nonlinearity of f is defined as Equation (1) [55].

$$NL(f) = \min_{g \in A_n} d_H(f, g), \tag{1}$$

where A_n is the set of affine functions in n variables and d_H is the Hamming distance. High nonlinearity ensures that f cannot be closely approximated by linear or affine expressions, thereby strengthening resistance against linear cryptanalysis. The theoretical maximum nonlinearity of an n-variable Boolean function is given by Equation (2) [55].

$$NL(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{2}$$

Bent functions represent Boolean functions that achieve the maximum possible distance from all affine functions, thereby providing the highest nonlinearity. However, a fundamental limitation is that bent functions are never balanced, which makes them unsuitable for S-Box design since balancedness is required to avoid biased outputs. Importantly, bent functions exist only when n is even. For instance, with $n = 8$, the theoretical upper bound for unbalanced Boolean functions is 120, achieved by bent functions, whereas the best attainable value for balanced functions is strictly lower, at 116 [1–3]. This bound of 116 therefore constitutes the true optimal target for the coordinate functions of an 8×8 S-Box.

The Walsh–Hadamard transform [56] is typically used to compute nonlinearity. For a Boolean function f, the Walsh spectrum is defined as Equation (3).

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle a, x \rangle}, \tag{3}$$

where $\langle a, x \rangle$ denotes the inner product of vectors a and x over $\mathbb{F}_2$. The nonlinearity can then be expressed equivalently as Equation (4).

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_f(a)|. \tag{4}$$

From this perspective, minimizing the maximum Walsh coefficient directly maximizes the nonlinearity of f. This theoretical foundation highlights why constructing balanced 8-variable Boolean functions with nonlinearity 116 has been considered one of the most difficult open problems in symmetric cryptography.

 doi:10.20944/preprints202509.0311.v1

3.2. Properties of Cryptographically Strong S-Boxes

Several well-established criteria are used to evaluate S-Box properties, including Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), Differential Approximation Probability (DAP), Linear Approximation Probability (LP) algebraic degree (AD), and some parameters related to side-channel attack, such as the Transparency Order (TO), Modified Transparency Order (MTO), Revised Transparency Order (RTO), Minimum Correlation Coefficient (MCC), Confusion Coefficient Variance (CCV), and Signal-to-Noise Ratio (SNR) [57–63]. The evaluation criteria for cryptographic S-Boxes have been presented in detail in many existing studies [21,64,65]. These metrics cover both classical cryptanalytic strength and resistance against side-channel attacks. For completeness, we provide in Table 1 a concise summary of the main properties and their desired values.

Table 1. Summary of cryptographic criteria for S-Box evaluation

Criterion	Definition / Meaning	Optimal Value
Bijectivity	One-to-one mapping between input and output, ensuring uniform distribution and balance.	Must be satisfied
NL	Distance from affine functions; higher NL strengthens resistance against linear cryptanalysis.	High
AD	Maximum degree of output Boolean functions; higher AD makes algebraic attacks harder.	High
DAP	Probability that a specific input difference leads to a specific output difference.	Low
LAP	Correlation between linear combinations of input and output bits.	Low
SAC	Probability that a single input bit flip changes each output bit.	0.5
BIC	Measures independence among output bits when an input bit is flipped.	High
TO, MTO, RTO	Indicators of resistance against DPA; lower values reduce leakage correlation.	Low
CCV, MCC	Correlation between leakage and key-dependent intermediates.	Low
SNR	Ratio of exploitable leakage to noise in side-channel signals.	Low

4. Proposed Method

4.1. Proposed Algorithm

In this study, we present a method to construct an 8×8 S-Box based on the combination of four 4×4 S-Boxes and multiplication in the subfield $GF(2^4)$. The objective of the proposed method is to exploit both the strong nonlinearity of the 4×4 lookup tables and the diffusion capability of finite field multiplication, thereby generating a mapping of sufficient complexity to resist modern cryptanalytic techniques. The algorithm takes as input an 8-bit word $x \in \{0,1\}^8$, and produces an 8-bit output $y \in \{0,1\}^8$. For computation, the input is divided into two halves: the upper nibble $x[7:4]$ and the lower nibble $x[3:0]$. Similarly, the output is represented by $y[7:4]$ and $y[3:0]$. Four independent 4×4 S-Boxes, denoted S_A, S_B, S_C, S_D, are employed in the construction. These components provide nonlinearity in each transformation step, while multiplication in $GF(2^4)$, denoted by $\otimes$, ensures strong interdependence between the two halves of the data. The upper nibble of the output is computed as Equation (5).

$$y[7:4] = \begin{cases} S_A(x[3:0]) \otimes x[7:4], & \text{if } x[7:4] \neq 0, \\ S_B(x[3:0]), & \text{if } x[7:4] = 0, \end{cases} \tag{5}$$

 doi:10.20944/preprints202509.0311.v1

that is, when the upper nibble of the input is nonzero, S_A is applied to the lower nibble and the result is multiplied with the upper nibble; otherwise, S_B is applied to the lower nibble. Next, the lower nibble of the output is computed as Equation (6).

$$y[3:0] = \begin{cases} S_C(x[7:4] \otimes y[7:4]), & \text{if } y[7:4] \neq 0, \\ S_D(x[7:4]), & \text{if } y[7:4] = 0. \end{cases} \tag{6}$$

Thus, the lower nibble depends on both halves of the input through the intermediate value $y[7:4]$, ensuring complete diffusion across the entire 8-bit word. Finally, the complete output is adjusted with a simple XOR by one ($y \leftarrow y \oplus 1$) to remove possible fixed points. This algorithm requires only two 4×4 S-Box lookups, two multiplications in $GF(2^4)$, and one XOR operation. As a result, it achieves strong nonlinearity with low implementation complexity, which is advantageous for hardware-oriented designs under resource constraints. The combination of nonlinear substitution and finite field multiplication ensures that the high and low nibbles of the data remain strongly correlated, thereby strengthening resistance against differential and linear cryptanalysis.

4.2. Experimental

To specify multiplication $\otimes$ in $GF(2^4)$, three irreducible polynomials of degree four over $GF(2)$ are employed as Equation (7).

$$f_1(x) = x^4 + x + 1, \qquad f_2(x) = x^4 + x^3 + 1, \qquad f_3(x) = x^4 + x^3 + x^2 + x + 1. \tag{7}$$

Each polynomial defines a distinct representation of the finite field, which leads to different multiplication tables and, consequently, different sets of 4×4 S-Boxes.

The 4×4 S-Boxes are generated from power mappings in the multiplicative group $GF(2^4)^*$ of order 15. A mapping $x \mapsto x^k$ is bijective if and only if $\gcd(k, 15) = 1$. Therefore, the valid exponents are $k \in \{1, 2, 4, 7, 8, 11, 13, 14\}$. Each exponent produces one distinct 4×4 S-Box. Hence, for each irreducible polynomial f_i, eight S-Boxes are obtained, denoted as $S1$ through $S8$. Table 2 lists all resulting 4×4 S-Boxes for the three polynomials.

Table 2. 4×4 S-Boxes generated from three irreducible polynomials.

Name	$f_1(x) = x^4 + x + 1$	$f_2(x) = x^4 + x^3 + 1$	$f_3(x) = x^4 + x^3 + x^2 + x + 1$
S1	0, 1, 2, 3, 4, 5, 6, 7 8, 9,10,11,12,13,14,15	0, 1, 2, 3, 4, 5, 6, 7 8, 9,10,11,12,13,14,15	0, 1, 2, 3, 4, 5, 6, 7 8, 9,10,11,12,13,14,15
S2	0, 1, 4, 5, 3, 2, 7, 6 12,13, 8, 9,15,14,11,10	0, 1, 4, 5, 9, 8,13,12 15,14,11,10, 6, 7, 2, 3	0, 1, 4, 5,15,14,11,10 2, 3, 6, 7,13,12, 9, 8
S3	0, 1, 3, 2, 5, 4, 6, 7 15,14,12,13,10,11, 9, 8	0, 1, 9, 8,14,15, 7, 6 3, 2,10,11,13,12, 4, 5	0, 1,15,14, 8, 9, 7, 6 4, 5,11,10,12,13, 3, 2
S4	0, 1,11,13, 9,14, 6, 7 12, 5, 8, 3,15, 2, 4,10	0, 1, 7, 5,12, 8, 2, 9 15, 6,10,11,14, 4,13, 3	0, 1, 4, 7,15,10, 3,14 2,11, 9, 5,12,13, 6, 8
S5	0, 1, 5, 4, 2, 3, 7, 6 10,11,15,14, 8, 9,13,12	0, 1,14,15, 2, 3,12,13 5, 4,11,10, 7, 6, 9, 8	0, 1, 8, 9, 2, 3,10,11 15,14, 7, 6,13,12, 5, 4
S6	0, 1,14, 9,11,13, 7, 6 8, 3,10, 4,12, 5, 2,15	0, 1,13, 3, 7, 5,14, 4 8,12,11,10, 9, 2, 6,15	0, 1, 2,11, 4, 7, 9, 5 8, 6,14, 3,13,12,10,15
S7	0, 1,13,11,14, 9, 6, 7 10, 4,15, 2, 8, 3, 5,12	0, 1, 6,15,13, 3, 9, 2 5, 7,10,11, 4,14,12, 8	0, 1, 8, 6, 2,11,14, 3 15,10, 5, 9,12,13, 7, 4
S8	0, 1, 9,14,13,11, 7, 6 15, 2,12, 5,10, 4, 3, 8	0, 1,12, 8, 6,15, 4,14 3,13,11,10, 2, 9, 7, 5	0, 1,15,10, 8, 6, 5, 9 4, 7, 3,14,13,12,11, 2

 doi:10.20944/preprints202509.0311.v1

During the experimentation, four S-Boxes were selected from each set of eight and assigned to S_A, S_B, S_C, and S_D in the proposed algorithm. For a single irreducible polynomial, this results in $8^4 = 4096$ possible configurations, and across the three considered polynomials the total number of generated S-Boxes reaches 12,288. The distribution of average Boolean function nonlinearities for these S-Boxes is summarized in Table 3. Among them, 2,304 S-Boxes achieve the optimal nonlinearity of 116 for all coordinate Boolean functions. This outcome highlights both the strength and flexibility of the proposed construction method, as it yields a large set of secure candidates from which practical designs can be selected. From this collection, we prioritize configurations with the lowest implementation cost, which corresponds to the case where all four component S-Boxes S_A, S_B, S_C, and S_D are identical. Using the irreducible polynomial $f_1(x) = x^4 + x + 1$, one representative configuration is obtained with four identical 4×4 S-Boxes defined as [0, 1, 9, 14, 13, 11, 7, 6, 15, 2, 12, 5, 10, 4, 3, 8]. The detailed results for this representative S-Box are presented in Table 4.

Table 3. Distribution of S-Boxes according to average Boolean function nonlinearity.

Average NL	Number of S-Boxes)
108	768
110	1536
112	3072
114	4608
116	2304

Table 4. Proposed S-Box.

i/*j*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	01	11	91	E1	D1	B1	71	61	F1	21	C1	51	A1	41	31	81
1	00	10	93	E2	D5	B4	77	66	F9	28	CB	5A	AD	4C	3F	8E
2	08	2C	18	F5	90	5D	E9	C4	D3	4E	BA	A7	72	8F	6B	36
3	0F	3A	84	1F	4B	E0	9E	A5	26	6D	73	F8	DC	C7	59	B2
4	0C	4F	2E	D0	1C	A2	F3	BD	98	86	57	79	E5	3B	CA	64
5	0A	58	B0	39	C3	1A	82	DB	65	AC	94	2D	47	7E	F6	EF
6	06	67	3D	2B	8A	FC	16	70	44	C2	E8	DE	9F	B9	A3	55
7	07	76	AF	C8	5E	49	60	17	BC	EB	22	85	33	F4	9D	DA
8	0E	8B	46	9C	2F	75	D8	52	1E	34	A9	E3	F0	6A	B7	CD
9	03	95	D9	7D	F2	C6	AA	3E	E7	13	6F	BB	54	20	8C	48
A	0D	AE	5C	63	B8	27	35	9A	C0	7F	1D	42	89	E6	D4	FB
B	04	B3	C5	87	69	9B	4D	FF	32	50	D6	14	2A	A8	EE	7C
C	0B	C9	62	4A	37	DF	24	EC	8D	B5	FE	96	1B	53	78	A0
D	05	D2	F7	A4	ED	6E	5B	88	7A	99	3C	CF	B6	15	40	23
E	02	E4	7B	BE	A6	83	CC	29	5F	FA	45	30	68	DD	12	97
F	09	FD	EA	56	74	38	BF	43	AB	D7	80	6C	CE	92	25	19

5. Security Analysis

A variety of essential criteria for evaluating the cryptographic strength of S-Boxes have been discussed in [57,58,64,65]. Instead of restating the complete mathematical formulations for these metrics, we present only the corresponding analytical results, as the detailed definitions are readily available in existing S-Box literature. To support reproducibility, a dedicated program for computing all evaluation parameters of the S-Box has been developed and is publicly accessible at https://github.com/dpp291187/S-Box-Cryptanalysis.

 doi:10.20944/preprints202509.0311.v1

5.1. Nonlinearity

By applying the standard formula for computing the nonlinearity of Boolean functions to each coordinate function of the S-Box, the results are obtained as shown in Table 5. Most existing constructions achieve average nonlinearity values in the range of 100–112, with the best reported results reaching about 114 on average. In contrast, the proposed S-Box achieves the maximum balanced nonlinearity of 116 uniformly across all eight Boolean functions, giving an average NL of 116.00. This uniform attainment of the theoretical optimum clearly surpasses all previously reported works and establishes a new benchmark for cryptographic S-Box design.

The constructed S-Box also achieves the maximum algebraic degree of 7. Although this value is commonly obtained in many strong S-Box designs, it remains a critical feature that prevents low-degree polynomial representations, thereby reinforcing robustness against algebraic cryptanalysis.

Table 5. Boolean functions nonlinearities comparison with other studies.

S-Box	Year	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	Avg. NL
[4]	2025	112	112	112	112	112	112	112	112	112.00
[6]	2024	112	112	112	112	112	112	112	112	112.00
[7]	2024	112	112	112	112	112	112	112	112	112.00
[8]	2024	112	112	112	112	112	112	112	112	112.00
[9]	2024	112	112	112	112	112	112	112	112	112.00
[10]	2023	112	112	112	112	112	112	112	112	112.00
[17]	2025	109	106	108	110	109	108	108	108	108.25
[20]	2024	112	112	112	112	112	112	112	112	112.00
[22]	2023	106	104	106	110	106	108	108	106	106.75
[25]	2023	106	102	106	106	106	104	106	098	104.25
[29]	2024	116	114	116	114	114	114	114	114	114.50
[32]	2024	112	110	112	112	110	110	110	112	111.00
[33]	2024	112	112	112	110	112	112	112	112	111.75
[36]	2023	110	108	110	108	110	108	110	108	109.00
[53]	2024	104	106	106	104	110	106	112	104	106.50
[66]	2024	104	106	108	108	104	102	100	102	104.25
[67]	2001	112	112	112	112	112	112	112	112	112.00
This work	2025	**116**	**116**	**116**	**116**	**116**	**116**	**116**	**116**	**116.00**

5.2. Strict Avalanche Criterion

One of the fundamental measures of diffusion in an S-Box is the Strict Avalanche Criterion (SAC), which evaluates whether flipping a single input bit produces random-like changes across the output bits with a probability close to 50%. When the SAC values approach 0.5, the S-Box is considered to exhibit strong randomness. Using the method described in [68], the SAC values for each coordinate function of the proposed S-Box were determined, and the outcomes are summarized in Table 6. The overall average value obtained is 0.5126, which is essentially optimal.

Table 6. SAC Values of the proposed S-Box.

i/*j*	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	0.5000	0.5000	0.5000	0.5000	0.5469	0.5469	0.5313	0.5469
2	0.5000	0.5000	0.4375	0.5000	0.5313	0.5313	0.5313	0.5469
3	0.5000	0.4375	0.5000	0.5000	0.5313	0.5313	0.5469	0.5469
4	0.4375	0.5000	0.5000	0.5000	0.5313	0.5469	0.5469	0.5313
5	0.5469	0.5469	0.5313	0.5469	0.4375	0.5000	0.5000	0.5000
6	0.5313	0.5313	0.5313	0.5469	0.4375	0.5000	0.5000	0.5000
7	0.5313	0.5313	0.5469	0.5469	0.4375	0.5000	0.5000	0.5000
8	0.5313	0.5469	0.5469	0.5313	0.4375	0.5000	0.5000	0.5000

 doi:10.20944/preprints202509.0311.v1

5.3. Bit Independence Criterion

The Bit Independence Criterion (BIC) serves as an important indicator of whether the output bits of an S-Box behave independently when a single input bit is modified. It is typically examined through two perspectives: the avalanche effect (BIC-SAC) and resistance to linear approximation (BIC-NL). The computed results, summarized in Tables 7 and 8, show that the proposed S-Box attains an average BIC-NL of 111.64 and an average BIC-SAC of 0.5103. These values confirm that the design satisfies the independence requirement and exhibits strong cryptographic quality.

Table 7. Nonlinearity BIC results (BIC-NL) of the proposed S-Box.

i/j	1	2	3	4	5	6	7	8
1	-	116	116	116	110	108	108	108
2	116	-	116	116	108	108	108	108
3	116	116	-	116	108	110	108	108
4	116	116	116	-	110	108	108	108
5	110	108	108	110	-	116	116	116
6	108	108	110	108	116	-	116	116
7	108	108	108	108	116	116	-	116
8	108	108	108	108	116	116	116	-

Table 8. Strict Avalanche Criterion values for BIC (BIC-SAC).

i/j	1	2	3	4	5	6	7	8
1	-	0.5176	0.5156	0.5078	0.4902	0.5117	0.5059	0.5020
2	0.5176	-	0.5137	0.5156	0.5039	0.5117	0.5332	0.5117
3	0.5156	0.5137	-	0.5156	0.5059	0.5176	0.5254	0.5039
4	0.5078	0.5156	0.5156	-	0.4941	0.5195	0.5078	0.5117
5	0.4902	0.5039	0.5059	0.4941	-	0.5098	0.5078	0.5078
6	0.5117	0.5117	0.5176	0.5195	0.5098	-	0.5059	0.5078
7	0.5059	0.5332	0.5254	0.5078	0.5078	0.5059	-	0.5078
8	0.5020	0.5117	0.5039	0.5117	0.5078	0.5078	0.5078	-

5.4. Differential Approximation Probability

An S-Box's resistance to differential cryptanalysis is commonly evaluated through its differential uniformity, which reflects how evenly output differences are distributed when input differences are applied [58,64]. This behavior is summarized using the XOR distribution table as shown in Table 9, where each entry shows the frequency of specific input–output difference pairs.

Table 9. XOR Distribution Table of Proposed S-Box.

0	6	4	4	4	4	4	4	4	4	4	4	4	4	4
6	4	4	4	4	4	4	4	4	6	4	6	4	6	6	4
4	4	4	6	4	4	4	4	4	4	4	4	4	4	6	4
4	4	6	4	4	4	4	4	4	6	4	4	4	4	4	4
4	4	4	4	4	6	4	4	4	4	4	6	4	4	4	4
4	4	4	4	6	4	4	4	4	4	4	4	4	6	4	4
4	6	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	6	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	6	4	4	4	4	4	4	6	4	4	4	6
4	4	4	6	6	4	6	6	4	4	6	6	6	4	4	4
4	4	6	4	4	4	4	4	4	4	4	4	6	4	6	4
4	4	6	4	6	4	6	6	6	4	4	4	4	4	6	6
4	4	4	6	4	4	4	4	4	6	4	4	4	4	4	4
4	4	4	6	4	6	6	6	6	6	4	4	4	4	4	6
4	4	6	4	4	6	6	6	4	4	6	4	6	6	4	4
4	4	4	4	4	6	4	4	6	4	4	4	4	6	4	4

 doi:10.20944/preprints202509.0311.v1

Table 10 highlights the distribution of differences across the S-Box. The largest entry, denoted as the differential uniformity, shows the maximum probability of a specific difference pair occurring. Smaller values indicate stronger resistance against differential cryptanalysis. Based on the table, the maximum observed frequency leads to a differential uniformity of 6. Consequently, the DAP, obtained by normalizing this value over the full input space, equals $6/256 = 0.0234$.

Table 10. Comparison with alternative S-Boxes.

S-Box	Year	NL	BIC-NL	SAC	BIC-SAC	DAP	LAP	FP	OFP
[4]	2025	112.00	107.14	0.5009	0.4780	0.070	0.125	0	0
[6]	2024	112.00	112.00	0.5049	0.5046	0.016	0.063	2	1
[7]	2024	112.00	112.00	0.5032	0.5057	0.016	0.063	1	2
[8]	2024	112.00	112.00	0.5044	0.5047	0.016	0.063	1	1
[9]	2024	112.00	103.07	0.5014	0.4979	0.039	0.133	0	0
[10]	2023	112.00	112.00	0.4892	0.5017	0.016	0.063	0	1
[17]	2025	108.25	108.79	0.5063	0.5019	0.031	0.105	0	2
[20]	2024	112.00	112.00	0.5045	0.5042	0.016	0.063	0	0
[22]	2023	106.75	103.57	0.5026	0.5019	0.039	0.132	2	0
[25]	2023	104.25	104.00	0.5029	0.5026	0.047	0.125	0	0
[29]	2024	114.50	103.29	0.4976	0.5050	0.039	0.133	2	1
[32]	2024	111.00	111.43	0.5017	0.5034	0.023	0.070	2	0
[33]	2024	111.75	111.00	0.5034	0.5050	0.023	0.070	1	0
[36]	2023	109.00	103.86	0.4936	0.5057	0.039	0.156	0	1
[53]	2024	106.50	103.21	0.5034	0.5040	0.039	0.148	1	0
[66]	2024	104.25	104.23	0.5056	0.5001	0.055	0.133	1	2
[67]	2001	112.00	112.00	0.5048	0.5046	0.016	0.063	0	0
This work	2025	116.00	111.64	0.5126	0.5103	0.023	0.078	0	0
Ideal value	–	**High**	**High**	**0.5000**	**0.5000**	**Low**	**Low**	**0**	**0**

5.5. Linear Approximation Probability

Another important property is the linear approximation probability, which evaluates the likelihood of linear relations existing between selected input and output bits of the S-Box [58,64]. This measure reflects vulnerability to linear cryptanalysis, where smaller values correspond to better resistance. The analysis shows that the S-Box under study achieves a maximum linear probability of 0.078, indicating that no strong linear correlations or structures are present. This outcome suggests that the transformation is resistant to linear approximations, thereby improving overall cryptographic strength.

The comparative results in Table 10 clearly demonstrate the superiority of the proposed S-Box over existing designs. In particular, our construction achieves the highest possible nonlinearity of 116, which significantly surpasses all previously reported works and reaches the theoretical optimum for balanced 8×8 Boolean functions. Furthermore, the obtained BIC-NL of 111.64 closely approaches the best results observed in strong S-Boxes such as [20], and AES S-Box [67], confirming its robustness against linear approximations of correlated outputs. With respect to the SAC and its BIC-SAC, the proposed design exhibits values close to the ideal 0.5, indicating equivalent diffusion performance to state-of-the-art alternatives.

Although the DAP and LAP of our S-Box are slightly weaker compared to AES, they remain lower than or comparable to the majority of alternative S-Boxes surveyed, reflecting a favorable trade-off between resistance to differential and linear cryptanalysis. Another noteworthy strength of the proposed S-Box is the complete elimination of both fixed points and opposite fixed points. In this design, the number of fixed points is zero ($FP = 0$), and likewise, the number of opposite fixed points is also zero ($OFP = 0$). A fixed point corresponds to an input x such that $S(x) = x$, while an opposite

 doi:10.20944/preprints202509.0311.v1

fixed point arises when $S(x) = \bar{x}$, with $\bar{x}$ denoting the bitwise complement of x. The presence of such properties can weaken security by introducing predictable structures exploitable by adversaries. The absence of both FP and OFP in our construction ensures that no trivial input–output patterns exist, thereby enhancing unpredictability and reinforcing the overall cryptographic strength of the proposed S-Box.

5.6. Side-Channel Attack Analysis

In addition to conventional cryptographic criteria, it is essential to assess the resistance of an S-Box against side-channel attacks. For this purpose, we computed several commonly used parameters, including TO. When making comparisons across different designs, however, the normalized forms TO_0, MTO_0, and RTO_0 are typically used, together with MCC, CCV, and SNR. These metrics provide a fair basis for evaluating how effectively an S-Box can mitigate leakage exploitable by power analysis or related techniques.

The results summarized in Table 11 show that the proposed design achieves parameter values closely aligned with those of AES and other recent strong constructions. The variations observed across different schemes are minimal, which indicates that at the theoretical level most modern S-Box designs, including the one proposed here, demonstrate a comparable degree of robustness against basic side-channel attacks. This also confirms that the cryptographic improvements obtained in the proposed S-Box do not compromise its side-channel security.

Table 11. Comparison SCA parameter with alternative S-Boxes.

S-Box	**Year**	TO_0	MTO_0	RTO_0	**MCC**	**CCV**	**SNR**
[4]	2025	7.852	6.872	7.432	0.800	0.116	14.950
[6]	2024	7.860	6.870	7.458	0.820	0.111	14.470
[7]	2024	7.851	6.905	7.541	0.844	0.080	12.219
[8]	2024	7.852	6.853	7.450	0.770	0.122	15.565
[9]	2024	7.833	6.833	7.373	0.738	0.148	19.973
[10]	2023	7.853	6.888	7.468	0.808	0.109	14.219
[17]	2025	7.844	6.843	7.467	0.855	0.111	15.162
[20]	2024	7.804	6.815	7.431	0.805	0.125	15.951
[22]	2023	7.820	6.850	7.440	0.820	0.117	15.088
[25]	2023	7.797	6.810	7.409	0.820	0.129	16.500
[29]	2024	7.854	6.903	7.441	0.804	0.115	14.877
[32]	2024	7.852	6.853	7.439	0.820	0.120	15.353
[33]	2024	7.858	6.865	7.463	0.820	0.109	14.276
[36]	2023	7.812	6.820	7.466	0.750	0.113	14.594
[53]	2024	7.807	6.794	7.401	0.785	0.143	18.837
[66]	2024	7.846	6.866	7.418	0.787	0.121	15.180
[67]	2001	7.860	6.869	7.458	0.820	0.111	14.473
This work	2025	7.908	6.967	7.511	0.801	0.092	12.991
Ideal value	–	**Low**	**Low**	**Low**	**Low**	**Low**	**Low**

Since theoretical analysis alone cannot fully capture practical leakage behavior, the next section turns to hardware implementation and experimental attacks to provide a more reliable evaluation of the proposed S-Box in realistic scenarios.

To evaluate the resistance of the proposed S-Box against side-channel attacks, a trace acquisition scenario similar to [4] was conducted. AES-128 was implemented on the Sakura-X FPGA board with a single-cycle-per-round architecture. Random plaintexts were generated on a computer and encrypted using a fixed 128-bit key. During encryption, the oscilloscope recorded the power consumption of the FPGA, while the corresponding ciphertexts were synchronized and stored on the computer. In total, 30,000 power traces were collected for the analysis.

 doi:10.20944/preprints202509.0311.v1

After trace acquisition, a Correlation Power Analysis (CPA) [69,70] targeting the last round of AES was performed. For each key byte, hypotheses were generated using the Hamming Distance power model, and the correlation coefficient between the hypothetical power values and the measured traces was computed. The correct key value was identified when its correlation clearly exceeded that of other hypotheses.

The evaluation considered two scenarios: AES with the standard Rijndael S-Box, and AES with the proposed S-Box.

- With the AES S-Box, approximately 9,000 traces were sufficient to recover 14 out of 16 key bytes, with the most difficult byte requiring about 11,000 traces.
- With the proposed S-Box, around 12,000 traces were necessary to recover 12 out of 16 key bytes, and the hardest byte required up to 17,000 traces.

As illustrated in Figure 1, the proposed S-Box requires more traces than the AES S-Box for successful key recovery. This suggests a marginal improvement in resistance to CPA; however, the difference remains insignificant in the unprotected evaluation setting. Overall, the results indicate that both S-Boxes exhibit comparable levels of side-channel resistance in practice.

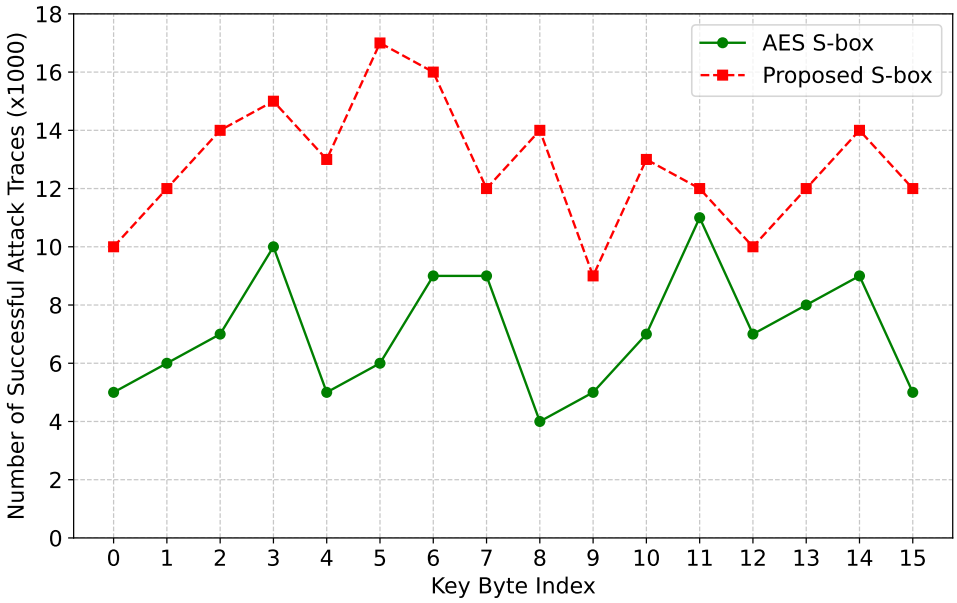

Figure 1. Number of traces required for successful CPA: AES S-Box and proposed S-Box.

6. Implementation

After selecting a representative configuration with four identical 4×4 S-Boxes that achieves both optimal nonlinearity and minimal implementation cost in the previous section, this section provides a detailed description of the hardware implementation in order to evaluate resource utilization. Since the 4×4 S-Box and the multiplication over $GF(2^4)$ are fundamental building blocks, the estimation of hardware cost is straightforward. According to Equations (5) and (6), the proposed architecture can be implemented with two 4×4 S-Box blocks, two multiplications in $GF(2^4)$, and two 2:1 multiplexers (each with 4-bit inputs). The overall hardware design is illustrated in Figure 2. In this figure, the two 4×4 S-Boxes are placed separately to compute output. However, to optimize resource usage, in practical implementation a single S-Box circuit can be reused sequentially for both computations through appropriate scheduling. In this way, the overall architecture not only reflects the algebraic definitions accurately but also achieves high efficiency in terms of hardware resource consumption.

 doi:10.20944/preprints202509.0311.v1

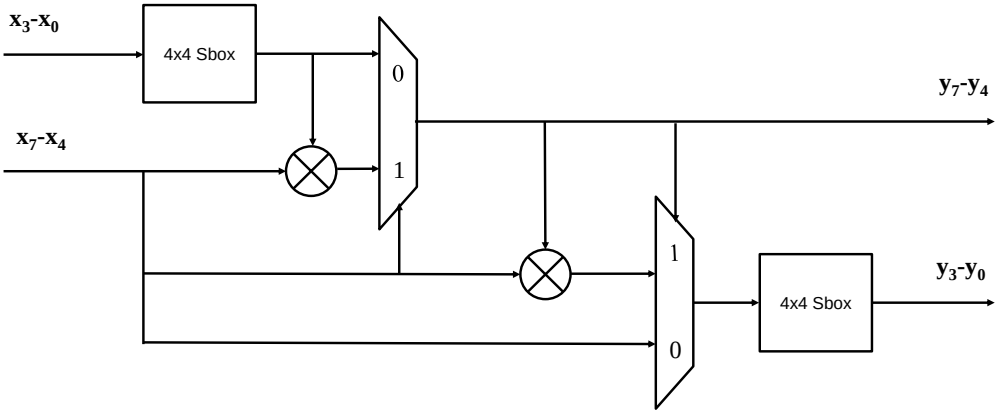

Figure 2. Hardware architecture of the proposed S-Box.

Table 12 presents a benchmark of logic gate utilization for the proposed S-Box in comparison with several established designs. The proposed structure is composed of 43 XOR/XNOR gates, 39 AND gates, 6 OR gates, and 8 multiplexers (2 × 4 MUX21), while entirely avoiding NAND, NOR, and NOT gates. This configuration results in a compact circuit with moderate overall complexity.

Table 12. Logic gate utilization comparison of the proposed S-Box with prior designs.

Studies	XOR/ XNOR	NAND/ NOR	AND	OR	NOT	MUX21	GE (*)
[43]	76	56	0	0	0	0	208.00
[44]	107	10	38	7	5	8	301.75
[71]	91	36	0	0	0	0	218.00
[72]	87	0	54	0	0	0	241.50
[73]	79	41	0	0	0	0	199.00
[74]	57	80	0	0	0	0	194.00
[75]	154	0	36	0	0	8	369.00
[76]	64	23	4	0	0	6	168.00
[77]	90	0	79	28	29	0	342.25
Proposed S-Box	43	0	39	6	0	8	159.75

**GE estimation: XOR/XNOR = 2, AND = 1.25, OR = 1.5, NAND/NOR = 1, NOT = 0.75, MUX21 = 2, based on STM 65nm parameters [73].*

Among these components, XOR gates are generally regarded as the most resource-demanding in terms of hardware cost. The proposed S-Box achieves a significant reduction in XOR usage compared to most prior works. For instance, Zhang [75] reports 154 XOR gates, Canright [71] 91 XOR gates, and Rashidi [74] 57 XOR gates, whereas our design employs only 43 XOR gates. This reduction is particularly important for hardware implementations, as it directly translates into lower area and power consumption.

The normalized hardware cost, expressed in Gate Equivalents (GE) based on STM 65nm technology parameters [73], further highlights the efficiency of the proposed design. The GE count of the proposed S-Box is calculated to be 159.75, which is smaller than most of the compared studies, including Canright (218.00 GE), Zhang (369.00 GE), and Kuznyechik (342.25 GE). Compared with the most efficient prior design by Maximov (168.00 GE), the proposed S-Box achieves a modest improvement, reducing the GE count by about 8.25. The results indicate that the proposed S-Box exhibits lower hardware resource consumption compared to most existing designs. While the main focus of this study lies in optimizing nonlinearity, the proposed S-Box simultaneously achieves improvements in hardware efficiency.

 doi:10.20944/preprints202509.0311.v1

Overall, these results confirm that the proposed S-Box achieves an attractive balance between low gate complexity and strong cryptographic criteria. The significant reduction in XOR gates and the smallest GE count among all compared implementations highlight its suitability for resource-constrained environments such as embedded systems and lightweight cryptographic applications.

7. Conclusion

This paper presents a novel method for constructing 8×8 S-Boxes from smaller 4×4 components, representing a significant advance in cryptographic design. Key findings and contributions are as follows:

- Optimal Nonlinearity: The S-Boxes developed using this new method achieve a nonlinearity of 116, which is the highest possible for balanced 8-variable Boolean functions. This breakthrough surpasses all previously reported results, setting a new benchmark in the field.
- Comprehensive Security: Beyond optimal nonlinearity, the S-Boxes also satisfy other key cryptographic criteria, including the Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), Differential Avalanche Probability (DAP), and Linear Avalanche Probability (LAP), all at robust levels.
- Proven Robustness and Efficiency: Practical evaluations show that these S-Boxes are highly resilient. They offer side-channel attack resistance comparable to the AES S-Box and are designed for efficient hardware implementation, making them suitable for resource-constrained systems.

In summary, this research is a major step forward, providing a new S-Box construction method that is not only a theoretical breakthrough but also a practical, efficient, and highly secure solution for modern block ciphers and data protection systems.

Author Contributions: Supervision, C.-K. P.; methodology, P.-P. D.; investigation, P.-P. D.; writing—original draft preparation, P.-P. D.; writing—review and editing, P.-P. D., C.-K. P. All authors have read and agreed to the published version of the manuscript.

Funding: Not applicable.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sarkar, P.; Maitra, S. Nonlinearity Bounds and Constructions of Resilient Boolean Functions. In Proceedings of the Advances in Cryptology — CRYPTO 2000. Springer Berlin Heidelberg, 2000, pp. 515–532.
2. Carlet, C.; Djurasevic, M.; Jakobovic, D.; Mariot, L.; Picek, S. Evolving constructions for balanced, highly nonlinear boolean functions. In Proceedings of the Proceedings of the Genetic and Evolutionary Computation Conference, 2022, p. 1147–1155. https://doi.org/10.1145/3512290.3528871.
3. Gini, A.; Méaux, P. Weightwise perfectly balanced functions and nonlinearity. Cryptology ePrint Archive, Paper 2022/1777, 2022.
4. Duong, P.P.; Dang, T.K.; Hoang, T.T.; Pham, C.K. Compact 8-Bit S-Boxes Based on Multiplication in a Galois Field GF(24). *Cryptography* **2025**, *9*. https://doi.org/10.3390/cryptography9020021.
5. Kuznetsov, O.; Poluyanenko, N.; Frontoni, E.; Kandiy, S. Enhancing Smart Communication Security: A Novel Cost Function for Efficient S-Box Generation in Symmetric Key Cryptography. *Cryptography* **2024**, *8*. https://doi.org/https://doi.org/10.3390/cryptography8020017.
6. Baowidan, S.A.; Alamer, A.; Hassan, M.; Yousaf, A. Group-Action-Based S-box Generation Technique for Enhanced Block Cipher Security and Robust Image Encryption Scheme. *Symmetry* **2024**, *16*. https://doi.org/https://doi.org/10.3390/sym16080954.

7. Alali, A.S.; Ali, R.; Jamil, M.K.; Ali, J.; Gulraiz. Dynamic S-Box Construction Using Mordell Elliptic Curves over Galois Field and Its Applications in Image Encryption. *Mathematics* **2024**, *12*. https://doi.org/https://doi.org/10.3390/math12040587.
8. Aribilola, I.; Lee, B.; Naveed Asghar, M. Möbius Transformation and Permutation Based S-Box to Enhance IoT Multimedia Security. *IEEE Access* **2024**, *12*, 140792–140808. https://doi.org/10.1109/ACCESS.2024.3466930.
9. Asif, M.; Wajiha, S.; Askar, S.; Ahmad, H. A Novel Scheme for Construction of S-Box Using Action of Power Associative Loop and Its Applications in Text Encryption. *IEEE Access* **2024**, *12*, 90853–90861. https://doi.org/10.1109/ACCESS.2024.3409387.
10. Ali, R.; Jamil, M.K.; Alali, A.S.; Ali, J.; Afzal, G. A Robust S Box Design Using Cyclic Groups and Image Encryption. *IEEE Access* **2023**, *11*, 135880–135890. https://doi.org/10.1109/ACCESS.2023.3337443.
11. Zahid, A.H.; Rashid, H.; Shaban, M.M.U.; Ahmad, S.; Ahmed, E.; Amjad, M.T.; Baig, M.A.T.; Arshad, M.J.; Tariq, M.N.; Tariq, M.W.; et al. Dynamic S-Box Design Using a Novel Square Polynomial Transformation and Permutation. *IEEE Access* **2021**, *9*, 82390–82401. https://doi.org/10.1109/ACCESS.2021.3086717.
12. Kuznetsov, A.; Frontoni, E.; Romeo, L.; Poluyanenko, N.; Kandiy, S.; Kuznetsova, K.; Beňová, E. Optimizing Hill Climbing Algorithm for S-Boxes Generation. *Electronics* **2023**, *12*. https://doi.org/10.3390/electronics12102338.
13. A. Mahboob, M. Asif, I. Siddique, A. Saleem, M. Nadeem, D. Grzelczyk, and J. Awrejcewicz. A Novel Construction of Substitution Box Based on Polynomial Mapped and Finite Field With Image Encryption Application. *IEEE Access* **Nov. 2022**, *10*, 119244–119258.
14. Ramzan, M.; Shah, T.; Hazzazi, M.M.; Aljaedi, A.; Alharbi, A.R. Construction of S-Boxes Using Different Maps Over Elliptic Curves for Image Encryption. *IEEE Access* **2021**, *9*, 157106–157123. https://doi.org/10.1109/ACCESS.2021.3128177.
15. Zahid, A.H.; Arshad, M.J.; Ahmad, M. A Novel Construction of Efficient Substitution-Boxes Using Cubic Fractional Transformation. *Entropy* **2019**, *21*. https://doi.org/https://doi.org/10.3390/e21030245.
16. Zahid, A.H.; Arshad, M.J. An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping. *Symmetry* **2019**, *11*. https://doi.org/https://doi.org/10.3390/sym11030437.
17. Song, R.; Zhao, H. Security-Enhanced Image Encryption: Combination of S-Boxes and Hyperchaotic Integrated Systems. *IEEE Access* **2025**, *13*, 105151–105164. https://doi.org/10.1109/ACCESS.2025.3575935.
18. Boobalan, S.; Gurunathan Arthanari, S.K. Lorenz and Chua Chaotic Key-Based Dynamic Substitution Box for Efficient Image Encryption. *Symmetry* **2025**, *17*. https://doi.org/10.3390/sym17081296.
19. Dutra e Silva Junior, É.C.; Cruz, C.A.d.M.; Saraiva, I.A.L.; Santos, F.G.; dos Santos Junior, C.R.P.; Indrusiak, L.S.; Finamore, W.A.; Glesner, M. Chaos-Based S-Boxes as a Source of Confusion in Cryptographic Primitives. *Electronics* **2025**, *14*. https://doi.org/10.3390/electronics14112198.
20. Alabduallah, B.; Banga, A.; Iqbal, N.; Ikram, A.; Diab, H. Advancing Cryptographic Security With a New Delannoy-Derived Chaotic S-Box. *IEEE Access* **2024**, *12*, 82926–82937. https://doi.org/10.1109/ACCESS.2024.3410668.
21. Y. Aydın and F. Özkaynak. Automated Chaos-Driven S-Box Generation and Analysis Tool for Enhanced Cryptographic Resilience. *IEEE Access* **Dec. 2023**, *12*, 312–328. https://doi.org/10.1109/ACCESS.2023.3346319.
22. A. W. Malik, A. H. Zahid, D. S. Bhatti, H. J. Kim, and K.-I. Kim. Designing S-Box Using Tent-Sine Chaotic System While Combining the Traits of Tent and Sine Map. *IEEE Access* **Jul. 2023**, *11*, 79265–79274. https://doi.org/10.1109/ACCESS.2023.3298111.
23. Alharbi, A.R.; Jamal, S.S.; Khan, M.F.; Gondal, M.A.; Abbasi, A.A. Construction and Optimization of Dynamic S-Boxes Based on Gaussian Distribution. *IEEE Access* **2023**, *11*, 35818–35829. https://doi.org/10.1109/ACCESS.2023.3262313.
24. Haque, A.; Abdulhussein, T.A.; Ahmad, M.; Waheed Falah, M.; Abd El-Latif, A.A. A Strong Hybrid S-Box Scheme Based on Chaos, 2D Cellular Automata and Algebraic Structure. *IEEE Access* **2022**, *10*, 116167–116181. https://doi.org/10.1109/ACCESS.2022.3218062.
25. Corona-Bermúdez, E.; Chimal-Eguía, J.C.; Corona-Bermúdez, U.; Rivero-Ángeles, M.E. Chaos Meets Cryptography: Developing an S-Box Design with the Rössler Attractor. *Mathematics* **2023**, *11*. https://doi.org/https://doi.org/10.3390/math11224575.
26. Shafique, A.; Khan, K.H.; Hazzazi, M.M.; Bahkali, I.; Bassfar, Z.; Rehman, M.U. Chaos and Cellular Automata-Based Substitution Box and Its Application in Cryptography. *Mathematics* **2023**, *11*. https://doi.org/https://doi.org/10.3390/math11102322.

 doi:10.20944/preprints202509.0311.v1

27. C. Yang, X. Wei, and C. Wang. S-Box Design Based on 2D Multiple Collapse Chaotic Map and Their Application in Image Encryption. *Entropy* **Oct. 2021**, *23*. https://doi.org/https://doi.org/10.3390/e23101312.
28. Yogi, B.; Roy, S.; Rawat, U.; Redkar, S. Advanced Image Ciphering: 1-D Group Cellular Automata and S-Box Strategies. In Proceedings of the 2025 International Conference on Next Generation Communication & Information Processing (INCIP), 2025, pp. 15–19. https://doi.org/10.1109/INCIP64058.2025.11019383.
29. Waheed, A.; Subhan, F.; Mohd Su'ud, M.; Mansoor Alam, M. Molding robust S-box design based on linear fractional transformation and multilayer Perceptron: Applications to multimedia security. *Egyptian Informatics Journal* **2024**, *26*, 100480. https://doi.org/https://doi.org/10.1016/j.eij.2024.100480.
30. Zhang, N.; Zhao, Q.; Zhang, H. Construction of Rotation Symmetric S-Boxes Based on a Hybrid Heuristic Algorithm. In Proceedings of the 2024 6th International Conference on Natural Language Processing (ICNLP), 2024, pp. 295–299. https://doi.org/10.1109/ICNLP60986.2024.10692460.
31. Kuznetsov, O.; Poluyanenko, N.; Kuznetsova, K.; Frontoni, E.; Arnesano, M. Hybrid Population-Based Hill Climbing Algorithm for Generating Highly Nonlinear S-boxes. *Computers* **2024**, *13*. https://doi.org/10.3390/computers13120320.
32. Hazzazi, M.M.; Baowidan, S.A.; Yousaf, A.; Adeel, M. An Innovative Algorithm Based on Chaotic Maps Amalgamated with Bit-Level Permutations for Robust S-Box Construction and Its Application in Medical Image Privacy. *Symmetry* **2024**, *16*. https://doi.org/10.3390/sym16081070.
33. Malik, D.S.; Shah, T.; Tehsin, S.; Nasir, I.M.; Fitriyani, N.L.; Syafrudin, M. Block Cipher Nonlinear Component Generation via Hybrid Pseudo-Random Binary Sequence for Image Encryption. *Mathematics* **2024**, *12*. https://doi.org/10.3390/math12152302.
34. Ahmad, M.; Alkanhel, R.; El-Shafai, W.; Algarni, A.D.; El-Samie, F.E.A.; Soliman, N.F. Multi-Objective Evolution of Strong S-Boxes Using Non-Dominated Sorting Genetic Algorithm-II and Chaos for Secure Telemedicine. *IEEE Access* **2022**, *10*, 112757–112775. https://doi.org/10.1109/ACCESS.2022.3209202.
35. Artuğer, F.; Özkaynak, F. SBOX-CGA: substitution box generator based on chaos and genetic algorithm. *Neural Computing and Applications* **2022**, *34*, 20203–20211.
36. A. I. Lawah, A. A. Ibrahim, S. Q. Salih, H. S. Alhadawi, and P. S. JosephNg. Grey Wolf Optimizer and Discrete Chaotic Map for Substitution Boxes Design and Optimization. *IEEE Access* **Apr. 2023**, *11*, 42416–42430.
37. Alsaif, H.; Guesmi, R.; Kalghoum, A.; Alshammari, B.M.; Guesmi, T. A Novel Strong S-Box Design Using Quantum Crossover and Chaotic Boolean Functions for Symmetric Cryptosystems. *Symmetry* **2023**, *15*. https://doi.org/10.3390/sym15040833.
38. L. Li, J. Liu, Y. Guo, and B. Liu. A New S-box Construction Method Meeting Strict Avalanche Criterion. *J. Inf. Secur. Appl.* **May 2022**, *66*, 103135.
39. J. Abdurazzokov. Dynamic S-Box Generation Algorithm with Improved Strict Avalanche Criterion by Selection of Adjacency Matrix Parameters. In Proceedings of the Int. Conf. on Tech. Advancements in Comp. Sciences (ICTACS), Nov. 2023, pp. 393–398.
40. Duong, P.P.; Nguyen, H.M.; Dao, B.A.; Tran, T.H.; Kieu-Do-Nguyen, B.; Pham, C.K.; Hoang, T.T. S-Boxes with Optimal Strict Avalanche Criterion using Chaotic Map. In Proceedings of the 2024 9th International Conference on Integrated Circuits, Design, and Verification (ICDV), 2024, pp. 85–90. https://doi.org/10.1109/ICDV61346.2024.10616714.
41. Sony, D.; Reddy, D.K. Dynamic Composite S-Boxes for High-Speed IoT Encryption with Enhanced Security. In Proceedings of the 2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT), 2025, pp. 371–375. https://doi.org/10.1109/CSNT64827.2025.10968911.
42. Kumar, S.; Kumar, D.; Lamkuche, H.; Sharma, V.S.; Alkahtani, H.K.; Elsadig, M.; Bivi, M.A. SHC: 8-bit Compact and Efficient S-Box Structure for Lightweight Cryptography. *IEEE Access* **2024**, *12*, 39430–39449. https://doi.org/10.1109/ACCESS.2024.3372388.
43. Rashidi, B. Compact and efficient structure of 8-bit S-box for lightweight cryptography. *Integration* **2021**, *76*, 172–182. https://doi.org/https://doi.org/10.1016/j.vlsi.2020.10.009.
44. Teng, Y.T.; Chin, W.L.; Chang, D.K.; Chen, P.Y.; Chen, P.W. VLSI Architecture of S-Box With High Area Efficiency Based on Composite Field Arithmetic. *IEEE Access* **2022**, *10*, 2721–2728. https://doi.org/10.1109/ACCESS.2021.3139040.
45. Y. Li and M. Wang. Constructing S-boxes for Lightweight Cryptography with Feistel Structure. In Proceedings of the Crypto. Hardware and Embedded Syst. (CHES), Sep. 2014, Vol. 8731, pp. 127–146.

 doi:10.20944/preprints202509.0311.v1

46. E. Boss, V. Grosso, T. Guneysu, G. Leander, A. Moradi, and T. Schneider. Strong 8-bit Sboxes with Efficient Masking in Hardware. In Proceedings of the Crypto. Hardware and Embedded Syst. (CHES), Mar. 2017, Vol. 7, pp. 171–193.
47. A. Canteaut, S. Duval, and G. Leurent. Construction of Lightweight S-Boxes Using Feistel and MISTY Structures. In Proceedings of the Selected Areas in Crypto. (SAC), Aug. 2015, pp. 373–393.
48. Yan, L.; Li, L.; Song, Q. Lightweight 6-bit S-Boxes With DPA Resistance. *IEEE Transactions on Network Science and Engineering* **2025**, *12*, 3719–3730. https://doi.org/10.1109/TNSE.2025.3564598.
49. Duong, P.P.; Minh Nguyen, H.; Dao, B.A.; Kieu-Do-Nguyen, B.; Tran, T.H.; Hoang, T.T.; Pham, C.K. Construction of Robust Lightweight S-Boxes Using Enhanced Logistic and Enhanced Sine Maps. *IEEE Access* **2024**, *12*, 63976–63994. https://doi.org/10.1109/ACCESS.2024.3396452.
50. Kang, M.; Wang, M. New Genetic Operators for Developing S-Boxes With Low Boomerang Uniformity. *IEEE Access* **2022**, *10*, 10898–10906. https://doi.org/10.1109/ACCESS.2022.3144458.
51. H. Kim, Y. Jeon, G. Kim, J. Kim, B.-Y. Sim, D.-G. Han, H. Seo, S. Kim, S. Hong, J. Sung, and D. Hong. A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application. *IEEE Access* **Nov. 2021**, *9*, 150592–150607.
52. Dimitrov, M.; Baicheva, T. On the Pentanomial Power Mapping Classification of 8-bit to 8-bit S-Boxes. *Mathematics* **2024**, *12*. https://doi.org/10.3390/math12142154.
53. Zhang, L.; Ma, C.; Zhao, Y.; Zhao, W. A Novel Dynamic S-Box Generation Scheme Based on Quantum Random Walks Controlled by a Hyper-Chaotic Map. *Mathematics* **2024**, *12*. https://doi.org/10.3390/math12010084.
54. Carlet, C. Boolean functions for cryptography and coding theory **2021**.
55. Kumar, S.; Chaudhary, D.; Lakshmanan, S.A.; Lee, C.C. Novel Approach to Degree, Balancedness, and Affine Equivalence of Boolean Functions and Construction of a Special Class of Non-Quadratic Balanced Boolean Functions. *Cryptography* **2025**, *9*. https://doi.org/10.3390/cryptography9030056.
56. Tariq, O.; Dastagir, M.B.A.; Han, D. Compact Walsh–Hadamard Transform-Driven S-Box Design for ASIC Implementations. *Electronics* **2024**, *13*. https://doi.org/10.3390/electronics13163148.
57. A. F. Webster and S. E. Tavares. On the Design of S-Boxes. In Proceedings of the Advances in Cryptology (CRYPTO), 1986, pp. 523–534. https://doi.org/10.1007/3-540-39799-X_41.
58. H. M. Heys. A Tutorial on Linear and Differential Cryptanalysis. *Cryptologia* **2002**, *26*, 189–221. https://doi.org/10.1080/0161-110291890885.
59. Mishra, P.; Sarkar, S.; Gupta, I. Determining the Minimum Degree of an S-box **2017**.
60. Heuser, A.; Picek, S.; Guilley, S.; Mentens, N. Lightweight Ciphers and Their Side-Channel Resilience. *IEEE Transactions on Computers* **2020**, *69*, 1434–1448. https://doi.org/10.1109/TC.2017.2757921.
61. Li, H.; Zhou, Y.; Ming, J.; Yang, G.; Jin, C. The Notion of Transparency Order, Revisited. *The Computer Journal* **2020**, *63*, 1915–1938. https://doi.org/10.1093/comjnl/bxz080.
62. ZHOU, Y.; ZHAO, W.; Chen, Z.; WANG, W.; DU, X. On the Signal-to-Noise Ratio for Boolean Functions. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **2020**, *E103.A*. https://doi.org/10.1587/transfun.2020EAL2037.
63. Li, H.; Yang, G.; Ming, J.; Zhou, Y.; Jin, C. Transparency order versus confusion coefficient: a case study of NIST lightweight cryptography S-Boxes. *Cybersecurity* **2021**, *4*, 35. https://doi.org/10.1186/s42400-021-00099-1.
64. E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology* **1991**, *4*, 3–72. https://doi.org/https://doi.org/10.1007/BF00630563.
65. C. Adams and S. Tavares. The Structured Design of Cryptographically Good S-Boxes. *J. Cryptology* **Jan. 1990**, *3*, 27–41. https://doi.org/https://doi.org/10.1007/BF00203967.
66. Alqahtani, J.; Akram, M.; Ali, G.A.; Iqbal, N.; Alqahtani, A.; Alroobaea, R. Elevating Network Security: A Novel S-Box Algorithm for Robust Data Encryption. *IEEE Access* **2024**, *12*, 2123–2134. https://doi.org/10.1109/ACCESS.2023.3348144.
67. J. Daemen and V. Rijmen. *The design of Rijndael*; Vol. 2, Springer, 2002.
68. H. Kim, Y. Jeon, G. Kim, J. Kim, B.-Y. Sim, D.-G. Han, H. Seo, S. Kim, S. Hong, J. Sung, and D. Hong. A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application. *IEEE Access* **Nov. 2021**, *9*, 150592–150607. https://doi.org/10.1109/ACCESS.2021.3126008.
69. Brier, E.; Clavier, C.; Olivier, F. Correlation Power Analysis with a Leakage Model. In Proceedings of the Cryptographic Hardware and Embedded Systems - CHES 2004. Springer Berlin Heidelberg, 2004, pp. 16–29. https://doi.org/https://doi.org/10.1007/978-3-540-28632-5_2.

 doi:10.20944/preprints202509.0311.v1

70. Mestiri, H.; Kahri, F.; Bouallegue, B.; Machhout, M. A CPA attack against cryptographic hardware implementation on SASEBO-GII. In Proceedings of the 2017 International Conference on Green Energy Conversion Systems (GECS), 2017, pp. 1–5. https://doi.org/10.1109/GECS.2017.8066139.
71. Canright, D. A Very Compact S-Box for AES. In Proceedings of the Cryptographic Hardware and Embedded Systems – CHES 2005, 2005, pp. 441–455. https://doi.org/https://doi.org/10.1007/11545262_32.
72. Ueno, R.; Homma, N.; Sugawara, Y.; Nogami, Y.; Aoki, T. Highly Efficient GF(2^8) Inversion Circuit Based on Redundant GF Arithmetic and Its Application to AES Design. In Proceedings of the Cryptographic Hardware and Embedded Systems – CHES 2015. Springer, 2015, Vol. 9293, pp. 63–80. https://doi.org/https://doi.org/10.1007/978-3-662-48324-4_4.
73. Reyhani-Masoleh, A.; Taha, M.; Ashmawy, D. New Area Record for the AES Combined S-Box/Inverse S-Box. In Proceedings of the 2018 IEEE 25th Symposium on Computer Arithmetic (ARITH), 2018, pp. 145–152. https://doi.org/10.1109/ARITH.2018.8464780.
74. Rashidi, B. Compact and efficient structure of 8-bit S-box for lightweight cryptography. *Integration* **2021**, *76*, 172–182. https://doi.org/https://doi.org/10.1016/j.vlsi.2020.10.009.
75. Zhang, X.; Parhi, K. High-speed VLSI architectures for the AES algorithm. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* **2004**, *12*, 957–967. https://doi.org/10.1109/TVLSI.2004.832943.
76. Maximov, A.; Ekdahl, P. New Circuit Minimization Techniques for Smaller and Faster AES SBoxes. *IACR Transactions on Cryptographic Hardware and Embedded Systems* **2019**, pp. 91–125. https://doi.org/https://doi.org/10.13154/tches.v2019.i4.91-125.
77. Avraamova, O.; Fomin, D.; Serov, V.; Smirnov, A.; Shokov, V. A compact bit-sliced representation of Kuznyechik S-box. Математические вопросы криптографии **2021**, *12*, 21–38. https://doi.org/10.4213/mvk354.