Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

An Strong Substitution Box Generated by Point of Order Two on Elliptic Curve Over $\mathbb{F}_{2^8}$

Samad Ali Dahri

Department of Mathematics and Statistics, Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah. dahrisamad8@gmail.com

Iqrar Ali Pali

Department of Mathematics and Statistics, Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah. iqraralipali@quest.edu.pk

Muhammad Afzal Soomro

Department of Mathematics and Statistics, Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah. m.a.soomro@quest.edu.pk

Muzaffar B. Arain*

Department of Mathematics and Statistics, Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah. Corresponding Auhtor Email: muzaffararain@quest.edu.pk

Manzar Bashir Arain

Department of Information Technology, SBBU Sanghar Campus, Sindh, Pakistan. manzar.arain_sng@sbbusba.edu.pk

ABSTRACT

Algebraic curves play a vital role in modern mathematical and cryptographic systems due to their extensive range of applications, particularly in cryptography. The efficiency and security of contemporary cryptographic algorithms largely stem from their formulation over finite fields. This study presents a novel method for constructing a secure substitution box (S-box) based on the rational points of order two on a supersingular elliptic curve defined over the finite field $\mathbb{F}_{2^8}$. Evaluation in accordance with established cryptographic benchmarks demonstrates that the proposed S-box satisfies the essential criteria of robustness and reliability required for secure cryptographic design.

Keywords: Elliptic Curve, Points of order two, Galois Field, Substitution Box and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Non-linearity.

Introduction

With the rapid advancement of communication technologies (Akram et al., 2021, 2022; Ramzan et al., 2023, 2025), maintaining data confidentiality has become an increasingly complex challenge. As a result, researchers have devoted significant attention to developing mechanisms that safeguard transmitted information while ensuring both its integrity and authenticity. Among the various cryptographic approaches, *block ciphers* form the backbone of modern cryptosystems, and within these systems, the *substitution box* (S-box) plays a decisive role in providing nonlinearity and resistance against attacks.

The S-box transforms input bit patterns into corresponding output patterns, introducing confusion and complexity into the encryption process. This nonlinear transformation is essential for making cryptographic algorithms secure against differential and linear cryptanalysis. It is widely recognized that the overall security of a block cipher is strongly influenced by the design quality of its S-box. Prominent cryptographic standards such as the Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), and the Advanced Encryption Standard (AES) heavily depend on well-constructed S-boxes. Consequently, the cryptographic strength of a cipher is closely tied to the robustness of its underlying substitution mechanism.

The introduction of DES in 1977 [32] marked a major milestone in the evolution of cryptography. However, its eventual compromise by university researchers revealed the need for more advanced encryption schemes. This motivated 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 confidentiality in digital communication systems [28].

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. Several analytical metrics are commonly applied

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

to assess S-box quality, including the *bit independence criterion* (BIC), the *strict avalanche criterion* (SAC), *nonlinearity* (NL), the *differential approximation probability* (DAP), and the *linear approximation probability* (LAP). 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. [18] proposed an approach based on elliptic curves, where ordinate values of the curve were used in the construction process. Similarly, Altaleb et al.[5] employed 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.

Elliptic curves have gained prominence in cryptography because they offer equivalent levels of security with substantially smaller key sizes. As shown by Galbraith et al.[16] , a 313-bit elliptic curve cryptographic key provides the same security strength as a 4096-bit RSA key. This reduction leads to advantages such as smaller chip area, lower power consumption, and faster computation making elliptic curve cryptography (ECC) highly suitable for resource-constrained environments. The foundation of ECC can be traced to the pioneering work of Miller[24] , who demonstrated how elliptic curves could be utilized to enhance cryptographic performance. His proposed elliptic curve–based system improved the Diffie–Hellman protocol by approximately 20%, highlighting the efficiency and potential of ECC for secure key exchange. Since then, elliptic curve cryptography has evolved into a dynamic field of study, forming the basis for numerous modern cryptographic applications.

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 constructing secure S-boxes. Koblitz [21] 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] further established that ECC

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

delivers stronger security than RSA while requiring shorter key lengths.

Koblitz's later study [22] addressed the discrete logarithm problem, reinforcing the superior resistance of ECC to cryptanalytic attacks. Vanstone et al. [36] 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 characteristics. Similarly, recent algebraic methods for generating robust S-boxes have been introduced by Razaq et al.[27] , Pali et al.[26] , and Umrani et al. [35]. These studies utilize different Galois fields to enhance nonlinearity and strengthen cryptographic resilience, demonstrating their effectiveness in secure communication and image encryption systems.

Basic Definitions

Finite Field

An algebraic structure known as a Galois Field is a finite set of elements over which the operations 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.

More formally, a finite field is a field containing exactly v elements, where $v = u^m$, with u being a prime number and $m \geq 1$ a positive integer. Such a field is denoted by $\mathbb{F}_v$ 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 $\mathbb{F}_u$.

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 $\mathbb{F}_u$ is the set $\{0,1,2,\ldots,u-1\}$ with addition and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

multiplication performed modulo u. It is the simplest form of a finite field and is called a *prime field*.

3. If $m > 1$, $\mathbb{F}_{u^m}$ is an extension field of degree m over $\mathbb{F}_u$, and its elements can be represented as polynomials of degree less than m with coefficients in $\mathbb{F}_u$, modulo an irreducible polynomial of degree m.
4. The non-zero elements of $\mathbb{F}_v$ form a cyclic group under multiplication. That is, there exists an element $\alpha \in \mathbb{F}_v$ such that every non-zero element of $\mathbb{F}_v$ 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.

Example

- $\mathbb{F}_2 = \{0,1\}$: The most basic finite field consisting of two elements. Arithmetic is performed modulo 2.
- A finite field consisting of eight elements can be created as the field of polynomials over $\mathbb{F}_2$ modulo an irreducible cubic polynomial like $s^3 + s + 1$.

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

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

of prime numbers (up to ordering and units), just as every polynomial 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.

Finite Fields

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

$$\mathbb{F}_u[s]/(g(s))$$

where $f(s)$ is a polynomial of degree m that cannot be factored over $\mathbb{F}_u$. In this framework, the elements of $\mathbb{F}_v$ are denoted by equivalence classes of polynomials with degrees lower than m.

Example

- Over $\mathbb{F}_2$, the polynomial $f(s) = s^2 + s + 1$ is irreducible since it has no roots in $\mathbb{F}_2$ and cannot be factored over $\mathbb{F}_2$.
- $f(s) = s^2 + 1$ is reducible over $\mathbb{R}$ (the field of real numbers) since $f(s) = (s + i)(s - i)$, but it is irreducible over $\mathbb{R}$.

Rational Points over a Finite Field

Consider $\mathbb{F}_v$ as a finite field containing v elements, where $v = u^m$ for a prime u and a positive integer m. Take into account an algebraic curve C described by a polynomial equation (in two variables) with coefficients from $\mathbb{F}_v$:

$f(s,t) = 0, \quad f(s,t) \in \mathbb{F}_v[t,s]$.

A point $P = (s,t)$ is referred to as a **rational point of the curve over** $\mathbb{F}_v$ if both s and t belong to the finite field $\mathbb{F}_v$, and the point fulfills the curve's defining equation: $f(s,t) = 0$.

Formal Definition

A **rational point** on a curve C over the finite field $\mathbb{F}_v$ is a point $(s,t) \in \mathbb{F}_v \times \mathbb{F}_v$ such that $f(s,t) = 0$. The set of all such points is denoted $C(\mathbb{F}_v)$ and is defined as:

$$C(\mathbb{F}_v) = \{(s,t) \in \mathbb{F}_v \times \mathbb{F}_v | f(s,t) = 0\}.$$

If the curve is a projective curve, then rational points may also include points at infinity defined in projective space $\mathbb{P}^2(\mathbb{F}_v)$.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Example

Consider the elliptic curve defined over $\mathbb{F}_5$ by the equation:

$$E: t^2 = s^3 + 2s + 1.$$

The rational points on E over $\mathbb{F}_5$ are found by finding all pairs $(s, t) \in \mathbb{F}_5 \times \mathbb{F}_5$ such that the equation holds. That is, we compute all values of $s \in \{0,1,2,3,4\}$, compute $s^3 + 2s + 1$, and check if it is a quadratic residue (i.e. a square) in $\mathbb{F}_5$.

Motivation

Rational points over finite fields are of central importance in many areas of number theory and cryptography, including:

- Elliptic curve cryptography (ECC),
- Algebraic geometry over finite fields,
- Coding theory (e.g. using algebraic-geometry codes),
- Counting points to compute zeta functions and arithmetic properties of curves.

Elliptic Curve over Finite Field

An elliptic curve defined over a finite field $\mathbb{F}_v$, with $v = u^m$ (where u is a prime and m is a positive integer), is a smooth algebraic curve of genus one that includes a specific point referred to as the point at infinity.

Weierstrass Form

Over a finite field $\mathbb{F}_v$ where $u \neq 2,3$, an elliptic curve E is usually given by the short

Weierstrass Equation

$$t^2 = s^3 + As + B$$

where $A, B \in \mathbb{F}_v$ and the curve is nonsingular meaning that its discriminant is non-zero:

$$\Delta = -16(4A^3 + 27B^2) \neq 0.$$

The set of solutions $(s, t) \in \mathbb{F}_v \times \mathbb{F}_v$ satisfying the equation together with the point at infinity $\mathcal{O}$ forms the set of points on the curve:

$$E(\mathbb{F}_v) = \{(s, t) \in \mathbb{F}_v \times \mathbb{F}_v | t^2 = s^3 + As + B\} \cup \{\mathcal{O}\}.$$

Group Structure

A significant characteristic of elliptic curves is that the collection of points $E(\mathbb{F}_v)$,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

which encompasses the point at infinity $\mathcal{O}$, constitutes an abelian group with a clearly defined addition operation:

- The point at infinity $\mathcal{O}$ acts as the identity element.
- Each point has an inverse (i.e., reflection across the s-axis).
- The group operation is geometrically defined using line intersections and algebraically via explicit formulas.

Elliptic Curves in Characteristics 2 or 3

In fields of characteristic 2 or 3, the general Weierstrass form must be used:

$$t^2 + a_1st + a_3t = s^3 + a_2s^2 + a_4s + a_6$$

with $a_i \in \mathbb{F}_v$ and some conditions ensuring that the curve is nonsingular.

Applications

Elliptic curves over finite fields are widely used in modern mathematics and cryptography. They have been used in:

- **Elliptic Curve Cryptography (ECC):** Key exchange, digital signatures, and encryption.
- Studying rational points, modular forms, and zeta functions.
- **Coding Theory:** Construction of error-correcting codes.
- **Random Number Generation:** Due to the complex group structure.

Example

Consider the finite field $\mathbb{F}_5 = \{0,1,2,3,4\}$. Let E be the elliptic curve

$$t^2 = s^3 + 2s + 1.$$

One can compute $E(\mathbb{F}_5)$ by evaluating the right-hand side for each $s \in \mathbb{F}_5$ and checking if it is a square in $\mathbb{F}_5$ (i.e., if a corresponding t exists).

Hasse's Theorem

The number of $\mathbb{F}_v$-rational points on an elliptic curve satisfies:

$$|\#E(\mathbb{F}_v) - (v+1)| \leq 2\sqrt{v}.$$

This result provides a tight bound on the number of rational points and is used in estimating the security of elliptic curve cryptosystems.

Supersingular Elliptic Curves

The term "supersingular elliptic curve" refers to a particular type of elliptic curve

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

that is characterized by its distinct algebraic and arithmetic characteristics and is defined over a finite field. In the theoretical investigation of elliptic curves and the creation of contemporary cryptographic systems, notably in the field of post-quantum cryptography, supersingular curves are extremely important.

Elliptic Curves over Finite Fields

Let $\mathbb{F}_v$ be a finite field of characteristic u and cardinality $v = u^m$, where u is a prime and $m \geq 1$. An elliptic curve E over $\mathbb{F}_v$ is a Weierstrass equation of the form:

$$t^2 = s^3 + As + B, \quad A, B \in \mathbb{F}_v, \Delta = -16(4A^3 + 27B^2) \neq 0.$$

Definition of Supersingular Curve

An elliptic curve E over a finite field $\mathbb{F}_v$ of characteristic u is said to be **supersingular** if it has no non-zero u-torsion points over the algebraic closure $\overline{\mathbb{F}}_v$. In other words:

$$E[u](\overline{\mathbb{F}}_v) = \{\mathcal{O}\},$$

where $E[u]$ is the group of points on E whose order divides u, and $\mathcal{O}$ is the point at infinity.

That is, E is supersingular if the u-torsion subgroup $E[u]$ is trivial.

Equivalent Characterizations

There are a number of equivalent characterizations of supersingular elliptic curves:

- The trace of Frobenius t satisfies $t \equiv 0 \mod u$.
- The number of rational points satisfies:

$$\#E(\mathbb{F}_v) = v + 1.$$

- The endomorphism ring of E over $\overline{\mathbb{F}}_v$ is not just an order in an imaginary quadratic field (as in the ordinary case), but a maximal order in a quaternion algebra.

Example

Let $\mathbb{F}_u$ be a finite field with $u \equiv 3 \mod 4$. The curve

$$E: t^2 = s^3 + s$$

is supersingular over $\mathbb{F}_u$. For example, $E: t^2 = s^3 + s$ is supersingular over $\mathbb{F}_5$.

Note

Contrary to common belief, supersingular elliptic curves are not geometrically

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

"singular" in that they lack singularities like nodes or cusps. As with all elliptic curves, they are smooth and non-singular. The exceptional algebraic structure of supersingular curves, however, sets them apart, notably the nature of their group rule and the characteristics of their endomorphism ring, which are very different from those of regular elliptic curves.

S-box Design

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

A function $f: \mathbb{F}_2^n \to \mathbb{F}_2$ is known as a Boolean function. Extending this, a *vectorial Boolean function* is defined as

$F(s) = \big(f_1(s), f_2(s), \ldots, f_m(s)\big),$

where $s = (s_1, s_2, \ldots, s_n) \in \mathbb{F}_2^n$, and each f_i for $1 \le i \le m$ is a Boolean function, commonly referred to as a coordinate Boolean function. An $n \times n$ S-box is thus formally defined as a vectorial Boolean function

$$S: \mathbb{F}_2^n \to \mathbb{F}_2^n.$$

Our approach to S-box construction is rooted in the algebraic properties of supersingular elliptic curves defined over finite fields. Consider an elliptic curve E given by:

$$E: t^2 = f(s),$$

where $f(s) \in \mathbb{F}_v[s]$ is a cubic polynomial with distinct roots in $\overline{\mathbb{F}_v}$. According to , the curve E is classified as supersingular if the coefficient of s^{u-1} in $f(s)^{(u-1)/2}$ is zero. One important property of supersingular elliptic curves is that, if $\mathbb{F}_v$ is a finite field of characteristic u, then the number of $\mathbb{F}_v$-rational points on E is given by:

$$\#E(\mathbb{F}_v) = v + 1.$$

Proposed S-box Construction Method

The construction of substitution boxes (S-boxes) generally requires a nonlinear, one-to-one mapping to ensure strong cryptographic performance. Various techniques have been proposed in the literature to design such mappings with enhanced security properties. In this study, we introduce a novel approach that exploits the rational points of supersingular elliptic curves defined over the finite field $\mathbb{F}_v$.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

The set of rational points on an elliptic curve forms a mathematical group under a well-defined operation known as the *group law*. It is important to emphasize that this group operation referred to as point addition differs fundamentally from ordinary field addition, which can sometimes lead to confusion. Nevertheless, this distinctive algebraic framework serves as the foundation of the proposed approach.

By leveraging the algebraic properties of the group formed by the rational points on a supersingular elliptic curve, we construct S-boxes that exhibit high degrees of nonlinearity, confusion, and resistance against well-known cryptanalytic attacks. A simple yet effective algorithm for generating cryptographically secure S-boxes is proposed. The construction is based on the second-order points of supersingular elliptic curves defined over a finite field $\mathbb{F}_v$. The proposed algorithm comprises four main phases:

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

  Consider an appropriate elliptic curve of the form $t^2 + st + s^3 + a_2s^2 + a_6$=0 defined over F_{2^8}.
- Step 2.

  Next, we incorporate the point of order two $(0, \sqrt{a_6})$ with all possible rational points on these curves.
- Step 3.

  Subsequently, we define an S-box as a 16×16 matrix with entries that are the y coordinates of the points obtained after adding the point of order two to the other rational points.
- Step 4.

  The generated S-box undergoes analysis. The outcomes are compared with well-known S-boxes.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Proposed S-Box

Table 1: ***The look up table of S-box***

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

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

2	44	210	154	25	246	212	88	6	90	22	80	203	194	132	174
83	125	63	54	177	235	167	251	169	45	11	232	103	47	213	255

Properties of S-Boxes

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:

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

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 basic 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 standard for determining the effectiveness and resilience of cryptographic methods in generating significant output variations in reaction to minor adjustments in input.

Bit Independence Criterion (BIC)

One of the most important features used to assess the statistical independence of output bits in cryptographic systems is the Bit Independence Criterion (BIC). This criteria, as outlined by Levinskas et al. in citelevinskas2021avalanche, 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 correlations between output bits, increasing resilience against linear and differential cryptanalysis.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Differential Uniformity

As highlighted in the work by Mohamed et al. [14], a smaller value of the Differential Uniformity (DU) 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. By determining how well a linear function can approximate the behavior of an S-box, linear approximation determines the vulnerability of an S-box to linear cryptanalysis. 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 :

$$BN = \min_{u_1, u_2 \neq u_1} \left[wt(u_1 \oplus u_2) + wt\big(S(u_1) \oplus S(u_2)\big) \right]$$

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 nonlinearity. The cryptographic robustness of an S-box is assessed using a number of criteria, including the Bit Independence Criterion (BIC), Strict Avalanche Criterion (SAC), Differential Uniformity (DU), and nonlinearity. The evaluation framework in this study is expanded to incorporate other variables, such as linearity, the Differential Branch Number (DBN), and the Linear Branch Number (LBN). 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

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

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.

Performance comparison of different S-boxes

Table 2: ***Comparison of different S-boxes***

S-box	non-linearity	SAC	BIC	DU	LP	DBN	LBN
Proposed S-box	109	0.4892	108.15	8	0.0771	3	3
Iqrar et al. (2023)[26]	108	0.4891	107.25	8	0.0763	3	3
AES 1999 [40]	112	0.5058	112	4	0.0625	...	...
Razaq et al.(2023)[27]	110.75	0.5012	110.64	6	0.0781		
Zhang et al.(2018) [23]	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) [20]	100	0.4812	96	16	0.1796	...	...
Guesmi et al. (2014) [17]	107.5	0.4971	196	10	0.125	...	...
Ahmad et al. (2015) [1]	107	0.5015	98	10	0.1484	...	...
Tian and Lu (2016) [33]	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) [23]	106.75	0.5034	100	10	0.1328	...	...
Ullah et al. (2017) [34]	106.75	0.4939	102	16	0.125	...	...
Jamal and Shah (2018)[10]	107.25	0.5034	98	12	0.1328	...	...
Özkaynak (2019) [25]	106.75	0.4941	98	10	0.1250	...	...

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

S-box	non-linearity	SAC	BIC	DU	LP	DBN	LBN
Ye and Zhimao (2018)[37]	106.75	0.4076	98	10	0.1328	...	...
Silva-García et al.(2018)[30]	106	0.5066	96	12	0.1445	...	...
Yi et al. (2019) [38]	107.75	0.4976	100	10	0.125	...	...
Alzaidi et al. (2018)[6]	109.5	0.4985	98	10	0.1328	...	...
Solami et al. (2018) [4]	108.5	0.5017	100	10	0.1328	...	...
Hussain et al. (2020) [19]	106.87	0.509	106.11	8	0.113	...	...

Conclusion

The formula $(t^2 = s^3 + As + B)$ describes the supersingular elliptic curves upon which the suggested method for producing numerous S-boxes is based. Every supersingular elliptic curve produces a unique S-box that is associated with particular values of A and B that meet the criteria for supersingularity. As a result, the algorithm is able to generate a number of different S-boxes by altering the values of the parameters A and B, giving the S-box design flexibility and diversity. In contrast, The cryptographic system is made more secure and flexible overall because of this flexibility, which allows for the production of a wide variety of S-boxes. The suggested technique is used to create a particular S-box in this study, and its features are examined by comparing its performance to that of other S-boxes. The generated S-box satisfies the fundamental requirements for a strong and secure replacement box, as shown by the analysis. Additionally, the proposed S-box is shown to be appropriate for secure and reliable cryptographic uses by its evaluation of its cryptographic properties, such as nonlinearity, differential uniformity, and associated parameters.

References

[1] 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.

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] Fırat Artu˘ger and Fatih ¨ Ozkaynak. A method for generation of substitution box based on random selection. Egyptian Informatics Journal, 23(1):127 135, 2022.

[10] 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.

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

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

[13] Jung Hee Cheon, Seongtaek Chee, and Choonsik Park. S-boxes with con

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

trollable nonlinearity. In International Conference on the Theory and Ap plications of Cryptographic Techniques, pages 286–294. Springer, 1999.

[14] 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.

[15] 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.

[16] Steven Galbraith. Elliptic curves in cryptography (london mathematical society lecture note series 265) by ian blake, gadiel seroussi, and nigel smart: 204 pp., $24.95 ($39.95, lms members price $18.70), isbn 0 521 65374 6 (cambridge university press, 1999). Bulletin of the London Mathematical Society, 32(5):619–640, 2000.

[17] 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.

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

[19] 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.

[20] 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.

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

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

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

[24] Victor S Miller. Use of elliptic curves in cryptography. In Conference on the

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

theory and application of cryptographic techniques, pages 417–426. Springer, 1985.

[25] Fatih ¨ Ozkaynak. Construction of robust substitution boxes based on chaotic systems. Neural Computing and Applications, 31(8):3317–3326, 2019.

[26] 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.

[27] 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.

[28] Vincent Rijmen. Cryptanalysis of advanced encryption standard. Summer School on Design and Security of Cryptographic Functions, Algorithms and Devices, 2013. [29] 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.

[30] 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.

[31] Joseph H. Silverman. The arithmetic of elliptic curves. Graduate Text in Mathematics 106. Springer- Verlag, New York, second edition, 2009.

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

[33] 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.

[34] 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.

[35] Naveed Ahmed Umrani, Iqrar Ali Pali, Safia Amir Dahri, Muhammad Afzal

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Soomro, and Kamran Nazir Memon. Construction of substitution boxes using finite fields. VFAST Transactions on Mathematics, 11(2):01–15, 2023.

[36] 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.

[37] 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.

[38] 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.

[39] Akram, H., Yingxiu, Y., Al-Adwan, A. S., & Alkhalifah, A. (2021). Technology Integration in Higher Education During COVID-19: An Assessment of Online Teaching Competencies Through Technological Pedagogical Content Knowledge Model. *Frontiers in Psychology*, 12, 736522-736522.

[40] Akram, H., Abdelrady, A. H., Al-Adwan, A. S., & Ramzan, M. (2022). Teachers' perceptions of technology integration in teaching-learning practices: A systematic review. *Frontiers in psychology*, *13*, 920317.

[41] Ramzan, M., Akram, H., & kynat Javaid, Z. (2025). Challenges and Psychological Influences in Teaching English as a Medium of Instruction in Pakistani Institutions. *Social Science Review Archives*, *3*(1), 370-379.

[42] Ramzan, M., Bibi, R., & Khunsa, N. (2023). Unraveling the Link between Social Media Usage and Academic Achievement among ESL Learners: A Quantitative Analysis. *Global. Educational Studies Review*, *8*, 407-421.

[43] 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.

[44] Sean Murphy. The advanced encryption standard (aes). Information Security Technical Report, 4(4):12–17, 1999.