Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about

Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Construction of Substitution Box using Affine Transformation over a Galois Field

Iqrar pali
Department of BS & RS SBBU nawab shah. iqraar.palli@sbbusba.edu.pk

Iqrar Ali Pali
Department of mathematics and statistics QUEST nawab shah
iqraralipali@quest.edu.pk

Muhammad Afzal Soomro
Department of mathematics and statistics QUEST nawab shah
m.a.soomro@quest.edu.pk

Sadarullah Lund
Department of mathematics and statistics QUEST nawab shah
sadarullah786@gmail.com

Waseem Khan
Department of BS & RS SBBU nawab shah
waseemkhansba@gmail.com

ABSTRACT

In symmetric-key encryption systems, S-boxes are fundamental com-ponents that provide confusion, prevent statistical and algebraic attacks, and they are integrated into the design of the encryption algorithm. This paper describes the detailed construction of S-boxes that are cryptograph-ically secure, in particular ones created using affine mappings. The con-struction operates on the finite field, $GF(2^8)$, in the field of cryptography. The process begins by computing the multiplicative inverse of the input byte with respect to a chosen irreducible polynomial. This byte inversion step alone is sufficient to guarantee a high degree of non-linearity and also and gives a one-to-one mapping of input and output values. The val-ues that have been inverse mapped are then processed through an affine transformation in $GF(2^8)$ that is defined by an affine vector and an invert-ible matrix. This particular affine transformation is chosen to optimize the diffusion of the bits, eliminate fixed points and provide an additional layer of protection from potential attacks. The processed S-Box under-goes a preliminary evaluation using various possible established techniques in cryptography: evaluation of its differential uniformity, linearity, strict avalanche criteria (SAC), bit independence criteria (BIC), and linear ap-proximation. Experimental results reveal that the constructed S-Box has a balanced output distribution and exhibits proper output uncertainty, with low volumes of differential and linear cryptanalysis. Because the case requires an affine transformation, the inverse S-Box will also exist, which serves the proposed design for both encryption and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

decryption. Addition-ally, the proposed design retains low computational complexity suitable for efficient implementations in both hardware and software. These at-tributes confirm that the suggested affine transformation-based S-Box will serve efficiently in modern block ciphers, especially in low-resource and lightweight cryptographic applications.

Keywords—Symmetric-Key Encryption, Galois Field, Substitution Box and Non-linearity

1 Introduction

With the rapid advancement of communication technologies, maintaining data confidentiality has become an increasingly complex challenge. As a result, re-searchers have devoted significant attention to developing mechanisms that safe-guard transmitted information while ensuring both its integrity and authentic-ity. Among the various cryptographic approaches, *block ciphers* form the back-bone of modern cryptosystems, and within these systems, the replacement box increase Nonlinearity and resistance against assaults.

The S-box transforms input bit patterns into corresponding output patterns, introducing confusion and complexity into the encryption process. Making cryp-tographic methods safe against differential and linear cryptanalysis depends on this nonlinear transformation. It is widely recognized that the overall secu-rity of a block cipher is strongly influenced by the design quality of its S-box. Well-designed S-boxes are essential to well-known cryptographic standards like the Data Encryption Standard (DES), the International Data Encryption Al-gorithm (IDEA), and the Advanced Encryption Standard (AES).Consequently, the cryptographic strength of a cipher is closely tied to the robustness of its underlying substitution mechanism.

The introduction of DES in 1977 [29] marked a major milestone in the evo-lution of cryptography. However, its eventual compromise by university re-searchers revealed the need for more advanced encryption schemes. This mo-tivated the development of the Advanced Encryption Standard (AES), which was officially adopted in 2002. AES quickly became a global standard due to its efficiency, high security, and proven resistance to numerous cryptanalytic attacks. Its implementation significantly strengthened data protection and con-fidentiality in digital communication systems [26].

The performance of any encryption algorithm is largely influenced by the strength of its S-box. A poorly constructed S-box can introduce vulnerabilities that compromise the entire cryptosystem. Therefore, evaluating its robustness is a necessary step before deployment. There are many widely used analyti-cal measures. used to evaluate the quality of S-boxes, including the bit inde-pendence criterion (BIC),the stringent avalanche criterion (SAC), nonlinearity (NL), the differential approximate, The linear approximation probability (LAP) and the imputation probability (DAP) are the two probabilities. Collectively, these parameters provide valuable insight into the cryptographic resistance and overall performance of an S-box. Extensive research has been carried out on S-box design and analysis, as discussed in studies such as [14] and [11]. These works offer theoretical and practical contributions toward improving substitution mechanisms. Hayat et al. [17] proposed an approach based on elliptic curves, where ordinate values of the curve were used in the construction process. Similarly, Altaleb et al. [5] em-ployed projective general linear groups to develop more efficient S-boxes. Such studies demonstrate continuous progress toward achieving both high security and practical efficiency in cryptographic transformations.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about

Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

An established method of constructing S-Boxes consists of performing the multiplicative inverse of elements from $GF\ (2^8)$. The inversion operation cre-ates high levels of nonlinearity and guarantees that the S-Box is bijective, a textbook requirement for the S-Box to allow for both reversible encryption and decryption. While effective, the multiplicative inverse alone may create some negative structural properties, such as fixed points, or symmetry which could be detrimental to attack resistance. To circumvent such issues, the inverted elements undergo an additional affine transformation over $GF\ (2^8)$.

The development of substitution boxes (S-boxes) based on affine transfor-
mations over a Galois Field can be linked to foundational ideas similar to those introduced by Miller's work in elliptic curve cryptography. Just as Miller demon-strated how elliptic curves could enhance cryptographic efficiency and improve protocols like Diffie–Hellman, the use of algebraic structures such as Galois Fields has significantly strengthened modern symmetric cryptographic design.

Subsequent research expanded the use of elliptic and hyperelliptic curves to enhance cryptographic systems. Cheon et al. [13] investigated properties of points on hyperelliptic curves and analyzed their nonlinear behavior for con-structing secure S-boxes. Koblitz [20] provided a comprehensive framework for applying elliptic curves over finite fields, emphasizing their robustness and computational advantages. The comparative work by Amara et al. [8] fur-ther established that ECC delivers stronger security than RSA while requiring shorter key lengths.

Koblitz's later study [21] addressed the discrete logarithm problem, reinforc-ing the superior resistance of ECC to cryptanalytic attacks. Vanstone et al. [33] also discussed the practical adoption of elliptic curve techniques across various cryptographic infrastructures.

More recently, Artuuger et al. [9] proposed an alternative approach to S-box construction using random selection techniques to improve security char-acteristics. Similarly, recent algebraic methods for generating robust S-boxes have been introduced by Razaq et al. [25], Pali et al. [24], and Umrani et al. [32]. These studies utilize different Galois fields to enhance nonlinearity and strengthen cryptographic resilience, demonstrating their effectiveness in secure communication and image encryption systems.

2 BasicDefinitions Finite Field

A Galois Field is a finite collection of elements along with the algebraic oper-
ations of addition, subtraction, multiplication, and division.(excluding division by zero) satisfy the fundamental field axioms. The existence of additive and multiplicative identities and inverses, as well as associativity, commutativity, and distributivity, are among these axioms.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about

Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

More formally, A finite field has precisely (v)*members, where*($v = u^m$), where (u) is a prime number and ($m > 1$) is a positive integer. Such a field is denoted by F_v or GF(v). In this context:

- u represents the *characteristic* of the field.
- m denotes the *degree of extension* of the field over its prime subfield F_u.

The mathematical basis for many applications like data encryption, error correction, and coding theory may be found in finite fields, which are essential to contemporary algebra and the creation of cryptographic primitives and security.

Key Properties

1. For any $v = u^m$, there exists (up to isomorphism) exactly one finite field with v elements.
2. If $m = 1$, the finite field F_u is the set $\{0, 1, 2, \ldots, u - 1\}$ with addition and multiplication performed modulo u. It is the simplest form of a finite field and is called a *prime field*.
3. If $m > 1$, F_um is an extension field of degree m over F_u, and its elements can be represented as polynomials of degree less than m with coefficients in F_u, modulo an irreducible polynomial of degree m.
4. The non-zero elements of F_v form a cyclic group under multiplication. That is, there exists an element $\alpha \in F_v$ such that every non-zero element of F_v is a power of α. Such an element is called a *primitive element*.

Applications: Finite fields are used in:

- Cryptography (e.g., elliptic curve cryptography, AES),
- Error-correcting codes (e.g., Reed–Solomon codes),
- Algebraic geometry and number theory,
- Combinatorics and finite geometry.

2.1 Example

- $F_2 = \{0, 1\}$: The most basic finite field consisting of two elements. Arith-metic is performed modulo 2.

A finite field consisting of eight elements can be created as the field of polynomials over F_2 modulo an irreducible cubic polynomial like $s^3 + s + 1$.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Irreducible Polynomials

A polynomial $f(s) \in F[s]$ defined over a field F is referred to as an **irreducible polynomial** over F if it meets these two criteria:

- $f(s)$ is a polynomial that is not constant, meaning $\deg(f) \geq 1$.
- $f(s)$ cannot be expressed as the product of two non-constant polynomials whose coefficients are in F.

To put it differently, $f(s) \in F[s]$ is irreducible if every time

$f(s) = g(s) * h(s)$

for some $g(s)$, $h(s) \in F[s]$, either $\deg(g) = 0$ or $\deg(h) = 0$; meaning, at least one of the factors is a constant polynomial (a unit in F).

In a field, irreducible polynomials serve a function comparable to that of prime numbers in the set of integers. Every integer can be uniquely factored into a product of prime numbers (up to ordering and units), just as every poly-nomial over a field can. be expressible as a product of irreducible polynomials. The basis for building polynomial rings and finite field extensions are these irreducible polynomials.

2.2 Finite Fields

Irreducible polynomials are crucial in the creation of finite fields (Galois fields). The finite field F_v of order $v = u^m$ can be formed as a quotient ring.

$F_u[s]/(g(s))$

where $f(s)$ is a polynomial of degree m that cannot be factored over F_u. In this framework, the elements of F_v are denoted by equivalence classes of polynomials with degrees lower than m.

2.3 Example

- Over F_2, the polynomial $f(s) = s^2 + s + 1$ is irreducible since it has no roots in F_2 and cannot be factored over F_2.
- $f(s) = s^2 + 1$ is reducible over R (the field of real numbers) since $f(s) = (s + i)(s - i)$, but it is irreducible over R.

3 S-box Design

This part describes the design and building approach of our suggested substitu-tion box (S-box). To grasp the foundational algorithm, it is crucial to examine several basic concepts

A function $f: F^n \rightarrow F_2$ is known as a Boolean function. Extending this, a *vectorial Boolean function* is defined as

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$F(s) = (f_1(s), f_2(s), \ldots, f_m(s))$,
where $s = (s_1, s_2, \ldots, s_n) \in F^n$, Additionally, each (f_i) for $1 \leq i \leq m$ is a Boolean function, also known as a coordinate Boolean function.[2] As a result, an S-box with dimensions of (n times n) is formally defined as a vectorial Boolean function.
$S : F^n \rightarrow F^n$.
2 2

Proposed S-box Construction Method

The construction of substitution boxes (S-boxes) generally requires a nonlin-ear, one-to-one mapping to ensure strong cryptographic performance. In the literature, several methods have been put out for creating such mappings with improved security features. In this study, we introduce a novel approach that exploits the rational points of supersingular elliptic curves defined over the finite field F_v.

The components of a Galois Field constitute a well-defined algebraic frame-work that is frequently employed in the creation of substitution boxes (S-boxes). In this approach, operations such as multiplicative inversion and affine trans-formation are applied, which differ from ordinary arithmetic operations. This structured framework provides a strong mathematical foundation for designing secure S-boxes.

By utilizing the properties of finite fields, particularly $GF(2^8)$, the con-structed S-boxes achieve important cryptographic characteristics such as high nonlinearity, strong confusion, and resistance against common cryptanalytic attacks like linear and differential attacks. The affine transformation further enhances diffusion and eliminates weaknesses such as fixed points.

Additionally, affine mappings over a Galois Field are used in a simple and effective manner to create cryptographically secure S-boxes. The construction process typically involves multiple steps, including inversion in the finite field followed by an affine transformation, ensuring both security and computational efficiency suitable for modern encryption systems. The proposed algorithm com-prises four main phases:

- The suggested S-box generation algorithm comprises four primary steps which are outlined below.
- Step 1.

We take an element in eight bits and its associated polynomial $p(z) \in \frac{F2[z]}{z8+z7+z2+z+1}$

- Step 2.

We find an inverse element o $p(z) \in \frac{F2[z]}{z8+z7+z2+z+1}$

This is say q(z) and take it associated eight bit number

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about

Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

- Step 3.

We apply affine transformation on inverse element that will give the new entry in eight bits.

- Step 4.

Finally, we convert these bits in hexadecimal forms and make a lookup table.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Proposed S-Box

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

The look up table of S-box

4 Properties of S-Boxes

4.1 Non-linearity

The non-linearity of a mapping $S : GF(2^n) \rightarrow GF(2^m$ such that
$S(u) = v$, $u \in GF(2^n)$ and $v \in GF(2^m)$,
is given by: [12]

$$NL_S = 2^{(n-1)} - \frac{1}{2}\max |W(u,v)|$$

Where $W(u, v)$ is the Walsh transform given by:

$$W(u,v) = \sum s \in GF(2^{n^{(-1)^{v.f(s)\oplus u.s}}})$$

Rigid Avalanche Criterion (RAC)

The avalanche effect in cryptographic algorithms is measured using the ba-sic measure known as the textbfRigid Avalanche Criterion (RAC). When the likelihood of altering each output bit is 50% as a consequence of switching a single input bit, this property is deemed ideal. The research by Levinskas et al. citelevinskas2021avalanche discovered that the RAC offers a quantitative stan-dard for determining the effectiveness and resilience of cryptographic methods in generating significant output variations in reaction to minor adjustments in input.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Bit Independence Criterion (BIC)
The Bit Independence Criterion (BIC) is one of the most significant charac-teristics used to evaluate the statistical independence of output bits in cryp-tographic systems. This criteria, as outlined by Levinskas et al. in citelevin-skas2021avalanche, requires that the induced changes in any bit in response to a change in the input bit i be such that The two output bits, j and k, should be statistically independent of one another. Meeting the BIC criteria ensures that the cryptographic algorithm's diffusion process effectively reduces corre-lations between output bits, increasing resilience against linear and differential cryptanalysis.

Differential Uniformity
As highlighted in the work by Mohamed et al. [14],A lower Differential Uni-formity (DU) value in an S-box is preferable. A critical metric for assessing the cryptographic robustness of an S-box, especially its resilience to differential cryptanalysis, is differential uniformity. The likelihood is reduced since minor changes in the input cause large and unpredictable variations in the output when the DU value is lower. of taking advantage of distinct traits in order to compromise the encryption system. In conclusion, decreasing the Differential Uniformity improves the entire security and resilience of the S-box.

Linear Approximation
The findings of Mohamed et al. citemohamed2014study show that a S-resistance box's to linear cryptanalysis improves as the values of Linear Approximation (LA) fall. Linear approximation assesses an S-box's susceptibility to linear cryptanalysis by figuring out how well a linear function can mimic the behavior of an S-box. A lower LA value suggests higher resistance, meaning that the connection between input and output bits is extremely nonlinear and challenging for an attacker to use.

Differential Branch Number
The **Differential Branch Number (DBN)** of an S-box $S : GF(2^n) \rightarrow GF(2^m)$ is defined as [27]:

$$BN = \min_{u1,\, u2 \neq u1} [wt(u_1 \oplus u_2) + wt(S(u_1) \oplus S(u_2))]$$

where $u_1, u_2 \in GF(2^n)$ and $wt(\cdot)$ denotes the Hamming weight function.
One of the most important characteristics of a good S-box is its high non-linearity. Several variables are used to determine the cryptographic strength of

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

an S-box, including nonlinearity, differential uniformity (DU), strict avalanche criterion (SAC), and bit independence criterion (BIC). The evaluation frame-work in this study is expanded to incorporate other variables, such as linearity, the Linear Branch Number (LBN) and the Differential Branch Number (DBN). These metrics, when taken together, offer a more comprehensive picture of the S-box's robustness and resistance to differential attacks. In addition, the 2016 election saw the largest increase in votes ever recorded in a single election. When it comes to its cryptographic capabilities, the Advanced Encryption Standard (AES) is still among the strongest symmetric block ciphers available. Notably, the highest possible nonlinearity for an 8x8 S-box is 120. However, it is well known that no S-box may have this degree of nonlinearity. has the ability to maximize all desired cryptographic features at once. Although nonlinearity is necessary for evaluating the quality of an S-box, it must be balanced with other characteristics. Greater nonlinearity may occasionally lead to trade-offs that compromise the satisfaction of other essential cryptographic requirements or perhaps reveal structural flaws.

5 Performance comparison of different S-boxes

S-box	non-linearity	SAC	BIC	DU	LP	DBN	LBN
Proposed S-box	110.25	0.4809	109.654		0.06913	3	
Iqrar et al. (2023) [68]	108	0.4891	107.258		0.07633	3	
AES(1999)	112	0.5058	112	4	0.0625...	...	
Razaq et al.(2023)[25]	110.75	0.5012	110.646		0.0781		
Zhang et al.(2018) [36]	108.75	0.4946	94	10	0.1328...	...	
Alzaidi et al.(2018b) [7]	110.25	0.50	104	10	0.125 ...	...	
Khan et al. (2016) [19]	100	0.4812	96	16	0.1796...	...	
Guesmi et al. (2014) [16]	107.5	0.4971	196	10	0.125 ...	...	
Ahmad et al. (2015) [1]	107	0.5015	98	10	0.1484...	...	
Tian and Lu (2016) [30]	108	0 .5073	100	10	0.1523...	...	
Ahmad et al. (2016) [2]	107.5	0 .5036	90	10	0.1484...	...	
Farah et al. (2017) [15]	106.5	0.4995	98	10	0.1172...	...	
Ahmed et al. (2019) [3]	107.5	0.4943	98	10	0.125 ...	...	
Lambi´c (2017) [22]	106.75	0.5034	100	10	0.1328...	...	
Ullah et al. (2017) [31]	106.75	0.4939	102	16	0.125 ...	...	
Jamal and Shah (2018) [10]	107.25	0.5034	98	12	0.1328...	...	
O¨ zkaynak (2019b) [23]	106.75	0.4941	98	10	0.1250...	...	
Ye and Zhimao (2018) [34]	106.75	0.4076	98	10	0.1328...	...	
Silva-Garc´ıa et al.(2018) [28]	106	0.5066	96	12	0.1445...	...	
Yi et al. (2019) [35]	107.75	0.4976	100	10	0.125 ...	...	
Alzaidi et al. (2018a) [6]	109.5	0.4985	98	10	0.1328...	...	

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about

Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Solami et al. (2018) [4]	108.5	0.5017	100	10	0.1328...	...	
Hussain et al. (2020) [18]	106.87	0.509	106.118		0.113	...	...

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about

Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

6 Conclusion

This research investigates the construction of a cryptographic Substitution Box (S-Box) using affine transformation over a Galois Field, with the aim of enhanc-ing nonlinearity, confusion strength, and overall resistance to classical crypt-analytic attacks. The suggested S-Box, by using affine transformations and operations in GF(2), proves to have the necessary good algebraic structure and remains within the primary guidelines for the design of secure block ciphers. It has been established that the created S-Box has low differential uniformity, considerable non-linearity, a fair distribution of the output and a high level of resilience against differential and linear assaults. The results support the no-tion that the combination of affine transformation and field inversion or other Galois field operations create a mathematically viable S-Box. Moreover, the construction's determination and algebraic attributes guarantee reproducibil-ity, implementation at a low cost, and adaptability to hardware, software, and resource-constrained systems. Most importantly, this study has emphasized the Galois-field-based affine transformation's usefulness and positive contributions to current modern cryptography, as well as its ability to construct secure, effi-cient, and scalable substitution patterns in symmetric-key algorithms.

References

Musheer Ahmad, Deepanshu Bhatia, and Yusuf Hassan. A novel ant colony optimization based scheme for substitution box design. *Procedia Computer Science*, 57:572–580, 2015.

Musheer Ahmad, Nikhil Mittal, Prerit Garg, and Manaff Maftab Khan. Efficient cryptographic substitution box design using travelling salesman problem and chaos. *Perspectives in Science*, 8:465–468, 2016.

Hussam A Ahmed, Mohamad Fadli Zolkipli, and Musheer Ahmad. A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. *Neural Computing and Applications*, 31:7201–7210, 2019.

Eesa Al Solami, Musheer Ahmad, Christos Volos, Mohammad Najam Doja, and Mirza Mohd Sufyan Beg. A new hyperchaotic system-based design for efficient bijective substitution-boxes. *entropy*, 20(7):525, 2018.

Anas Altaleb, Muhammad Sarwar Saeed, Iqtadar Hussain, and Muhammad Aslam. An algorithm for the construction of substitution box for block ci-phers based on projective general linear group. *AIP Advances*, 7(3):035116, 2017.

Amer Awad Alzaidi, Musheer Ahmad, Hussam S Ahmed, and Eesa Al Solami. Sine-cosine optimization-based bijective substitution-boxes con-struction using enhanced dynamics of chaotic map. *Complexity*, 2018:1–16, 2018.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about

Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Amer Awad Alzaidi, Musheer Ahmad, Mohammad Najam Doja, Eesa Al Solami, and MM Sufyan Beg. A new 1d chaotic map and backslash *beta*-hill climbing for generating substitution-boxes. *IEEE Access*, 6:55405–55418, 2018.

Moncef Amara and Amar Siad. Elliptic curve cryptography and its appli-cations. In *International workshop on systems, signal processing and their applications, WOSSPA*, pages 247–250. IEEE, 2011.

Fırat Artu˘ger and Fatih O¨ zkaynak. A method for generation of substitution box based on random selection. *Egyptian Informatics Journal*, 23(1):127–135, 2022.

Attaullah, Sajjad Shaukat Jamal, and Tariq Shah. A novel algebraic tech-nique for the construction of strong substitution box. *Wireless Personal Communications*, 99:213–226, 2018.

Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosys-tems. *Journal of CRYPTOLOGY*, 4(1):3–72, 1991.

Claude Carlet and Cunsheng Ding. Nonlinearities of s-boxes. *Finite fields and their applications*, 13(1):121–135, 2007.

Jung Hee Cheon, Seongtaek Chee, and Choonsik Park. S-boxes with con-trollable nonlinearity. In *International Conference on the Theory and Ap-plications of Cryptographic Techniques*, pages 286–294. Springer, 1999.

Lingguo Cui and Yuanda Cao. A new s-box structure named affine-power-affine. *International Journal of Innovative Computing, Information and Control*, 3(3):751–759, 2007.

Tarek Farah, Rhouma Rhouma, and Safya Belghith. A novel method for designing s-box based on chaotic map and teaching–learning-based opti-mization. *Nonlinear dynamics*, 88(2):1059–1074, 2017.

Ramzi Guesmi, Mohamed Amine Ben Farah, Abdennaceur Kachouri, and Mounir Samet. A novel design of chaos based s-boxes using genetic al-gorithm techniques. In *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, pages 678–684. IEEE, 2014.

Umar Hayat and Naveed Ahmed Azam. A novel image encryption scheme based on an elliptic curve. *Signal Processing*, 155:391–402, 2019.

Sadam Hussain, Sajjad Shaukat Jamal, Tariq Shah, and Iqtadar Hussain. A power associative loop structure for the construction of non-linear com-ponents of block cipher. *IEEE Access*, 8:123492–123506, 2020.

Majid Khan, Tariq Shah, and Syeda Iram Batool. Construction of s-box based on chaotic boolean functions and its application in image encryption. *Neural Computing and Applications*, 27:677–685, 2016.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about

Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

Neal Koblitz, Alfred Menezes, and Scott Vanstone. The state of elliptic curve cryptography. *Designs, codes and cryptography*, 19(2):173–193, 2000.

Dragan Lambi´c. A novel method of s-box design based on discrete chaotic map. *Nonlinear dynamics*, 87:2407–2413, 2017.

Fatih O¨ zkaynak. Construction of robust substitution boxes based on chaotic systems. *Neural Computing and Applications*, 31(8):3317–3326, 2019.

Iqrar Ali Pali, Muhammad Afzal Soomro, Muhammad Memon, Asgher Ali Maitlo, Sanaullah Dehraj, and Naveed Ahmed Umrani. Construction of an s-box using suppersingular elliptic curve over finite field. *Journal of Hunan University Natural Sciences*, 50(7), 2023.

Abdul Razaq, Musheer Ahmad, and Ahmed A Abd El-Latif. A novel algebraic construction of strong s-boxes over double gf (27) structures and image protection. *Computational and Applied Mathematics*, 42(2):90, 2023.

Vincent Rijmen. Cryptanalysis of advanced encryption standard. *Summer School on Design and Security of Cryptographic Functions, Algorithms and Devices*, 2013.

Sumanta Sarkar and Habeeb Syed. Bounds on differential and linear branch number of permutations. In *Australasian conference on information secu-rity and privacy*, pages 207–224. Springer, 2018.

VM Silva-Garc´ıa, Rolando Flores-Carapia, Carlos Renter´ıa-M´arquez, B Luna-Benoso, and Mario Aldape-P´erez. Substitution box generation using chaos: An image encryption application. *Applied Mathematics and Computation*, 332:123–135, 2018.

Data Encryption Standard. National bureau of standards (us)/federal in-formation processing standards publication 46//national technical informa-tion service. *Springfield, VA*, 1977.

Ye Tian and Zhimao Lu. S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm. *Journal of Systems Engineering and Electronics*, 27(1):232–241, 2016.

Atta Ullah, Sajjad Shaukat Jamal, and Tariq Shah. A novel construction of substitution box using a combination of chaotic maps with improved chaotic range. *Nonlinear Dynamics*, 88:2757–2769, 2017.

Naveed Ahmed Umrani, Iqrar Ali Pali, Safia Amir Dahri, Muhammad Afzal Soomro, and Kamran Nazir Memon. Construction of substitution boxes using finite fields. *VFAST Transactions on Mathematics*, 11(2):01–15, 2023.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Scott A Vanstone. Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments. *Informa-tion security technical report*, 2(2):78–87, 1997.

Tian Ye and Lu Zhimao. Chaotic s-box: Six-dimensional fractional lorenz–duffing chaotic system and o-shaped path scrambling. *Nonlinear Dynamics*, 94:2115–2126, 2018.

Longteng Yi, Xiaojun Tong, Zhu Wang, Miao Zhang, Honghong Zhu, and Jing Liu. A novel block encryption algorithm based on chaotic s-box for wireless sensor network. *IEEE Access*, 7:53079–53090, 2019.

Tong Zhang, CL Philip Chen, Long Chen, Xiangmin Xu, and Bin Hu. Design of highly nonlinear substitution boxes based on i-ching operators. *IEEE transactions on cybernetics*, 48(12):3349–3358, 2018.