JOIN (Jurnal Online Informatika)
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 11 Number 2 | December 2026: 314-325
DOI: 10.15575/join.v11i2.1841

Hybrid S-box Construction over GF(2^8) Using Irreducible Polynomial and Affine Transformation

Alamsyah[1]*, Yusuf Muhammad[2], Budi Prasetiyo[3], Yahya Nur Ifriza[4], Much Aziz Muslim[5], Shahrul Nizam Salahudin[6], Nur Atiqah Sia Abdullah[7], Yusuf Wisnu Mandaya[8]

[1,2,3,4,5]Department of Computer Science, Universitas Negeri Semarang, Semarang, Indonesia
[6]Faculty of Technology Management and Business, Universiti Tun Hussein Onn Malaysia, Malaysia
[7]College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Malaysia
[8]Universitas Islam Negeri Sunan Kudus, Indonesia

Article Info

Article history:

Received January 22, 2026
Revised June 11, 2026
Accepted June 11, 2026
Published September 26, 2026

Keywords:

AES
Affine Transformation
Irreducible Polynomial
S-box
SDGs

ABSTRACT

The S-box, also known as the substitution box, is an essential component in symmetric encryption because it provides the nonlinear mapping required to transform input bits into output bits. The most widely used S-box is the AES S-box, which is constructed using the irreducible polynomial $P_{\text{AES}}(x) = x^8 + x^4 + x^3 + x + 1$, an 8×8 affine matrix with the first row (10001111), and an 8-bit constant (01100011). This study presents a Hybrid S-box construction over GF(2^8) that combines irreducible-polynomial arithmetic and affine transformation to obtain a secure and lightweight substitution mapping. The proposed method uses the irreducible polynomial $P_{\text{Hybrid}}(x) = x^8 + x^7 + x^5 + x + 1$, an 8×8 affine matrix with the first row (01010111), and an 8-bit constant (00000000). The originality of this research lies in combining polynomial-based finite-field inversion and affine bit mixing to produce a reproducible Hybrid S-box design that balances cryptographic strength and implementation efficiency. The resulting Hybrid S-box is evaluated using six standard cryptographic indicators: Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion in terms of nonlinearity (BIC-NL) and avalanche (BIC-SAC), Differential Uniformity (DU), and Algebraic Degree (AD). The experimental results show that the proposed Hybrid S-box achieves NL = 112, SAC = 0.49756, BIC-NL = 112, BIC-SAC = 0.50119, DU = 4, and AD = 7. Compared with the AES S-box and recent S-box designs, the proposed Hybrid S-box attains AES-level nonlinearity and differential uniformity while producing SAC and BIC-SAC values closer to the ideal value of 0.5. These findings indicate that the proposed Hybrid S-box can enhance data security in Internet of Things devices, embedded controllers, and smart-card platforms. This work also supports Sustainable Development Goal 9 by contributing to secure, resilient, and resource-efficient digital infrastructure.

Corresponding Author:

Alamsyah,
Department of Computer Science, Faculty of Mathematics and Natural Sciences, Universitas Negeri Semarang, Indonesia
Email: alamsyah@mail.unnes.ac.id

1. INTRODUCTION

The rapid development of technology has provided significant convenience in data communication, storage, and processing. However, this development has also introduced new security challenges, particularly when transmitted and stored data become more vulnerable to unauthorized

access. Therefore, transmitted and stored data must be properly protected to ensure confidentiality and security. Several approaches have been proposed to secure data through encryption and data hiding. Alamsyah et al. [1] demonstrated that combining cryptographic primitives with bit-matching steganography can securely hide data without compromising the quality of the resulting stego image.

One of the most widely used encryption algorithms is the Advanced Encryption Standard (AES). This algorithm was originally known as Rijndael and was developed by Daemen and Rijmen [2]. After standardization, it was officially adopted as AES. The strength of AES is strongly influenced by the substitution box (S-box) used in its encryption process. The S-box provides nonlinear substitution by transforming input bits into output bits and contributes significantly to the confusion property of the cipher. The AES S-box is known for its strong nonlinearity and avalanche behavior, which are important factors in maintaining the security of the AES algorithm.

Many recent studies have attempted to construct S-boxes with stronger cryptographic properties. In a previous study, Alamsyah et al. [3] explored affine matrices while using the same irreducible polynomial as the AES S-box. Their method showed improvements in several security indicators compared with the standard AES S-box. Additional improvements were also proposed by modifying the ShiftRows operation and combining it with dynamic S-box generation [4]. Other researchers have developed S-box constructions using various mathematical and computational approaches, including combinatorial methods [5], hyperchaotic dynamics [6], [7], Frobenius automorphisms [8], two-dimensional chaotic polynomial maps [9], DNA-level randomization [10], hyperchaotic lattice frameworks [11], FPGA-oriented optimization [12], bent Boolean functions [13], double affine substitution [14], signal-sensing chaotic mappings [15], quadratic polynomial transformations [16], novel chaotic maps [17], Latin square ordering [18], Möbius group theory [19], multi-image three-dimensional chaotic schemes [20], discrete chaotic maps assisted by artificial bee colony optimization [21], three-layer S-box optimization [22], mixed pseudo-random PS map lattices [23], combined modifications of irreducible polynomials and affine matrices [24], and particle-swarm optimization strategies [25].

Moreover, several recent S-box constructions have been applied to image encryption and related security applications. Podder et al. [26] proposed a robust medical and color image cryptosystem using array indices and chaotic S-boxes to strengthen obfuscation and diffusion properties. Sani et al. [27] introduced an S-box construction method based on a chaotic piecewise map with watermarking applications. Ali and Ali [28] developed a color image encryption scheme based on a dynamic compound chaotic map integrated with S-boxes. These studies indicate that S-box construction remains an active research area for improving cryptographic security in different application domains.

However, existing S-box constructions continue to reveal an unresolved tension between cryptographic strength and practical implementability. Although various designs have attempted to improve resistance to linear and differential cryptanalysis, many still face limitations in simultaneously maintaining a high algebraic degree and computational efficiency for constrained platforms. For this reason, a more robust formulation is required to construct an S-box that can respond to both security and implementation demands. The method proposed in this study is therefore expected to produce a superior S-box that preserves strong cryptographic properties while remaining computationally lightweight for deployment in resource-constrained environments, particularly Internet of Things (IoT) devices and embedded systems.

Accordingly, this research aims to develop and evaluate a Hybrid S-box construction over GF(2^8) by combining irreducible-polynomial arithmetic with affine transformation. More specifically, this study addresses the challenge of obtaining an S-box that can sustain high nonlinearity and low differential uniformity while retaining a level of structural simplicity suitable for constrained digital infrastructure.

Based on the reviewed state of the art, chaotic-map-based, Boolean-function-based, FPGA-oriented, and optimization-based S-box constructions have been widely investigated. Nevertheless, these approaches often foreground image encryption performance or selected statistical indicators, while the interrelation among polynomial selection, affine mixing, differential behavior, algebraic degree, and lightweight implementation is not always articulated within a single coherent framework. The proposed method responds to this gap by linking the mathematical construction phase, the cryptographic evaluation phase, and the intended application in constrained-device environments.

The main contributions of this paper are fourfold. First, this paper proposes a reproducible Hybrid S-box construction based on the irreducible polynomial $P_{\text{Hybrid}}(x) = x^8 + x^7 + x^5 + x + 1$ and an invertible affine matrix selected to achieve balanced bit mixing. Second, this paper evaluates the

p-ISSN: 2528-1682
e-ISSN: 2527-9165

proposed Hybrid S-box using six cryptographic indicators: Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion in terms of nonlinearity (BIC-NL) and avalanche behavior (BIC-SAC), Differential Uniformity (DU), and Algebraic Degree (AD). Third, this paper presents a comparative analysis against the AES S-box and recent S-box designs in order to clarify the security position of the proposed construction. Fourth, this paper discusses the implementation relevance of the proposed Hybrid S-box for lightweight platforms, particularly IoT devices and embedded controllers.

2. METHOD

This study proposes a new S-box design, named the Hybrid S-box, by combining finite-field inversion over GF(2^8) with an affine transformation. The method consists of four main stages:

(1) Preparation and Parameter Selection,
(2) Hybrid S-box Construction,
(3) Cryptographic Property Evaluation, and
(4) Comparative Analysis.

The relationship among the stages of the proposed method is presented in Figure 1.

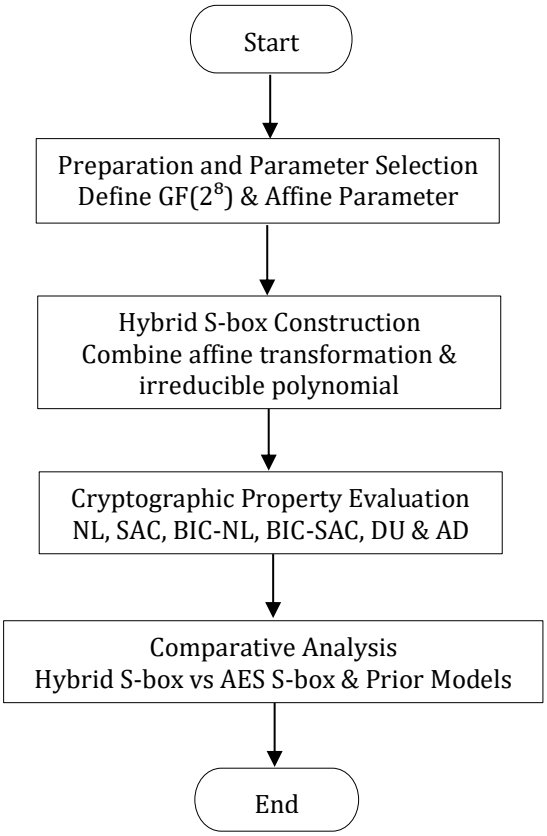

Figure 1. Methodological Flow of Hybrid S-box Design

The process begins by defining the irreducible polynomial in GF(2^8) and the affine parameters used in the construction. Next, finite-field inversion based on the selected irreducible polynomial is combined with affine transformation to generate the proposed Hybrid S-box. The generated Hybrid S-box is then evaluated using six standard cryptographic properties, namely Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion in terms of nonlinearity (BIC-NL) and avalanche (BIC-SAC), Differential Uniformity (DU), and Algebraic Degree (AD). Finally, the proposed Hybrid S-box is compared with the AES S-box and recent S-box designs from the literature.

The research phases are arranged as a problem-solution workflow. The preparation phase defines the mathematical domain and parameters required to construct a bijective 8×8 mapping. The construction phase transforms these parameters into a complete S-box lookup table. The evaluation phase then tests whether the constructed S-box satisfies the expected cryptographic properties by measuring resistance to linear, differential, independence-based, and algebraic weaknesses. Finally, the comparative phase positions the proposed solution against AES and recent state-of-the-art S-box designs. Thus, the method section is not intended as a theoretical review only, but as the operational procedure used to generate, verify, and compare the proposed S-box.

2.1. Preparation and Parameter Selection

a. Finite Field

All operations are performed over the finite field GF(2^8) defined by the irreducible polynomial given in Equation (1).

$$P_{\text{Hybrid}}(x) = x^8 + x^7 + x^5 + x + 1. \quad (1)$$

The irreducible polynomial $P_{\text{Hybrid}}(x) = x^8 + x^7 + x^5 + x + 1$ was selected because it is irreducible over GF(2). Therefore, arithmetic modulo $P_{\text{Hybrid}}(x)$ forms a valid finite field GF(2^8) with a unique multiplicative inverse for every non-zero element. This property is required to obtain a bijective inverse mapping and to avoid repeated S-box outputs.

b. Affine Transformation

The affine transformation matrix has been identified and explored in previous research [3]. The finite-field inversion output and the affine-transformation output are represented by the column vectors $x = (x_0, x_1, \dots, x_7)^T$and $y = (y_0, y_1, \dots, y_7)^T$, respectively. Both vectors use LSB-first ordering, where x_0 and y_0 are the least significant bits. The 8×8 affine matrix A is presented in Equation (2).

$$A=\begin{bmatrix} 0&1&0&1&0&1&1&1 \\ 1&0&1&0&1&0&1&1 \\ 1&1&0&1&0&1&0&1 \\ 1&1&1&0&1&0&1&0 \\ 0&1&1&1&0&1&0&1 \\ 1&0&1&1&1&0&1&0 \\ 0&1&0&1&1&1&0&1 \\ 1&0&1&0&1&1&1&0 \end{bmatrix} \quad (2)$$

The affine matrix was selected from previously explored candidates because it is invertible and provides balanced row-wise bit mixing. Therefore, it can diffuse the nonlinear inverse components across all output bits without reducing bijectivity or the nonlinearity class of the inverse-based mapping.

c. Affine Constant

The affine constant vector is set to $c = (0,0,0,0,0,0,0,0)^T$, or equivalently $c = (00000000)$, to simplify implementation while preserving the desired cryptographic strength. The use of a zero affine constant eliminates additional XOR operations with a non-zero constant, making the transformation more lightweight for constrained platforms. The affine transformation is formulated in Equation (3).

$$y = A \cdot x \oplus c \quad (3)$$

where multiplication and addition are performed over GF(2), and $\oplus$ denotes the XOR operation.

2.2. Hybrid S-box Construction

The S-box is generated through the following steps:

1. Field Initialization – Enumerate all input elements a ∈ {0, …, 255} and represent each element as an 8-bit vector.

2. Finite-Field Inversion – Compute the multiplicative inverse of each non-zero element in GF(2^8) using modular reduction by $P_{\text{Hybrid}}(x) = x^8 + x^7 + x^5 + x + 1$, while mapping zero to zero.
3. Affine Transformation – Represent the finite-field inversion output as the column vector $x = (x_0, x_1, \dots, x_7)^T$ using LSB-first ordering and apply $y = A \cdot x \oplus c$. Convert the output vector into the S-box output byte using $S(a) = \sum_{i=0}^{7} y_i \, 2^i$.
4. Table Generation – Collect all 256 unique outputs to form the final 16×16 S-box lookup table and verify bijectivity.

2.3. Cryptographic Property Evaluation

To assess the cryptographic strength of the constructed S-box, each output bit is treated as a Boolean function, as defined in Equation (4).

$$f_j : F_2^8 \to F_2, \quad j = 1, \dots, 8 \tag{4}$$

where:

f_j is the Boolean function representing the *j*-th output bit of the S-box
F_2 is the finite field of two elements {0,1}
j indexes the output bits ($1 \le j \le 8$)

Six standard criteria are evaluated:

1. Nonlinearity (NL)

NL measures the minimum Hamming distance between f_j and all affine functions $l(x)$ as expressed in Equation (5).

$$\text{NL}(f_j) = 2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} \left| W_{f_j}(a) \right| \tag{5}$$

where:

$n = 8$ is the number of input bits,
$a \in F_2^n$ is a frequency vector for the Walsh-Hadamard transform,
$W_{f_j}(a) = \sum_{x \in F_2^n} (-1)^{f_j(x) \oplus \langle a, x \rangle}$ is the Walsh spectrum of f_j,
$\langle a, x \rangle = \bigoplus_{k=1}^{n} a_k x_k$ is the inner product modulo two,
$\oplus$ denotes XOR, or addition modulo two.

2. Strict Avalanche Criterion (SAC)

SAC evaluates the probability that flipping a single input bit changes the output bit f_j, computed according to Equation (6).

$$\widehat{\text{SAC}}(i, j) = \frac{1}{2^n} \sum_{x \in F_2^n} \left[f_j(x) \oplus f_j(x \oplus e_i) \right] \tag{6}$$

where:

$i \in \{1, \dots, n\}$ is the position of the input bit being toggled,
e_i is the unit vector with a 1 in position i and zeros elsewhere,
$x \oplus e_i$ represents the input vector with bit i flipped

3. Bit Independence Criterion – Nonlinearity (BIC-NL)

BIC-NL measures the nonlinearity of the XOR of every pair of output bits f_j and f_k as given in Equation (7).

$$\text{BIC-NL} = \frac{2}{m(m-1)} \sum_{1 \le j < k \le m} \left[2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} \left| W_{f_j \oplus f_k}(a) \right| \right] \quad (7)$$

where:

$m = 8$ is the number of output bits, the summation runs over all distinct output bit pairs j, k

$W_{f_j \oplus f_k}(a)$ is the Walsh spectrum of the XOR of output bits j and k.

4. Bit Independence Criterion – SAC (BIC-SAC)

BIC-SAC evaluates the independence of avalanche effects between pairs of output bits when a single input bit is toggled, as described in Equation (8).

$$\widehat{BIC-SAC} = \frac{2}{m(m-1)n} \sum_{i=1}^{n} \sum_{1 \le j < k \le m} \frac{1}{2^n} \sum_{x \in F_2^n} \left[\Delta_j^{(i)}(x) \oplus \Delta_k^{(i)}(x) \right] \quad (8)$$

where:

$\Delta_j^{(i)}(x) = f_j(x) \oplus f_j(x \oplus e_i)$ is the avalanche bit of output j when the i-th input bit is flipped

The outer summations average the independence measure over all input bit positions i and all unordered pairs of output bits j, k

5. Differential Uniformity (DU)

Differential Uniformity (DU) measures the maximum number of input pairs that produce the same output difference for a given non-zero input difference. Let S be an $n \times n$ S-box defined as $S: GF(2^n) \to GF(2^n)$. For each input difference $a \in GF(2^n)$, $a \neq 0$, and output difference $b \in GF(2^n)$, the difference distribution table (DDT) entry is defined in Equation (9).

$$\delta_S(a, b) = \#\{x \in GF(2^n) \mid S(x) \oplus S(x \oplus a) = b\} \quad (9)$$

The Differential Uniformity of the S-box is then defined in Equation (10).

$$DU(S) = \max_{\substack{a \in GF(2^n), a \neq 0 \\ b \in GF(2^n)}} \delta_S(a, b) \quad (10)$$

where $\#\{\cdot\}$ denotes the number of elements in the set, a is the input difference, b is the output difference, and $\oplus$ denotes bitwise XOR. A smaller DU value indicates stronger resistance to differential cryptanalysis. For an 8×8 S-box, $DU = 4$ is widely used as a strong benchmark, including for the AES S-box.

6. Algebraic Degree (AD)

Algebraic Degree (AD) measures the highest degree of the algebraic normal form (ANF) of the coordinate Boolean functions of an S-box. Let an $n \times n$ S-box be represented by n coordinate Boolean functions as shown in Equation (11).

$$S(x) = (f_1(x), f_2(x), \ldots, f_n(x)), f_j: F_2^n \to F_2 \quad (11)$$

Each coordinate Boolean function $f_j(x)$ can be expressed in algebraic normal form as given in Equation (12).

$$f_j(x) = \bigoplus_{I \subseteq \{1,2,\ldots,n\}} a_I \prod_{i \in I} x_i \quad (12)$$

where $a_I \in F_2$ is the coefficient of the monomial $\prod_{i \in I} x_i$, and $\oplus$ denotes addition over F_2. The algebraic degree of f_j is defined in Equation (13).

p-ISSN: 2528-1682
e-ISSN: 2527-9165

$$\deg(f_j) = \max\{|\ I\ ||\ a_I \neq 0\} \quad (13)$$

The Algebraic Degree of the S-box is then defined as the maximum algebraic degree among all coordinate Boolean functions, as shown in Equation (14).

$$AD(S) = \max_{1 \leq j \leq n} \deg(f_j) \quad (14)$$

A higher AD value indicates that the S-box coordinate functions cannot be represented by low-degree Boolean expressions, thereby improving resistance against algebraic attacks. For an 8×8 S-box, the maximum achievable algebraic degree for a bijective mapping is 7, which is also achieved by the AES S-box.

2.4. Comparative Analysis

The final stage of this methodology involves a comparative analysis to assess the performance of the proposed Hybrid S-box against the AES S-box and recent S-boxes from previous studies. This comparison is conducted using the main cryptographic indicators, namely Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion in terms of BIC-NL and BIC-SAC, Differential Uniformity (DU), and Algebraic Degree (AD).

3. RESULTS AND DISCUSSION

The proposed Hybrid S-box was generated using the irreducible polynomial $P_{\text{Hybrid}}(x) = x^8 + x^7 + x^5 + x + 1$, the selected 8×8 affine matrix, and the affine constant $c = (00000000)$. The evaluation was conducted to determine whether the proposed construction satisfies the main cryptographic requirements of a secure 8×8 S-box. The evaluated properties include Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion in terms of nonlinearity (BIC-NL) and avalanche (BIC-SAC), Differential Uniformity (DU), and Algebraic Degree (AD).

The strong nonlinearity achieved by the proposed Hybrid S-box is mathematically supported by the combination of finite-field inversion over GF(2^8) and an invertible affine transformation. The inverse mapping over GF(2^8) is known to provide a highly nonlinear permutation, while the selected affine matrix redistributes the nonlinear components across the output bits without reducing bijectivity. Since affine transformations preserve the nonlinearity class of inverse-based mappings, the proposed construction can maintain NL = 112. In addition, the selected polynomial and affine matrix produce balanced output-bit interactions, which contributes to SAC and BIC-SAC values that are close to the ideal value of 0.5 and supports the observed DU = 4 and AD = 7 results.

3.1. Multiplicative Inverse Table

The multiplicative inverse transformation is widely used in modern cryptography because it produces a nonlinear mapping with strong resistance to linear approximation. Although the operation can be implemented efficiently over GF(2^8), its input-output pattern is difficult to approximate using linear functions. The inverse transformation is also utilized in constructing the multiplicative inverse matrix, as defined in Equation (15).

$$a \cdot a^{-1} \equiv 1 (\text{mod}\ P_{\text{Hybrid}}(x)) \quad (15)$$

According to Equation (15), each non-zero element a has a unique multiplicative inverse a^{-1} over GF(2^8). The selected irreducible polynomial, $P_{\text{Hybrid}}(x) = x^8 + x^7 + x^5 + x + 1$, differs from the irreducible polynomial used in the standard AES S-box. The result of the implementation of Equation (15) is a multiplicative inverse matrix. The 16 × 16 multiplicative inverse matrices with hexadecimal or decimal values are shown in Tables 1 and 2.

Table 1. Hybrid Multiplicative Inverse Matrix (Hexadecimal)

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

Table 2. Hybrid Multiplicative Inverse Matrix (Decimal)

0	1	209	158	185	235	79	86	141	50	164	243	246	129	43	89
151	55	25	122	82	176	168	127	123	18	145	143	196	81	253	132
154	124	202	204	221	188	61	174	41	40	88	14	84	228	238	148
236	112	9	140	153	183	150	17	98	180	249	192	175	38	66	241
77	206	62	240	101	212	102	131	191	230	94	108	207	64	87	6
197	29	20	177	44	229	7	78	42	15	114	147	119	97	74	109
118	93	56	181	213	68	70	130	157	251	138	199	75	95	217	245
49	237	90	146	173	211	96	92	134	233	19	24	33	155	169	23
247	13	103	71	31	252	120	232	227	166	106	198	51	8	144	27
142	26	115	91	47	239	54	16	182	52	32	125	250	104	3	208
179	215	223	170	10	242	137	226	22	126	163	222	210	116	39	60
21	83	214	160	57	99	152	53	234	4	225	200	37	220	231	72
59	248	255	219	28	80	139	107	187	224	34	205	35	203	65	76
159	2	172	117	69	100	178	161	244	110	254	195	189	36	171	162
201	186	167	136	45	85	73	190	135	121	184	5	48	113	46	149
67	63	165	11	216	111	12	128	193	58	156	105	133	30	218	194

a. Proposed Hybrid S-box

The proposed Hybrid S-box is constructed by applying the selected affine transformation to the finite-field inverse values generated over GF(2^8). The construction begins by enumerating all input elements $a \in \{0, \ldots, 255\}$, representing each element as an 8-bit vector, computing the finite-field inverse using $P_{\text{Hybrid}}(x)$, and applying the affine transformation $y = A \cdot x \oplus c$. The constant vector $c = (00000000)$ is used to simplify the transformation while preserving the desired cryptographic properties.

The resulting Hybrid S-box is presented in hexadecimal and decimal forms in Tables 3 and 4. The generated table contains 256 unique output values, confirming that the proposed Hybrid S-box is bijective. Bijectivity is an important requirement for block cipher substitution layers because it ensures that each input value maps to a unique output value and that the inverse substitution can be defined during decryption.

p-ISSN: 2528-1682
e-ISSN: 2527-9165

Table 3. Proposed Hybrid S-box (Hexadecimal)

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

Table 4. Proposed Hybrid S-box (Decimal)

0	174	184	47	179	175	151	166	54	98	56	48	36	249	83	154
244	118	49	188	28	104	247	168	18	183	19	107	70	239	162	237
149	91	212	51	119	167	94	16	14	160	52	146	251	147	187	7
230	148	219	152	102	33	90	68	35	210	24	252	190	50	246	109
202	110	173	195	106	172	153	164	84	206	211	177	192	171	8	231
232	139	80	198	26	61	73	57	253	60	201	78	221	208	131	31
115	32	74	124	2	17	76	10	220	69	127	181	45	125	205	215
145	72	105	224	227	229	126	142	176	242	25	159	123	59	89	163
138	97	55	226	214	12	225	92	218	101	86	27	204	117	189	108
197	194	103	199	233	21	216	234	143	133	213	245	235	11	243	22
155	95	42	170	40	158	140	116	13	6	113	132	75	46	156	240
254	178	241	130	228	141	200	43	1	186	135	137	193	217	96	222
185	182	255	144	37	65	209	248	238	41	136	157	38	122	5	100
129	93	77	128	191	196	53	44	121	236	81	15	9	111	4	223
39	64	203	34	180	85	112	250	30	79	29	20	63	58	71	169
88	3	150	134	99	66	207	87	82	23	114	165	67	120	62	161

b. Cryptographic Evaluation

After the proposed Hybrid S-box was generated, its cryptographic strength was evaluated using six standard indicators: Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion in terms of nonlinearity (BIC-NL) and avalanche (BIC-SAC), Differential Uniformity (DU), and Algebraic Degree (AD). NL measures the resistance of the S-box against linear approximation, while SAC evaluates the avalanche behavior when a single input bit is changed. BIC-NL and BIC-SAC measure the independence between output bits in terms of nonlinearity and avalanche behavior. DU evaluates resistance to differential cryptanalysis, whereas AD measures resistance to low-degree algebraic representation.

The experimental results show that the proposed Hybrid S-box achieves NL = 112, SAC = 0.49756, BIC-NL = 112, BIC-SAC = 0.50119, DU = 4, and AD = 7. These values indicate that the proposed

Hybrid S-box has strong cryptographic properties. The NL value of 112 is equal to the standard AES S-box and the design in [14], and higher than the values reported in [5], [7], [11], [12], and [13]. This result shows that the proposed Hybrid S-box achieves AES-level nonlinearity and provides strong resistance to linear cryptanalysis.

Table 5 presents a comparison between the proposed Hybrid S-box, the standard AES S-box, and several recent S-box designs from the literature using six cryptographic indicators: NL, SAC, BIC-NL, BIC-SAC, DU, and AD. The comparison shows that the proposed Hybrid S-box achieves competitive performance across all evaluated metrics, particularly by obtaining AES-level NL, BIC-NL, DU, and AD, while producing SAC and BIC-SAC values close to the ideal value of 0.5.

Table 5. Cryptographic Strength Comparison

S-box Design	NL	SAC	BIC-NL	BIC-SAC	DU	AD
Proposed Hybrid	112	0.49756	112	0.50119	4	7
Standard AES [2]	112	0.50488	112	0.50460	4	7
In [5]	96	0.51001	103	0.49665	10	7
In [7]	94	0.50415	104	0.50272	10	7
In [11]	94	0.50610	103	0.50377	12	7
In [12]	92	0.49951	105	0.50426	12	7
In [13]	90	0.50806	101	0.49254	20	7
In [14]	112	0.50317	112	0.50279	4	7

The SAC value of the proposed Hybrid S-box is 0.49756, which is very close to the ideal value of 0.5. Its deviation from the ideal SAC value is $|0.5 - 0.49756| = 0.00244$. This deviation is smaller than that of the standard AES S-box, which has a deviation of $|0.5 - 0.50488| = 0.00488$. Compared with the other designs, the proposed Hybrid S-box also shows a competitive avalanche property. Although the design in [12] has a SAC value of 0.49951, which is slightly closer to 0.5, its NL is lower and its DU is higher than those of the proposed Hybrid S-box. Therefore, the proposed design provides a more balanced cryptographic profile.

The BIC-NL value of the proposed Hybrid S-box is 112, which is equal to the standard AES S-box and the design in [14]. This value is higher than those reported in [5], [7], [11], [12], and [13]. A high BIC-NL value indicates that the XOR combinations of output-bit pairs maintain strong nonlinearity. Therefore, the proposed Hybrid S-box provides strong bit independence in terms of nonlinear behavior.

The BIC-SAC value of the proposed Hybrid S-box is 0.50119, which is also very close to the ideal value of 0.5. Its deviation from the ideal value is $|0.5 - 0.50119| = 0.00119$. This deviation is smaller than that of the standard AES S-box and all compared designs in Table 5. This result indicates that the proposed Hybrid S-box provides highly balanced avalanche independence between output-bit pairs.

The proposed Hybrid S-box obtains the same DU value as the standard AES S-box and the design in [14], namely DU = 4. This value is lower than the DU values reported in [5] and [7], which are 10, in [11] and [12], which are 12, and in [13], which is 20. Since a lower DU value indicates stronger resistance to differential cryptanalysis, the proposed Hybrid S-box shows a strong differential property comparable to AES.

The AD value of the proposed Hybrid S-box is 7, which is equal to that of the standard AES S-box and all compared designs listed in Table 5. An algebraic degree of 7 is the maximum attainable degree for the coordinate functions of an 8×8 bijective S-box. Therefore, the proposed Hybrid S-box maintains a high algebraic degree and provides resistance against low-degree algebraic attacks.

Overall, the proposed Hybrid S-box demonstrates a balanced and competitive cryptographic profile. Its performance reaches the level of the AES S-box in terms of NL, BIC-NL, DU, and AD, while its SAC and BIC-SAC values remain close to the ideal value of 0.5. In comparison with recent S-box designs, the proposed Hybrid S-box offers stronger resistance to linear and differential cryptanalysis than most alternatives reported in Table 5, without sacrificing avalanche behavior or bit independence. These findings indicate that the proposed construction is not only mathematically robust but also practically relevant for strengthening data security in constrained digital environments, including Internet of Things devices, embedded controllers, and smart-card platforms.

To make the relevance to SDG 9 more concrete, the proposed design was also analyzed under an on-the-fly ARM Cortex-M implementation model. Unlike the AES affine transformation, which applies the non-zero affine constant 0x63, the proposed Hybrid S-box uses c = 0x00 and therefore eliminates one byte-wise XOR operation with the affine constant for each generated S-box output. If this XOR is compiled as a single-cycle exclusive-OR operation, the estimated saving is approximately 1 clock cycle per

substituted byte, 16 clock cycles per 128-bit round, and about 160 clock cycles over ten AES-like rounds. This advantage mainly applies to on-the-fly generation or memory-saving implementations; if both S-boxes are stored as 256-byte lookup tables, their runtime lookup costs are expected to be comparable.

4. CONCLUSION

This study has presented a Hybrid S-box construction over GF(2^8) by integrating finite-field inversion, defined through the irreducible polynomial $P_{\text{Hybrid}}(x) = x^8 + x^7 + x^5 + x + 1$, with an invertible affine transformation. The proposed construction was developed to generate a bijective 8×8 substitution mapping that combines strong cryptographic characteristics with a structurally simple design suitable for lightweight implementation.

The experimental results demonstrate that the proposed Hybrid S-box achieves $NL = 112$, $SAC = 0.49756$, $BIC\text{-}NL = 112$, $BIC\text{-}SAC = 0.50119$, $DU = 4$, and $AD = 7$. These results show that the proposed Hybrid S-box reaches AES-level performance in terms of nonlinearity, bit-independence nonlinearity, differential uniformity, and algebraic degree. Moreover, its SAC and BIC-SAC values remain close to the ideal value of 0.5, indicating balanced avalanche behavior and strong independence among output bits.

Compared with the standard AES S-box and recent S-box designs, the proposed Hybrid S-box demonstrates a competitive cryptographic profile. It achieves the same NL, DU, and AD values as the AES S-box, while producing SAC and BIC-SAC values that are closer to the ideal value. This comparison indicates that the proposed construction offers strong resistance to linear cryptanalysis, differential cryptanalysis, and low-degree algebraic representation.

From an implementation perspective, the use of an 8-bit zero affine constant, $c = (00000000)$, simplifies the affine transformation and supports a lightweight design. Therefore, the proposed Hybrid S-box is suitable for strengthening data security in resource-constrained environments, including Internet of Things devices, embedded controllers, and smart-card platforms. In a broader context, this work also supports Sustainable Development Goal 9 by contributing to the development of secure, resilient, and resource-efficient digital infrastructure. For a concrete ARM Cortex-M on-the-fly implementation estimate, the zero affine constant removes one affine-constant XOR per S-box output, corresponding to about 1 clock cycle per substituted byte, 16 clock cycles per 128-bit round, and 160 clock cycles over ten AES-like rounds compared with the AES affine constant step.

Future work will focus on hardware and software implementation analysis of the proposed Hybrid S-box, including memory usage, execution time, throughput, power consumption, and energy efficiency on constrained platforms such as ARM Cortex-M-based microcontrollers and FPGA devices. Further research may also evaluate the integration of the proposed Hybrid S-box into complete lightweight block cipher architectures.

ACKNOWLEDGEMENTS

This research was supported by Universitas Negeri Semarang through the provision of research facilities and institutional support that enabled this study to be conducted.

REFERENCES

[1] Alamsyah, M. A. Muslim, and B. Prasetiyo, "Data hiding security using bit matching-based steganography and cryptography without changing the stego image quality," *Journal of Theoretical and Applied Information Technology*, vol. 82, no. 1, pp. 106–112, 2015.

[2] J. Daemen and V. Rijmen, *The Design of Rijndael: AES — The Advanced Encryption Standard*, 2nd ed. Berlin, Heidelberg: Springer, 2020, doi: 10.1007/978-3-662-60769-5.

[3] Alamsyah, A. Setiawan, A. T. Putra, et al., "AES S-box modification uses affine matrices exploration for increased S-box strength," *Nonlinear Dynamics*, vol. 113, pp. 3869–3890, 2025, doi: 10.1007/s11071-024-10414-3.

[4] Alamsyah, B. Prasetiyo, and M. N. Ardian, "Enhancement security AES algorithm using a modification of transformation ShiftRows and dynamic S-box," *Journal of Physics: Conference Series*, vol. 1567, no. 3, Art. no. 032025, 2020, doi: 10.1088/1742-6596/1567/3/032025.

[5] F. Artuğer, "Strong S-box construction approach based on Josephus problem," *Soft Computing*, vol. 28, pp. 10201–10213, 2024, doi: 10.1007/s00500-024-09751-7.

[6] Y. Ma, Y. Tian, L. Zhang, and P. Zuo, "Two-dimensional hyperchaotic effect coupled mapping lattice and its application in dynamic S-box generation," *Nonlinear Dynamics*, vol. 112, pp. 17445–17476, 2024, doi: 10.1007/s11071-024-09907-y.
[7] H. Ning, G. Zhao, Z. Li, S. Gao, Y. Ma, and Y. Dong, "A novel method for constructing dynamic S-boxes based on a high-performance spatiotemporal chaotic system," *Nonlinear Dynamics*, vol. 112, pp. 1487–1509, 2024, doi: 10.1007/s11071-023-09125-y.
[8] R. Ali, J. Ali, P. Ping, and M. K. Jamil, "A novel S-box generator using Frobenius automorphism and its applications in image encryption," *Nonlinear Dynamics*, vol. 112, pp. 19463–19486, 2024, doi: 10.1007/s11071-024-10003-4.
[9] W. Q. Wu and L. S. Kong, "Image encryption algorithm based on a new 2D polynomial chaotic map and dynamic S-box," *Signal, Image and Video Processing*, vol. 18, pp. 3213–3228, 2024, doi: 10.1007/s11760-023-02984-3.
[10] A. Chemlal, H. Tabti, H. El Bourakkadi, H. Rrghout, A. Jarjar, and A. Benazzi, "DNA-level action accompanied by Vigenere using strong pseudo random S-box for color image encryption," *Multimedia Tools and Applications*, vol. 84, pp. 19915–19946, 2025, doi: 10.1007/s11042-024-19774-9.
[11] S. Zhou, Y. Qiu, X. Wang, and Y. Zhang, "Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box," *Nonlinear Dynamics*, vol. 111, pp. 9571–9589, 2023, doi: 10.1007/s11071-023-08312-1.
[12] Y. Aydin, A. M. Garipcan, and F. Özkaynak, "A novel secure S-box design methodology based on FPGA and SHA-256 hash algorithm for block cipher algorithms," *Arabian Journal for Science and Engineering*, vol. 50, pp. 1247–1260, 2025, doi: 10.1007/s13369-024-09251-8.
[13] S. Arshad and M. Khan, "Construction of nonlinear component based on bent Boolean functions," *Computational and Applied Mathematics*, vol. 43, pp. 1–18, 2024, doi: 10.1007/s40314-023-02545-x.
[14] M. Khan, S. S. Jamal, M. M. Hazzazi, K. M. Ali, I. Hussain, and M. Asif, "An efficient image encryption scheme based on double affine substitution box and chaotic system," *Integration*, vol. 81, pp. 108–122, 2021, doi: 10.1016/j.vlsi.2021.05.007.
[15] C. Ding and R. Xue, "Signal-sensing dynamic S-box image encryption with 2D Griewank–sin map," *Nonlinear Dynamics*, vol. 111, pp. 22595–22620, 2023, doi: 10.1007/s11071-023-08985-8.
[16] A. H. Zahid, H. Rashid, M. M. U. Shaban, S. Ahmad, E. Ahmed, M. T. Amjad, et al., "Dynamic S-box design using a novel square polynomial transformation and permutation," *IEEE Access*, vol. 9, pp. 82390–82401, 2021, doi: 10.1109/ACCESS.2021.3086717.
[17] A. Manzoor, A. H. Zahid, and M. T. Hassan, "A new dynamic substitution box for data security using an innovative chaotic map," *IEEE Access*, vol. 10, pp. 74164–74174, 2022, doi: 10.1109/ACCESS.2022.3184012.
[18] Z. Hua, J. Li, Y. Chen, and S. Yi, "Design and application of an S-box using complete Latin square," *Nonlinear Dynamics*, vol. 104, pp. 807–825, 2021, doi: 10.1007/s11071-021-06308-3.
[19] B. Arshad, N. Siddiqui, Z. Hussain, and M. Ehatisham-ul-Haq, "A novel scheme for designing secure substitution boxes (S-boxes) based on Möbius group and finite field," *Wireless Personal Communications*, vol. 124, pp. 3527–3548, 2022, doi: 10.1007/s11277-022-09524-1.
[20] M. Tanveer, T. Shah, A. Rehman, A. Ali, G. F. Siddiqui, et al., "Multi-images encryption scheme based on 3D chaotic map and substitution box," *IEEE Access*, vol. 9, pp. 73924–73937, 2021, doi: 10.1109/ACCESS.2021.3081362.
[21] M. Long and L. Wang, "S-box design based on discrete chaotic map and improved artificial bee colony algorithm," *IEEE Access*, vol. 9, pp. 86144–86154, 2021, doi: 10.1109/ACCESS.2021.3069965.
[22] Y. Su, X. Tong, M. Zhang, and Z. Wang, "A new S-box three-layer optimization method and its application," *Nonlinear Dynamics*, vol. 111, pp. 2841–2867, 2023, doi: 10.1007/s11071-022-07956-9.
[23] P. Zhou, J. Du, K. Zhou, and S. Wei, "2D mixed pseudo-random coupling PS map lattice and its application in S-box generation," *Nonlinear Dynamics*, vol. 103, pp. 1151–1166, 2021, doi: 10.1007/s11071-020-06098-0.
[24] Alamsyah, "Improving the quality of AES S-box by modifications irreducible polynomial and affine matrix," in *Proc. 2020 5th International Conference on Informatics and Computing (ICIC)*, 2020, doi: 10.1109/ICIC50835.2020.9288567.
[25] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami, and W. Alhakami, "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications," *IEEE Access*, vol. 8, pp. 116132–116147, 2020, doi: 10.1109/ACCESS.2020.3004449.
[26] D. Podder, S. Deb, D. Banik, N. Kar, and A. K. Sahu, "Robust medical and color image cryptosystem using array index and chaotic S-box," *Cluster Computing*, vol. 27, pp. 4321–4346, 2024, doi: 10.1007/s10586-024-04584-3.
[27] R. H. Sani, S. Behnia, and J. Ziaei, "Construction of S-box based on chaotic piecewise map: Watermark application," *Multimedia Tools and Applications*, vol. 82, pp. 1131–1148, 2023, doi: 10.1007/s11042-022-13278-0.
[28] T. S. Ali and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box," *Multimedia Tools and Applications*, vol. 81, pp. 20585–20609, 2022, doi: 10.1007/s11042-022-12268-6.