American Journal of Science, Engineering and Technology
2026, Vol. 11, No. 3, pp. 186–194
https://doi.org/10.11648/j.ajset.20261103.18

SciencePG
Science Publishing Group

Research Article

An AES-inspired Construction of a Cryptographically Strong 8×8 S-box Using Modified Algebraic and Affine Parameters

Javokhir Abdurazzokov*

Department of Exact Sciences and Digital Technologies, Tashkent International University, Tashkent, Uzbekistan

Abstract

Substitution boxes (S-boxes) are essential nonlinear components in symmetric-key block ciphers and play a central role in providing resistance against linear and differential cryptanalytic attacks. In this paper, a new 8×8 S-box is proposed based on an AES-inspired inverse-affine construction. Unlike the standard AES S-box, the proposed design simultaneously modifies the irreducible polynomial, the nonsingular affine matrix, and the constant vector to generate a different substitution table over GF (2^8). The novelty of the proposed approach lies in the joint modification of these three structural parameters while preserving the mathematical clarity and reproducibility of the AES inverse-affine construction. The main objective of this approach is to preserve the strong algebraic structure of AES-like S-box construction while maintaining important cryptographic properties. The proposed S-box was implemented in Python and evaluated using several standard cryptographic criteria, including nonlinearity, algebraic degree, Strict Avalanche Criterion (SAC), Linear Approximation Probability (LAP), and Differential Probability (DP). The experimental results show that the proposed S-box achieves minimum, maximum, and mean nonlinearity values of 112, while its algebraic degree is equal to 7. Moreover, the SAC values range from 0.4375 to 0.5469, with an average value of 0.5, indicating balanced avalanche behavior. The proposed S-box also obtains an LAP value of 0.0625 and a DP value of 4/256, demonstrating competitive resistance against linear and differential attacks. The obtained results were compared with AES, SM4, O‘zDSt 1105: 2009, and several recently reported 8×8 S-box constructions. The comparative analysis confirms that the proposed S-box provides a strong balance between nonlinearity, avalanche behavior, linear approximation resistance, and differential uniformity. Therefore, the proposed AES-inspired parameter modification approach can be considered a promising and reproducible method for designing secure substitution boxes for symmetric-key block cipher algorithms.

Keywords

S-box, AES, Finite Field, Affine Transformation, Nonlinearity, Strict Avalanche Criterion, Linear Approximation Probability, Differential Probability

*Correspondence: Javokhir Abdurazzokov (javohirjon.1992@gmail.com)

Received: 17 May 2026; **Accepted:** 4 August 2026; **Published:** 22 August 2026

1. Introduction

The rapid expansion of digital technologies has made secure data transmission, storage, and processing a fundamental requirement for modern information systems. Today, cryptographic mechanisms are used in banking platforms, cloud services, mobile applications, Internet of Things (IoT) environments, medical information systems, and governmental digital infrastructures. In such systems, symmetric-key block ciphers remain highly important because they provide efficient encryption, fast implementation, and practical protection for large volumes of data.

A substitution box (S-box) is one of the most important nonlinear components of a block cipher. Its main role is to introduce confusion into the encryption process and to weaken direct algebraic or statistical relationships between plaintext, key, and ciphertext. For this reason, the security of an entire block cipher is strongly influenced by the cryptographic quality of its S-box. A weak S-box may create exploitable patterns, whereas a carefully designed S-box can improve resistance to differential, linear, algebraic, and statistical cryptanalytic attacks.

The importance of S-box design was clearly demonstrated by classical cryptanalytic studies. Biham and Shamir introduced differential cryptanalysis and showed that input-output difference propagation can reveal weaknesses in DES-like cryptosystems [1]. Matsui later introduced linear cryptanalysis, proving that approximate linear relations inside a cipher can also be used to recover secret information [2]. Nyberg's work on differentially uniform mappings further established the theoretical importance of controlling differential behavior in cryptographic functions [3]. These studies created the foundation for evaluating S-boxes using criteria such as nonlinearity, differential uniformity, and linear approximation probability.

The Advanced Encryption Standard (AES) remains one of the most influential examples of a practical block cipher with a strong and well-studied S-box [4]. Its design has motivated many researchers to investigate algebraic and affine transformations as reliable tools for constructing substitution components. However, although AES-inspired constructions are mathematically strong and practically meaningful, the search for alternative S-boxes with balanced cryptographic properties remains an active research direction.

Several studies have proposed different methods for constructing S-boxes. Sattarov and Abdurahimov presented an algorithm for block symmetric encryption with attention to algebraic immunity and nonlinearity [5]. Chaotic systems have also been widely used: Lu et al. proposed a compound-chaotic-system method [6], while Zhu et al. combined chaotic dynamics with optimization mechanisms [7]. These approaches can produce complex substitution structures, but their practical value depends on reproducible parameter selection, sensitivity analysis, and a clear explanation of how the generated S-box can be integrated into a conventional cipher architecture.

Another important direction is heuristic and evolutionary S-box generation. Picek et al. introduced a cost function for evolving S-boxes [8], Marochok and Zajac generated S-boxes under prescribed differential-spectrum restrictions [9], and Kuznetsov et al. investigated efficient cost functions for rapid S-box generation [10]. Optimization-based methods are effective for exploring a large permutation space, but their results are strongly influenced by the selected objective function, stopping criterion, and search strategy. Consequently, high numerical scores should be accompanied by a transparent construction rule and a multi-criteria security assessment.

Abdurazzokov introduced a genetic-algorithm-based method that constructs nonsingular adjacency matrices from graph structures and applies an AES-inspired affine transformation [11]. Razaq et al. developed an S-box design based on coset graphs and matrix operations [12]. Compared with purely random or chaotic generation, these approaches provide a more explicit mathematical structure; however, the influence of each selected matrix parameter on the final cryptographic indicators must still be demonstrated through systematic evaluation.

Strict avalanche behavior is another important requirement for modern S-boxes. Li et al. proposed an S-box construction method designed to satisfy the strict avalanche criterion while maintaining good nonlinearity, differential uniformity, and algebraic characteristics [13]. This is important because a secure S-box should react strongly to small input changes: ideally, changing a single input bit should affect approximately half of the output bits. Therefore, improving the strict avalanche criterion without weakening other cryptographic properties is an important design challenge.

Recent research has also revisited AES-related constructions through alternative algebraic parameters. Saukhanova et al. proposed S-boxes based on alternative irreducible polynomials and constant vectors [14]. This direction preserves the deterministic inverse-affine framework and therefore offers better reproducibility than many stochastic generation methods. Nevertheless, modifying a single parameter does not by itself guarantee an improvement in every cryptographic metric, which motivates evaluating the combined effect of the field polynomial, affine matrix, and constant vector.

Although many strong S-box generation methods have been reported, several limitations remain. Some studies emphasize only one or two indicators, whereas practical cipher design requires a balanced analysis of nonlinearity, algebraic degree, differential behavior, linear approximation resistance, avalanche behavior, and structural properties. Chaotic and heuristic approaches may provide strong numerical results but can be difficult to reproduce or explain structurally. AES-inspired constructions are more transparent, yet

the combined effect of modifying the irreducible polynomial, affine matrix, and constant vector has received comparatively less attention.

Therefore, this paper proposes a new 8×8 S-box based on an AES-inspired construction by modifying its irreducible polynomial, affine matrix, and constant vector. The generated S-box is evaluated using nonlinearity, algebraic degree, the Strict Avalanche Criterion (SAC), Differential Probability (DP), Linear Approximation Probability (LAP), fixed points, and opposite fixed points.

The main contributions are threefold: first, the construction of a new AES-inspired S-box with modified structural parameters; second, a detailed cryptographic evaluation of the obtained S-box; and third, a comparative analysis with existing algebraic, chaotic, heuristic, graph-based, and AES-related S-box designs. The results aim to show whether the proposed S-box achieves a competitive balance between simplicity, structural clarity, and cryptographic strength.

2. Materials and Methods

2.1. Construction and Use of the S-box in AES

Substitution boxes, commonly referred to as S-boxes, are among the most important nonlinear components in modern symmetric-key block ciphers. In the Advanced Encryption Standard (AES), the S-box is used as a byte-wise substitution mechanism in which each 8-bit input value is transformed into a corresponding 8-bit output value. Although the AES S-box is usually implemented as a fixed lookup table, its entries are not selected randomly. They are obtained from a deterministic algebraic construction over a finite field.

The mathematical basis of the AES S-box is the binary extension field GF (2^8), where GF denotes a Galois field. In this field, each byte is interpreted as a polynomial of degree at most seven with coefficients in GF (2). Thus, an arbitrary byte is represented by Eq (1).

$$a(x) = a_7x^7 + a_6x^6 + \cdots + a_1x + a_0, \quad a_i \in GF(2), \quad i = 0, 1, \ldots, 7 \tag{1}$$

The field GF (2^8) can be represented as the quotient ring in Eq (2).

$$GF(2^8) \cong \frac{GF(2)[x]}{m(x)} \tag{2}$$

Here, m(x) is an irreducible polynomial of degree eight. In the standard AES specification, the polynomial is defined by Eq (3).

$$m_{\text{AES}}(x) = x^8 + x^4 + x^3 + x + 1 \tag{3}$$

In this representation, addition of two field elements is performed by the bitwise XOR operation applied to their polynomial coefficients. Multiplication is carried out as ordinary polynomial multiplication followed by reduction modulo the irreducible polynomial *m(x)*. This algebraic structure allows AES to process byte values as elements of a well-defined finite field.

The AES S-box may be viewed as the bijective mapping shown in Eq (4).

$$S: GF(2^8) \to GF(2^8) \tag{4}$$

Its construction consists of two main steps. First, the multiplicative inverse of each nonzero input element is computed in GF (2^8); zero, which has no multiplicative inverse, is mapped to itself at this stage. Second, an affine transformation over GF (2) is applied to the resulting byte.

The overall transformation is expressed in Eq (5), where x^{-1} denotes the multiplicative inverse of x in GF (2^8), A is an invertible 8×8 binary matrix, and b is a fixed binary constant vector. The matrix A mixes the output bits, while b introduces a constant binary shift; together they form the affine layer of the AES S-box.

$$S(x) = Ax^{-1} \oplus b \tag{5}$$

For the standard AES S-box, the affine matrix A and constant vector b are specified in Eq (6).

$$A_{\text{AES}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad b_{\text{AES}} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{6}$$

By applying the multiplicative inversion followed by the affine transformation to all 256 possible byte values, the complete AES S-box is obtained. This construction provides a strong nonlinear substitution layer and contributes to the resistance of AES against important classes of cryptanalytic attacks, particularly differential and linear cryptanalysis.

In the present study, this classical AES-inspired construction is used as the starting point for generating a new S-box. Instead of directly adopting the standard polynomial, affine matrix, and constant vector, the proposed method modifies these parameters in order to obtain a new substitution box with competitive cryptographic properties. The detailed selection of the modified parameters and the evaluation procedure are presented in the following subsections.

2.2. Generation of the Proposed S-box Based on Modified AES Parameters

In this subsection, the proposed 8×8 S-box is generated by

modifying the main parameters of the AES-inspired inverse-affine construction. A new irreducible polynomial, an alternative nonsingular binary affine matrix, and a different constant vector are selected and used to compute a new substitution table over GF (2^8).

The binary polynomial selected for the proposed finite field is given in Eq (7).

$$m_{\text{bin}} = 100011101_2 \tag{7}$$

In algebraic form, the selected binary polynomial is written as shown in Eq (8).

$$m(x) = x^8 + x^4 + x^3 + x^2 + 1 \tag{8}$$

Consequently, the finite field used in the proposed construction is represented by Eq (9).

$$GF(2^8) \cong \frac{GF(2)[x]}{x^8+x^4+x^3+x^2+1} \tag{9}$$

The affine layer of the proposed S-box is determined by the nonsingular binary matrix in Eq (10).

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \tag{10}$$

The constant vector used in the affine transformation is selected as shown in Eq (11).

$$b = 01000101_2 \tag{11}$$

For each input value x ∈ GF (2^8), the multiplicative inverse is first computed in the finite field defined by m(x). The resulting field element is then transformed by the selected affine mapping. Therefore, the proposed S-box is generated according to Eq (12).

$$S_{\text{prop}}(x) = Ax^{-1} \oplus b \tag{12}$$

In Eq (12), x^{-1} denotes the multiplicative inverse of x in GF (2^8), A is the selected nonsingular binary matrix, and b is the selected constant vector.

Table 1. *The proposed S-box generated using the modified polynomial, affine matrix, and constant vector in hexadecimal form.*

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

Applying Eq (12) to all 256 possible input bytes produces

the proposed substitution table, which is presented in hexadecimal form in Table 1.

The obtained substitution table contains all hexadecimal values from 00 to FF exactly once. Therefore, the proposed S-box is bijective and can be used as a valid 8×8 substitution component in symmetric-key block cipher structures. Its cryptographic strength is evaluated using standard S-box criteria, including nonlinearity, differential uniformity, linear approximation probability, and the strict avalanche criterion.

3. Comparison of Results

3.1. Analysis of the Cryptographic Properties of the Proposed S-box

The efficiency and cryptographic performance of the proposed S-box were evaluated using a Python implementation. After generation, the substitution table was verified to satisfy the basic structural requirements of an 8×8 S-box. The analysis was then extended to widely used cryptographic indicators to assess the strength of the proposed construction.

First, the nonlinearity of the generated S-box was computed, since this criterion reflects the resistance of the substitution layer against linear cryptanalysis. A higher nonlinearity value indicates that the Boolean component functions of the S-box have lower correlation with affine functions, which is a desirable property for secure block cipher design.

Furthermore, Differential Probability (DP) was examined to measure resistance to differential attacks, and the maximum DP value was determined from the differential distribution table. The Strict Avalanche Criterion (SAC) was evaluated to analyze diffusion when one input bit is changed; minimum, maximum, mean, and standard-deviation values were calculated from the SAC matrix.

The obtained results were compared with those of existing S-box constructions reported in previous studies. This comparison demonstrates the relative performance of the proposed S-box and shows its effectiveness with respect to nonlinearity, differential approximation, and avalanche behavior.

3.2. Nonlinearity (N)

Nonlinearity is one of the most important cryptographic indicators used to evaluate the resistance of an S-box against linear cryptanalysis. In general, it measures how far the component Boolean functions of an S-box are from all affine Boolean functions. A higher nonlinearity value indicates that the input-output relationship of the S-box is more difficult to approximate by linear expressions, which is a desirable property for secure block cipher design.

For an n-variable Boolean function f, the Walsh spectrum used to compute nonlinearity is defined by Eq (13).

$$W_f(\omega) = \sum_{x \in GF(2)^n} (-1)^{f(x) \oplus (\omega \cdot x)} \tag{13}$$

In Eq (13), $\omega \in GF(2)^n$, and $\omega \cdot x$ denotes the scalar product over GF (2).

The nonlinearity of a Boolean function f is calculated using Eq (14).

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in GF(2)^n} |W_f(\omega)| \tag{14}$$

For an n×n S-box, nonlinearity is computed by evaluating the nonlinearity of its component Boolean functions. An 8×8 S-box has eight component Boolean functions, each of which is analyzed separately.

The nonlinearity values and algebraic degrees of the proposed S-box and selected 8×8 S-box constructions are presented in Table 2. The proposed S-box achieves a nonlinearity of 112 for all eight component Boolean functions; therefore, its minimum, maximum, and mean nonlinearity values are all 112.

This result indicates that the proposed S-box has a strong ability to reduce linear correlations between input and output bits. Such behavior is important because low correlation with affine functions makes the S-box more resistant to linear cryptanalytic attacks. The obtained nonlinearity results are also compared with those of existing S-box constructions in order to demonstrate the relative cryptographic strength of the proposed design.

Table 2. *Comparative Evaluation of Nonlinearity and Algebraic Degree for Selected 8×8 S-boxes.*

S-box	Year	Nonlinearity			deg(*f*)
		N_{min}	N_{max}	N_{mean}	
Proposed S-box	2026	112	112	112	7
AES [4]	1998	112	112	112	7
SM4 [15]	2012	112	112	112	7
O‘zDST [5]	2014	92	110	92	7
In [16]	2016	92	108	104	7

S-box	Year	Nonlinearity			deg(*f*)
		N_{min}	N_{max}	N_{mean}	
In [17]	2020	92	110	104	7
In [18]	2020	96	110	102	7
In [19]	2023	96	112	96	7
In [20]	2020	112	112	112	7
In [21]	2020	112	112	112	7
In [22]	2007	112	112	112	7

3.3. Differential Probability

Differential Probability (DP) is an essential criterion for measuring the resistance of an S-box to differential cryptanalysis. It determines how likely a specific input difference is transformed into a specific output difference.

Lower differential probability values are preferred, since they reduce the possibility of predicting output differences from known input differences.

For an S-box S, the differential probability associated with a nonzero input difference Δx and an output difference Δy is defined by Eq (15).

$$DP(\Delta x \to \Delta y) = \frac{|\{x \in GF(2)^n | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}|}{2^n}, \quad \Delta x \neq 0 \tag{15}$$

The numerator in Eq (15) is the cardinality of the set of inputs satisfying the stated differential relation. A lower maximum DP indicates a more uniform differential distribution and stronger resistance to differential cryptanalysis.

This criterion is closely related to the differential distribution table of the S-box. A smaller maximum DP value indicates a more uniform distribution of output differences and, consequently, better resistance against differential attacks.

In this study, the maximum DP value is used to summarize the differential behavior of the proposed substitution box.

3.4. Strict Avalanche Criterion

The Strict Avalanche Criterion (SAC) is used to evaluate the diffusion behavior of an S-box at the bit level. It describes how changes in input bits affect the corresponding output bits. A cryptographically strong S-box should produce a significant change in its output when only one input bit is complemented. Ideally, a single-bit change in the input should cause each output bit to change with a probability close to 0.5.

To evaluate the SAC property, all input pairs that differ in exactly one bit are considered. For each such pair, the corresponding S-box outputs are compared, and the number of changed output bits is recorded. The SAC value is then obtained by normalizing the number of output bit changes over all possible single-bit input variations.

Let S be an n ×n S-box. For the i-th input bit and j-th output bit, the SAC value is defined by Eq (16).

$$SAC_{i,j} = \frac{1}{2^n} \sum_{x \in GF(2)^n} \left(f_j(x) \oplus f_j(x \oplus e_i) \right) \tag{16}$$

In Eq (16), f_j denotes the j-th component Boolean function of the S-box, and e_i is the unit vector whose i-th coordinate is one.

The resulting SAC matrix provides a detailed view of the avalanche behavior of the proposed S-box. Values close to 0.5 indicate that output bits respond nearly randomly to one-bit input changes, which is an important diffusion property. The SAC matrix of the proposed S-box is presented in Table 3.

Table 3. *Strict Avalanche Criterion Matrix for the Proposed S-box.*

bit0	bit1	bit2	bit3	bit4	bit5	bit6	bit7
0.5156	0.5000	0.4531	0.5000	0.5000	0.5156	0.4531	0.5313
0.5313	0.4844	0.5156	0.5313	0.4531	0.4844	0.4531	0.5000
0.4844	0.5000	0.4844	0.5000	0.4844	0.5313	0.5156	0.4844

bit0	bit1	bit2	bit3	bit4	bit5	bit6	bit7
0.5156	0.5156	0.5156	0.5469	0.5156	0.5000	0.5313	0.5000
0.4688	0.5313	0.5156	0.5156	0.5469	0.4844	0.5156	0.5000
0.5156	0.4844	0.5313	0.5313	0.4844	0.5000	0.4375	0.4531
0.5000	0.5000	0.5469	0.4844	0.5469	0.5000	0.5000	0.4844
0.4531	0.4844	0.4688	0.5156	0.5313	0.4531	0.4531	0.5156

3.5. Linear Approximation Probability

Linear Approximation Probability (LAP) measures the extent to which the input-output relation of an S-box can be approximated by a linear expression. It is one of the most important indicators for evaluating resistance to linear cryptanalysis. A lower LAP value means that the S-box has weaker linear correlations, which makes it more difficult for an attacker to exploit linear relations between input and output masks.

Let Γ_x and Γ_γ be nonzero input and output masks, respectively. The Linear Approximation Probability of an S-box S is defined by Eq (17), where the dot product is computed over GF (2).

$$LAP = \max_{\Gamma_x,\Gamma_y\neq 0} \left| \frac{\left|\{x\in GF(2)^n | x\cdot\Gamma_x = S(x)\cdot\Gamma_y\}\right|}{2^n} - \frac{1}{2} \right| \quad (17)$$

The LAP value reflects the maximum deviation of the S-box from ideal random linear behavior. Therefore, a smaller LAP value is considered better from a cryptographic point of view. In this work, the LAP of the proposed S-box is computed and compared with the values reported for other S-box constructions.

This comparison helps to evaluate the effectiveness of the proposed S-box against linear cryptanalytic techniques.

3.6. Summary of the Cryptographic Evaluation

The proposed S-box was evaluated using standard cryptographic criteria, including nonlinearity, Strict Avalanche Criterion, Differential Probability, and Linear Approximation Probability. These indicators provide complementary information about the security of the substitution layer. Nonlinearity measures resistance to affine approximation, SAC describes bit-level diffusion, DP evaluates differential behavior, and LAP determines the strength of possible linear approximations.

The obtained results are compared with several existing S-box constructions reported in the literature. This comparative evaluation demonstrates whether the proposed S-box provides a competitive balance between nonlinear strength, differential resistance, linear resistance, and avalanche behavior.

The comparative assessment of SAC, LAP, and DP values for the proposed S-box and selected 8×8 S-box constructions is presented in Table 4.

Table 4. *Comparative Analysis of SAC, LAP, and DP Values for Selected 8×8 S-boxes.*

S-box	SAC				LAP	DP
	Min	Max	Mean	Standard deviation		
Proposed S-box	0.4375	0.5469	0.5	0.0272	0.0625	4/256
AES [4]	0.4531	0.5625	0.5048	0.0314	0.0625	4/256
SM4 [15]	0.4375	0.5625	0.4997	0.0346	0.0625	4/256
O‘zDST [5]	0.3750	0.6250	0.4956	0.0460	0.1406	10/256
In [16]	0.4063	0.5938	0.4988	0.0418	0.1406	10/256
In [17]	0.4063	0.5938	0.4988	0.0418	0.1406	10/256
In [18]	0.4219	0.6328	0.5110	0.0379	0.1094	12/256
In [19]	0.3906	0.5937	0.5002	0.0428	0.1250	12/256
In [20]	0.4375	0.5625	0.5060	0.0332	0.0625	4/256

S-box	SAC				LAP	DP
	Min	Max	Mean	Standard deviation		
In [21]	0.4375	0.5625	0.5010	0.0323	0.0625	4/256
In [22]	0.4375	0.5469	0.4978	0.0340	0.0625	4/256

4. Conclusions

This paper proposed a new 8×8 S-box by jointly modifying the principal algebraic and affine parameters of an AES-inspired inverse-affine construction. A new irreducible polynomial, a nonsingular affine matrix, and a constant vector were selected to generate the substitution table over GF (2^8).

The proposed S-box was evaluated using standard cryptographic criteria. Its minimum, maximum, and mean nonlinearity values are all 112, and its algebraic degree is 7. The SAC values range from 0.4375 to 0.5469, with a mean of 0.5 and a standard deviation of 0.0272. The LAP and DP values are 0.0625 and 4/256, respectively.

The comparative results show that the proposed S-box has competitive cryptographic characteristics relative to AES, SM4, O‘zDSt 1105: 2009, and several recently reported 8×8 S-boxes. In particular, it combines high nonlinearity, balanced avalanche behavior, and strong resistance to linear and differential attacks. These findings indicate that joint, controlled modification of AES-inspired algebraic and affine parameters is a reproducible approach to constructing secure substitution boxes for symmetric-key block ciphers.

Abbreviations

AES	Advanced Encryption Standard
S-box	Substitution Box
GF	Galois Field
SAC	Strict Avalanche Criterion
LAP	Linear Approximation Probability
DP	Differential Probability
IoT	Internet of Things

Author Contributions

Javokhir Abdurazzokov: Conceptualization, Formal Analysis, Investigation, Methodology, Software, Validation, Visualization, Writing – original draft, Writing – review & editing

Funding

This work was partially supported by the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan under grant number AL-9624115223 and partially supported by the Ministry of Digital Technologies of the Republic of Uzbekistan under scientific project number 36 entitled "Development of key generation algorithms for establishing secure communication at the transport layer".

Conflicts of Interest

The author declares no competing interests.

References

[1] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology 1991; 4: 3–72. https://doi.org/10.1007/BF00630563

[2] Matsui M. Linear Cryptanalysis Method for DES Cipher. Lecture Notes in Computer Science 1994; 765: 386–97. https://doi.org/10.1007/3-540-48285-7_33

[3] Nyberg K. Differentially uniform mappings for cryptography. Lecture Notes in Computer Science 1994; 765: 55–64. https://doi.org/10.1007/3-540-48285-7_6

[4] National Institute of Standards and Technology. Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1

[5] Sattarov AB, Abdurahimov BF. An algorithm for constructing S-boxes for block symmetric encryption. Universal Journal of Mathematics and Applications 2018; 1: 29–32. https://doi.org/10.32323/ujma.393155

[6] Lu Q, Zhu C, Wang G. A Novel S-Box Design Algorithm Based on a New Compound Chaotic System. Entropy 2019; 21: 1004. https://doi.org/10.3390/e21101004

[7] Zhu D, Tong X, Zhang M, Wang Z. A New S-Box Generation Method and Advanced Design Based on Combined Chaotic System. Symmetry (Basel) 2020; 12: 2087. https://doi.org/10.3390/sym12122087

[8] Picek S, Cupic M, Rotim L. A New Cost Function for Evolution of S-Boxes. Evolutionary Computation 2016; 24: 695–718. https://doi.org/10.1162/EVCO_a_00191

[9] Marochok S, Zajac P. Algorithm for Generating S-Boxes with Prescribed Differential Properties. Algorithms 2023; 16: 157. https://doi.org/10.3390/a16030157

[10] Kuznetsov O, Poluyanenko N, Frontoni E, Arnesano M, Smirnov O. Enhancing Smart Communication Security: A Novel Cost Function for Efficient S-Box Generation in Symmetric Key Cryptography. Cryptography 2024; 8: 17. https://doi.org/10.3390/cryptography8020017

[11] Abdurazzokov J. S-Box Generation Algorithm by Constructing the Non-Singular Adjacency Matrix Using the Genetic Algorithm. American Journal of Science, Engineering and Technology 2024; 9(1): 14–20. https://doi.org/10.11648/j.ajset.20240901.12

[12] Razaq A, Alhamzi G, Abbas S, Ahmad M, Razzaque A. Secure communication through reliable S-box design: A proposed approach using coset graphs and matrix operations. Heliyon 2023; 9: e15902. https://doi.org/10.1016/j.heliyon.2023. e15902

[13] Li L, Liu J, Guo Y, Liu B. A new S-box construction method meeting strict avalanche criterion. Journal of Information Security and Applications 2022; 66: 103135. https://doi.org/10.1016/j.jisa.2022.103135

[14] Saukhanova Z, Shakhmetova G, Sharipbay A, Barlybayev A, Raykul S, Khassenov A. Design of S-Boxes Based on Alternative Irreducible Polynomials. The Eurasia Proceedings of Science Technology Engineering and Mathematics 2025; 36: 102–109. https://doi.org/10.55549/epstem.1157

[15] Abdurakhimov B, Abdurazzokov J, Lingyun L. Analysis of the use of artificial neural networks in the cryptanalysis of the SM4 block encryption algorithm. *AIP Conf Proc* 2023; 2812: 020048. https://doi.org/10.1063/5.0161859

[16] Ahmad M, Malik M. Design of chaotic neural network based method for cryptographic substitution box. 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016; 864–8. https://doi.org/10.1109/ICEEOT.2016.7754809

[17] Zahid AH, Al-Solami E, Ahmad M. A Novel Modular Approach Based Substitution-Box Design for Image Encryption. IEEE Access 2020; 8: 150326–40. https://doi.org/10.1109/ACCESS.2020.3016401

[18] Hussain S, Jamal SS, Shah T, Hussain I. A Power Associative Loop Structure for the Construction of Non-Linear Components of Block Cipher. IEEE Access 2020; 8: 123492–506. https://doi.org/10.1109/ACCESS.2020.3005087

[19] Corona-Bermúdez E, Chimal-Eguía JC, Corona-Bermúdez U, Rivero-Ángeles ME. Chaos Meets Cryptography: Developing an S-Box Design with the Rössler Attractor. Mathematics 2023; 11: 4575. https://doi.org/10.3390/math11224575

[20] Siddiqui N, Yousaf F, Murtaza F, Ehatisham-ul-Haq M, Ashraf MU, Alghamdi AM, et al. A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. PLoS One 2020; 15: e0241890. https://doi.org/10.1371/journal.pone.0241890

[21] Nizam Chew LC, Ismail ES. S-box Construction Based on Linear Fractional Transformation and Permutation Function. Symmetry (Basel) 2020; 12: 826. https://doi.org/10.3390/sym12050826

[22] Chen G, Chen Y, Liao X. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. *Chaos Solitons Fractals* 2007; 31: 571–9. https://doi.org/ 10.1016/j.chaos.2005.10.022