湖南大学学报（自然科学版）
Journal of Hunan University (Natural Sciences)

第 50 卷 第 7 期
2023 年 7 月

Available online at http://jonuns.com/index.php/journal/index

Vol. 50 No. 7
July 2023

Open Access Article

https://doi.org/10.55463/issn.1674-2974.50.7.5

Construction of an S-Box Using Suppersingular Elliptic Curve over Finite Field

Iqrar Ali Pali[1]*, Muhammad Afzal Soomro[1], Muhammad Memon[2], Asgher Ali Maitlo[1], Sanaullah Dehraj[1], Naveed Ahmed Umrani[1]

[1] Department of Mathematics and Statistics, Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah, 67480, Pakistan

[2] Department of Basic Science and Related Studies, Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah, 67480, Pakistan

* Corresponding author: iqraralipali@quest.edu.pk

Received: April 7, 2023 / Revised: May 3, 2023 / Accepted: June 1, 2023 / Published: July 31, 2023

Abstract: This research aims to develop an S-box using elliptic curve cryptography (ECC) that provides higher security than other cryptographic schemes with equivalent key size. In this paper, a supersingular elliptic curve $2^2\ 2\ 2^2\ 2\ 22\ 2\ 2$ has been taken of characteristic more than three. The generated S-box depends on the values of a and b used in the supersingular elliptic curve. The robustness of the recently constructed S-box is thoroughly evaluated against prevalent attacks, including linear, differential, and algebraic attacks, through an analysis of its nonlinearity, linear approximation, differential branch number, and other established properties. The achieved findings are additionally contrasted with some well-known S-boxes.

Keywords: finite fields, supersingular elliptic curves, group law, rational points, substitution boxes.

有限域上使用超奇异椭圆曲线构造 S 盒

摘要: 本研究旨在开发一种使用椭圆曲线加密(ECC)的 S 盒，它比具有同等密钥大小的其他加密方案提供更高的安全性。本文取了一条超奇异椭圆曲线曲线 $t^2 = s^3 + \boldsymbol{a}s + \boldsymbol{b}$的 3 以上特征。生成的 S 盒取决于超奇异椭圆曲线中使用的 a 和 b 的值。通过分析其非线性、线性逼近、差分分支数和其他既定属性，对最近构建的 S 盒的鲁棒性进行了彻底评估，以应对流行的攻击，包括线性、差分和代数攻击。所取得的发现还与一些著名的 S 盒进行了对比。

关键词：有限域、超奇异椭圆曲线、群律、有理点、替换框。

1. Introduction

Advancements in communication technology have accelerated significantly in recent times. Consequently, safeguarding data security poses a formidable challenge for cryptographers. Numerous research papers have been published in order to enhance the protection of transmitted information, thereby ensuring its safety and integrity [2-3]. In the realm of modern cryptographic systems, the block encryption algorithm plays a crucial role. A fundamental and significant component within this algorithm is the substitution box (S-box). The S-box assumes a significant role in

ensuring the confidentiality and integrity of sensitive information. It is designed to transform input bit patterns into output bit patterns through nonlinear mapping, enhancing the cryptographic strength of the system. Researchers and experts in the field recognize the paramount importance of the S-box in achieving robust data security. The S-box serves as a critical component in various cryptosystems, such as the Data Encryption Standards (DES), International Data Encryption Algorithm (IDEA), and Advanced Encryption Standards (AES). The security potency of the S-box directly influences the overall security of the cryptosystem. Thus, the S-box holds significant importance as a nonlinear element for ensuring the security and resilience of cryptosystems.

DES was introduced in 1977 [4]. Subsequently, a significant event occurred when a team of university students successfully compromised the security of the Data Encryption Standard (DES). This incident served as a wake-up call, highlighting the need for alternative encryption methods that could offer both enhanced security and efficiency. As a response to this demand, the Advanced Encryption Standard (AES) was developed and introduced in 2002. Since its inception, AES has gained widespread recognition and acceptance as the industry standard for encryption. The AES algorithm is renowned for its robust security features, making it a trusted choice for safeguarding sensitive information across various sectors and applications. Its efficiency and resistance to cryptanalysis have solidified its position as a cornerstone of modern cryptographic systems. The creation and adoption of the AES algorithm underscore the continuous efforts to evolve encryption techniques, ensuring the privacy and integrity of data in an ever-evolving digital landscape [5].

The S-box plays a crucial role in encryption quality. Using a weak S-box compromises the security of the encryption process. Therefore, it is essential to evaluate the strength of an S-box before employing it in a cryptosystem. To assess the strength of the S-box, several analyses are employed, including several analytical techniques to measure the strength of cryptographic schemes, including the assessment of nonlinearity using the NL method, evaluation of linear approximation probabilities through the LAP method, verification of bit independence using the BIC, evaluation of the strict avalanche effect based on the SAC, and examination of differential approximation probabilities using the DAP method. These diverse methodologies provide a comprehensive understanding of the cryptographic properties and robustness of the schemes under scrutiny. By using multiple evaluation criteria, researchers gain insights into various aspects of cryptographic schemes, enabling a more thorough assessment of their security and effectiveness. In the literature, notable studies regarding the construction of S-boxes and their strength can be found in [6-7]. These works provide valuable insights and contributions to the understanding and evaluation of S-box designs and their cryptographic properties

In [8], a new approach is presented for constructing an S-box using elliptic curves. The construction of the S-box is based on considering the ordinate of the curve as a key element in the process. According to [9], the projective general linear group is used to construct an S-box. The study focuses on exploring different aspects of S- box construction, aiming to develop a secure and improved S-box that enhances the encryption process.

The use of elliptic curves in cryptographic scenarios is of paramount importance for several reasons. The key advantage lies in the fact that elliptic curves offer a level of security comparable to classical systems while requiring fewer bits. A notable illustration can be found in [10], where it is estimated that a 4096-bit key size in RSA provides an equivalent security level to a mere 313 bits in an elliptic curve system. This remarkable reduction in key size implies several practical benefits such as smaller chip sizes, reduced power consumption, and more efficient implementations in elliptic cryptosystems.

Consequently, elliptic curves (EC) play a pivotal role in the development of robust and efficient cryptosystems. The concept of elliptic curves in cryptography was initially introduced in [11]. This groundbreaking research marked the advent of elliptic curve cryptography (ECC) as a promising field of study and application within the realm of cryptography. The introduction of elliptic curves opened up new avenues for developing secure and efficient cryptographic algorithms, paving the way for significant advancements in data security.

Furthermore, Miller presents a cryptosystem in [11] that exhibits a notable improvement in efficiency compared to the Diffie-Hellman protocol. The cryptosystem described in this publication demonstrates a remarkable 20 percent increase in speed, making it an attractive alternative for secure key exchange and cryptographic operations. This advancement contributes to the ongoing evolution and optimization of cryptographic protocols, highlighting the potential benefits of incorporating elliptic curves in cryptographic systems.

The publication [12] presents the correlation between the points found on hyperelliptic curves, and the nonlinearity exhibited by S-boxes is investigated. A cryptosystem based on elliptic curves (EC) over finite fields is discussed in [13]. This research explores the application of elliptic curves in cryptographic systems, shedding light on their potential for secure and efficient encryption. By utilizing EC over finite fields, the cryptosystem presented in this publication offers a valuable alternative for ensuring the confidentiality and integrity of sensitive information. A comprehensive

comparison between elliptic curve cryptography (ECC) and RSA is provided in [14].

The concept of the discrete logarithm problem is discussed in detail in the work by Koblitz [15]. Extensive research has revealed that ECC offers enhanced security compared to RSA, even with considerably reduced key sizes. This observation underscores the advantages of ECC in terms of cryptographic strength. A comprehensive discussion on the applications and advantages of elliptic curve cryptography (ECC) is provided in [16].

Moreover, [17] introduces an alternative and innovative method to tackle the challenges associated with the design of substitution boxes (S-boxes) using random selection approaches.

Overall, [1] introduces a novel algebraic scheme for designing S-boxes that satisfy robustness criteria, utilizes multiple Galois fields for construction, optimizes nonlinearity, and demonstrates promising results in terms of performance for secure communication and image encryption.

It is important to mention that we have considered a novel approach to construct the S-box using the supersingular elliptic curve over a finite field.

2. Preliminaries

2.1. Finite Field

A finite field, also referred to as a Galois field, is characterized by a limited set of elements. The field with cardinality of q is denoted as $\mathbb{F}_q$. For instance, an example of a finite field is $\mathbb{F}_2$, which can be represented as $\mathbb{Z}/2\mathbb{Z}$ or simply as $\mathbb{Z}_2 = \{0,1\}$.

2.2. Irreducible Polynomial

Let F be a field. A polynomial $p(s) \in F[s]$ is said to be an irreducible if it cannot be factored into lower-degree polynomials over the field F. In other words, an irreducible polynomial has no nontrivial divisors apart from the constant polynomials (or units) in the field. Irreducible polynomials are fundamental building blocks in polynomial factorization and play a significant role in various areas of mathematics and algebraic structure.

2.3. Field Extension

Let two fields F and K are given with $F \subseteq K$, then we say that K is an extension field of F.

2.3.1. Example

• Since $t^2 + 1$ is an irreducible polynomial in $\mathbb{R}$, so $\mathbb{R}[t]/(t^2 + 1)$ is a field extension of $\mathbb{R}$ and isomorphic to $\mathbb{C}$. Hence $\mathbb{C}$ is a field extension of $\mathbb{R}$.

• Since $\mathbb{F}_2$ is a finite field and $t^8 + t^4 + t^3 + t + 1$ is an irreducible polynomial in $\mathbb{F}_2$. Then, its extension field or Galois field $GF\ (2^8)$ is defined as

$$\mathbb{F}_2[t]/(t^8 + t^4 + t^3 + t + 1) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_7\alpha^7 : a_i \in \mathbb{F}_2\}$$

2.4. Rational Points

A rational point on a curve $C/\mathbb{F}_q$ is defined by having its coordinates belonging to a finite field $\mathbb{F}_q$. Example: $(0:0:1)$ is a rational point on the curve $C: x^2 + xy = yz$ over $\mathbb{F}_2$.

2.5. Weierstrass Form

The most general form of a cubic in terms of s and t is:

$$f(s,t) = as^3 + bs^2t + cst^2 + dt^3 + es^2 + fst + gt^2 + hs + it + j = 0$$

Weierstrass made a significant contribution by demonstrating that it is possible to transform any cubic curve with a rational point into a standardized representation called the Weierstrass normal form. This form simplifies the equation of the cubic curve, making it easier to analyze and manipulate mathematically. The Weierstrass normal form has become a fundamental concept in the study of cubic curves, providing a standardized framework for further exploration and analysis in various mathematical disciplines. Here, let us define these special forms and then define the set of points forming the group structure on an elliptic curve E.

2.6. Normalized Weierstrass Form

A cubic of the form

$$t^2 = s^3 + as + b$$

is called the normal form. It is an important concept in the study of cubic curves. It is worth noting that for any cubic curve E defined over a field K that does not have characteristic 2 or 3, it is always possible to transform the curve into normal form.

2.7. Elliptic Curve over a Finite Field

In the context of this discussion, an elliptic curve defined over a finite field $\mathbb{F}_q$ can be characterized as follows, considering $\mathbb{F}_q$ where q is a power of a prime number p:

$$E(\mathbb{F}_q) = \{(s,t) \in \mathbb{F}_q^2 \,|\, t^2 = s^3 + as + b \bmod q, \text{ where } a,b,s,t \in \mathbb{F}q \cup \infty.$$

The condition $4a^3 + 27b^2 \neq 0$ is imposed, ensuring that the curve does not possess singular points. Here ∞, represents the point at infinity, which is an essential element in the group structure associated with elliptic curves.

This definition establishes the set of points on the elliptic curve over the finite field $\mathbb{F}_q$ satisfying the specified equation. The exclusion of singular points guarantees that the curve exhibits the desired properties required for elliptic curve cryptography and other related applications.

2.8. Group Law

Consider an elliptic curve E defined by the equation $t^2 = s^3 + as + b$. Let $P = (s_1, t_1)$ and $Q = (s_2, t_2)$ be distinct points on the curve E , excluding the point at infinity denoted as ∞. The sum of P and Q is $R = (s_3, t_3)$ defined as follows:

- If $s_1 \neq s_2$, then $s_3 = m^2 - s_1 - s_2, t_3 = m(s_1 - s_3) - t_1$, where $m = \frac{t_2 - t_1}{s_2 - s_1}$.
- If $s_1 = s_2$ but $t_1 \neq t_2$ then $P + Q = \infty$.
- If $P = Q$ and $t_1 \neq 0$, then $s_3 = m^2 - 2s_1, t_3 = m(s_1 - s_3)$, where $m = \frac{3s_1^2 + a}{2t_1}$.
- If $P = Q$ and $t_1 = 0$, then $P + Q = \infty$.
- Moreover, it is defined that $P + \infty = P$ for all points P on E.

2.9. Hasse Weil Bound

$$q + 1 - 2g\sqrt{q} \leq N_q(g) \leq q + 1 + 2g\sqrt{q}$$

where $N_q(g)$ denotes the number of rational points of an elliptic C over a finite field $\mathbb{F}_q$.

2.10. The Frobenius Trace

Consider an elliptic curve $E/\mathbb{F}_q$, where $\mathbb{F}_q$ is a finite field. In this context, Frobenius trace can be defined as follows:

$a = q + 1 - \#E(\mathbb{F}_q)$.

2.11. Supersingular Elliptic Curve

Consider a finite field $\mathbb{F}_q$ with characteristic p greater than or equal to 3.Suppose $E/\mathbb{F}_q$ is an elliptic curve represented by a Weierstrass form.

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

where $f(s) \in \mathbb{F}_q[s]$ is a cubic polynomial with different roots in $\overline{\mathbb{F}}_q$. Then, E is supersingular if the co-efficient of s^{p-1} in $f(s)^{\frac{p-1}{2}}$ is zero.

It is well known that in supersingular elliptic curve if q is the order of a finite field with characteristic p, then $\#E(\mathbb{F}_q) = q + 1$.

3. S-Box Construction Technique

This section primarily focuses on the composition and design of our S-box. To better understand the algorithm, it is necessary to review certain fundamental facts and concepts.

A function $f: \mathbb{F}_2^n \to \mathbb{F}_2$ is referred to as a Boolean function. We establish a vectorial Boolean function $F: \mathbb{F}_2^n \to \mathbb{F}_2^m$ as

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

where $s = (s_1, s_2, .., s_n) \in \mathbb{F}_2^n$ and each of f_i 's for $1 \leq i \leq m$ *is* a Boolean function also known as a coordinate Boolean function. An $n \times n$ S-box is precisely defined as a vectorial Boolean function

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

For constructing S-boxes, the use of a nonlinear bijective map is generally required. Numerous algorithms have been proposed in the literature employing such maps or their compositions to synthesize S-boxes with robust cryptographic properties. In our research, we propose a novel approach for constructing S-boxes using rational points of supersingular elliptic curves over a finite field. The rational points form an Abelian group under the previously mentioned composition known as the Group Law. It is worth noting that the addition of points in this group does not correspond to conventional addition, which can lead to confusion. However, we leverage this unique group structure to construct the S-box. By harnessing the properties of this group, we aim to develop S-boxes that possess enhanced cryptographic strength and resistance against attacks.

This section introduces an uncomplicated approach for producing S-boxes with robust cryptographic strength. The construction method relies on using supersingular elliptic curves over a finite field $\mathbb{F}_q$. The proposed algorithm encompasses five key steps, outlined as follows:

- Considering a supersingular elliptic curve $E: t^2 = s^3 + as + b$ over $\mathbb{F}_q$.
- Generating number of rational points of E over $\mathbb{F}_q$.

It gives $E(\mathbb{F}_q)$ the set of rational points. By the property of the supersingular elliptic curve $\#E(\mathbb{F}_q) = q + 1$.

- Let E_t denotes the set of all $t - coordinates$ of the rational points of E.
- Applying modulo 256 on the set E_t . This operation confines the values of E_t within the range of 0 to 255.
- Finally, an S-box is derived by meticulously choosing the initial 256 unique integers from the set E_t.

3.1. Example of an S-Box

In this section, we present a straightforward technique for generating S-boxes that possess robust cryptographic properties. The construction method is based on using a supersingular elliptic curve over a finite field $\mathbb{F}_{257}$. The algorithm proposed comprises five fundamental steps, as given below:

- Considering a supersingular elliptic curve $E: t^2 = s^3 + 3$ over $\mathbb{F}_{257}$.
- Generating number of rational points of E over $\mathbb{F}_{257}$.

It gives

$E(\mathbb{F}_{257}) =$
$\{(0:1:0), (1:2:1), (1:255:1), \ldots, (256:197:1)\}$.

By the property of supersingular curve $\#E(\mathbb{F}_{257}.) = 258$.

- Let E_t denotes the set of all $t - coordinates$ of the rational points of E.

• Applying modulo 256 on the set E_t. This operation confines the values of E_t within the range of 0 to 255.

• Finally, an S-box is derived by meticulously choosing the initial 256 unique integers from the set E_t.

Table 1 The proposed S-box

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

4. Properties of S-Boxes

4.1. Nonlinearity

For an S-box $S: GF(2^n) \rightarrow GF(2^m)$ such that $S(u) = v$, where $u \in GF(2^n); v \in GF(2^m)$.

Nonlinearity can be calculated as [18]:

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

where $W(u,v)$ is Walsh transform defined as:

$$W(u,v) = \sum_{x \in GF(2^n)} (-1)^{v \cdot f(x) \oplus u \cdot x}$$

4.2. Strict Avalanche Criterion

The strict avalanche criterion (SAC) serves as a formal measure of the avalanche effect in cryptographic systems. According to the SAC, a desirable property is achieved when the complementation of a single input bit results in each output bit changing with an equal probability of 50%. As explained in [19], this criterion provides a quantifiable standard for assessing the effectiveness and strength of cryptographic algorithms in terms of their ability to produce significant changes in output for even minor modifications in input.

4.3. Bit Independence Criterion

As outlined in [19], the bit independence criterion (BIC) stipulates that in a cryptographic system, when a single input bit i is inverted, the resulting changes in output bits j and k should occur independently. This criterion emphasizes that there should be no correlation or dependency between the changes in different output bits when a single input bit is modified.

4.4. Differential Uniformity

According to [20], the resistance of an S-box against differential cryptanalysis is improved with smaller values of differential uniformity. It is a measure used to assess the quality of an S-box, indicating how effectively it resists differential cryptanalysis. Its lower value indicates a stronger S-box, as it implies that small input differences lead to significant output differences, making it harder for an attacker to exploit differential characteristics and break the encryption scheme. Therefore, minimizing the differential uniformity is crucial for enhancing the resistance of an S-box.

4.5. Linear Approximation

According to [20], the resistance of an S-box against linear cryptanalysis is improved with lower values of linear approximation. Linear approximation is a metric used to evaluate the strength of an S-box, measuring its susceptibility to linear cryptanalysis.

4.6. Differential Branch Number

The differential branch number of an S-box $S: GF(2^n) \rightarrow GF(2\text{^}m)$ is calculated by the formula [21]:

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

where $u_1, u_2 \in GF(2^n)$.

The primary characteristic sought in a high-quality S-box is its elevated nonlinearity. Typically, researchers evaluate several parameters such as BIC, SAC, DU, and nonlinearity to assess S-box cryptographic strength. We have expanded the scope to include additional indicators such as the DBN, linearity, and linear branch number. These metrics provide valuable insights into the S-box resistance to differential attacks, enhancing its overall resilience and robustness.

Advanced Encryption Standard (AES) stands out as one of the leading symmetric block ciphers due to its exceptional cryptographic properties. In particular, AES achieves a nonlinearity value of 112, which is considered highly desirable. It is worth noting that for an 8×8 S-box, the maximum attainable nonlinearity is 120. Constructing an S-box that satisfies all desirable

properties simultaneously is an inherent challenge, making nonlinearity a primary consideration in assessing S-box quality. However, a trade-off exists between nonlinearity and other important properties as higher nonlinearity can lead to potential weaknesses or inadequacies in satisfying other desirable criteria. This necessitates a careful balance between nonlinearity and the overall cryptographic strength of an S-box.

5. Comparing Performance of Different S-Boxes

Table 2 Comparison of different S-boxes with the proposed S-box

S-box	Non-linearity	SAC	BIC	DU	LP	DBN	LBN
Proposed S-box	108	0.4891	107.25	8	0.0763	3	3
AES (1999)	112	0.5058	112	4	0.0625	..	..
[1]	110.75	0.5012	110.64	6	0.0781	..	..
[22]	108.75	0.4946	94	10	0.1328	..	..
[23]	110.25	0.50	104	10	0.125	..	..
[24]	100	0.4812	96	16	0.1796	..	..
[25]	109	0.5026	102	10	0.1406	..	..
[26]	107.5	0.4971	196	10	0.125	..	..
[27]	107	0.5015	98	10	0.1484	..	..
[28]	108	0 .5073	100	10	0.1523	..	..
[29]	107.5	0 .5036	90	10	0.1484	..	..
[30]	106.5	0.4995	98	10	0.1172	..	..
[31]	107.5	0.4943	98	10	0.125	..	..
[32]	105.5	0.4946	96	10	0.1328	..	..
[33]	109.25	0.5012	104	8	0.0937	..	..
[34]	106.75	0.5034	100	10	0.1328	..	..
[35]	106.75	0.4939	102	16	0.125	..	..
[36]	107.25	0.5034	98	12	0.1328	..	..
[37]	106.75	0.4941	98	10	0.1250	..	..
[38]	106.75	0.4076	98	10	0.1328	..	..
[39]	106	0.5066	96	12	0.1445	..	..
[40]	107.75	0.4976	100	10	0.125	..	..
[41]	109.5	0.4985	98	10	0.1328	..	..
[42]	108.5	0.5017	100	10	0.1328	..	..

6. Conclusion

In our research, we devised a comprehensive algorithm for constructing diverse S-boxes using supersingular elliptic curves represented by the equation $t^2 = s^3 + as + b$. Notably, the suppersingular elliptic curves yield distinct S-boxes based on the specific values of parameters a and b, satisfying the condition of supersingularity. Each supersingular elliptic curve corresponds to a unique S-box, allowing for several possibilities and variations in S-box construction. This approach offers flexibility and versatility in generating different S-boxes, expanding the options available for cryptographic systems, and enhancing their resistance against attacks. Furthermore, as part of our research we have successfully constructed a specific S-box and rigorously evaluated its properties according to the performance metrics outlined in the table of Performance comparison of different S-boxes. The results of this evaluation demonstrate that the proposed S-box satisfies the essential criteria of a high-quality and effective S-box. The thorough analysis of the proposed S-box considering its performance in terms of cryptographic strength, nonlinearity, differential uniformity, and other relevant factors confirms its suitability for secure and reliable cryptographic applications.

References

[1] RAZAQ A, AHMAD M, & EL-LATIF A A A. A novel algebraic construction of strong S-boxes over double GF (27) structures and image protection. *Computational and Applied Mathematics*, 2023, 42(2): 90. https://doi.org/10.1007/s40314-023-02215-y

[2] BELAZI A, ABD EL-LATIF A A, & BELGHITH S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, 2016, 128:155-170. https://doi.org/10.1016/j.sigpro.2016.03.021

[3] BELAZI A, ABD El-LATIF A A, RHOUMA R, & BELGHITH S. Selective image encryption scheme based on DWT, AES S-box and chaotic permutation. In *2015 International wireless communications and mobile computing conference (IWCMC)* 2015, 606-610. IEEE. https://doi.org/10.1109/IWCMC.2015.7289152

[4] STANDARD D E. National Bureau of Standards (US). Federal Information Processing Standards Publication 46. National Technical Information Service. *Springfield, VA*,1977.

[5] RIJMEN V. Cryptanalysis of Advanced Encryption Standard. *Summer School on Design and Security of Cryptographic Functions, Algorithms and Devices*, 2013.

[6] CUI L, & CAO Y. A new S-box structure named affine-power-affine. *International Journal of Innovative Computing, Information and Control*, 2007, 3(3): 751-759.

[7] BIHAM E, & SHAMIR A. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 1991, 4: 3-

72.
[8] HAYAT U, & AZAM N A. A novel image encryption scheme based on an elliptic curve. *Signal Processing*, 2019, 155: 391-402. https://doi.org/10.1016/j.sigpro.2018.10.011.
[9] ALTALEB A, SAEED M. S, HUSSAIN I, & ASLAM M. An algorithm for the construction of substitution box for block ciphers based on projective general linear group. *AIP Advances*, 2017, *7*(3). https://doi.org/10.1063/1.4978264
[10] BLAKE I, SEROUSSI G, & SMART N. *Elliptic Curves in Cryptography* (London Mathematical Society Lecture Note Series). Cambridge: Cambridge University Press, 1999. https://doi.org/10.1017/CBO9781107360211
[11] MILLER V S. Use of Elliptic Curves in Cryptography. *Conference on the Theory and Application of Cryptographic Techniques*, 1985.
[12] CHEON J H, CHEE S, & PARK C. S-boxes with controllable nonlinearity. *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques* Berlin, Heidelberg: Springer Berlin Heidelberg, 1999: 286-294.
[13] KOBLITZ N. Elliptic curve cryptosystems. *Mathematics of Computation*, 1987, 48(177): 203-209.
[14] AMARA M, & SIAD A. Elliptic curve cryptography and its applications. *Proceedings of the International workshop on Systems, signal processing and their applications WOSSPA*, 2011: 247-250 IEEE. https://doi.org/10.1109/WOSSPA.2011.5931464
[15] KOBLITZ N, MENEZES A, & VANSTONE S. The state of elliptic curve cryptography. *Designs, Codes and Cryptography*, 2000 19: 173-193.
[16] VANSTONE S. A. Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments. *Information Security Technical Report*, 1997, 2(2): 78-87.
[17] ARTUGER F, & ÖZKAYNAK F. A method for generation of substitution box based on random selection. *Egyptian Informatics Journal*, 2022, 23(1): 127-135. https://doi.org/10.1016/j.eij.2021.08.002
[18] CARLET C, & DING C. Nonlinearities of S-boxes. *Finite Fields and their Applications*, 2007, 13(1): 121-135. https://doi.org/10.1016/j.ffa.2005.07.003
[19] LEVINSKAS M, & MIHALKOVICH A. Avalanche effect and bit independence criterion of perfectly secure Shannon cipher based on matrix power. *Mathematical Models in Engineering*, 2021, 7(3): 50-53.
[20] MOHAMED K, PAUZI M N M, ALI F H H M, ARIFFIN S, & ZULKIPLI N H. N. Study of S-box properties in block cipher. *Proceedings of the 2014 International Conference on Computer, Communications, and Control Technology*, 2014, 362-366.
[21] SARKAR S, & SYED H. Bounds on differential and linear branch number of permutations. *Proceedings of the Australasian Conference on Information Security and Privacy*, 2018, 207-224. Cham: Springer International Publishing.
[22] ZHANG T, CHEN C P, CHEN L, XU X, & HU B. Design of highly nonlinear substitution boxes based on I-Chingoperators. *IEEE Transactions on Cybernetics*, 2018, 48(12): 3349-3358. https://doi.org/10.1109/TCYB.2018.2846186.
[23] ALZAIDI A A, AHMAD M, DOJA M N, AL SOLAMI E, & BEG M S. A new 1D chaotic map and $\beta $-hill climbing for generating substitution-boxes. *IEEE Access*, 2018, 6: 55405-55418.
[24] KHAN M, SHAH T, & BATOOL S I. Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Computing and Applications*, 2016, 27: 677-685. https://doi.org/10.1007/s00521-015-1887-y
[25] YONG W, & PENG L. An improved method to obtaining S-box based on chaos and genetic algorithm. *HKIE Transactions*, 2012, 19(4): 53-58. https://doi.org/10.1080/1023697X.2012.10669006.
[26] GUESMI R, FARAH M A B, KACHOURI A, & SAMET M. A novel design of Chaos based S-Boxes using genetic algorithm techniques. *Proceedings of the International Conference on Computer Systems and Applications*, 2014, 678-684 https://doi.org/10.1109/AICCSA.2014.7073265.
[27] AHMAD M, BHATIA D, & HASSAN Y. A novel ant colony optimization based scheme for substitution box design. *Procedia Computer Science*, 2015, 57: 572-580. https://doi.org/10.1016/j.procs.2015.07.394
[28] TIAN Y, & LU Z. S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm. *Journal of Systems Engineering and Electronics*, 2016, 27(1): 232-241.
[29] AHMAD M, MITTAL N, GARG P, & KHAN M M. Efficient cryptographic substitution box design using travelling salesman problem and chaos. *Perspectives in Science*, 2016, 8: 465-468. https://doi.org/10.1016/j.pisc.2016.06.001
[30] FARAH T, RHOUMA R, & BELGHITH S. A novel method for designing S-box based on chaotic map and teaching–learning-based optimization. *Nonlinear Dynamics*, 2017, 88(2): 1059-1074. https://doi.org/10.1007/s11071-016-3295-y.
[31] AHMED H A, ZOLKIPLI M F, & AHMAD M. A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. *Neural Computing and Applications*, 2019, 31: 72017210. https://doi.org/10.1007/s00521-018-3557-3
[32] KHAN M, SHAH T, MAHMOOD H, & GONDAL M A. An efficient method for the construction of block cipher with multi-chaotic systems. *Nonlinear Dynamics*, 2013, 71: 489-492. https://doi.org/10.1007/s11071-012-0675-9
[33] LAMBIC D. A novel method of S-box design based on chaotic map and composition method. *Chaos, Solitons & Fractals*, 2014, 58: 16-21. https://doi.org/10.1016/j.chaos.2013.11.001.
[34] LAMBIC D. A novel method of S-box design based on discrete chaotic map. *Nonlinear Dynamics*, 2017, 8: 2407-2413. https://doi.org/10.1007/s11071-016-3199-x.
[35] ULLAH A, JAMAL S S, & SHAH T. A novel construction of substitution box using a combination of chaotic maps with improved chaotic range. *Nonlinear Dynamics*, 2017, 88: 2757-2769. https://doi.org/10.1007/s11071-017-3409-1
[36] ATTAULLAH, JAMAL, S. S, & SHAH, T. A novel algebraic technique for the construction of strong substitution box. *Wireless Personal Communications 99*, 2018: 213–226 https://doi.org/10.1007/s11277-017-5054-x
[37] ÖZKAYNAK F. Construction of robust substitution boxes based on chaotic systems. *Neural Computing and Applications*, 2019, 31(8): 3317-3326. https://doi.org/10.1007/s00521-017-3287-y

[38] YE T, & ZHIMAO L. Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. *Nonlinear Dynamics*, 2018, 94: 2115-2126. https://doi.org/10.1007/s11071-018-4478-5.
[39] SILVA-GARCIA V M, FLORES-CARAPIA R, RENTERIA-MARQUEZ C, LUNA-BENOSO B, & ALDAPE-PEREZ M. Substitution box generation using Chaos: An image encryption application. *Applied Mathematics and Computation*, 2018, 332: 123-135. https://doi.org/10.1016/j.amc.2018.03.019
[40] YI L, TONG X, WANG Z, et al. A novel block encryption algorithm based on chaotic S-box for wireless sensor network. *IEEE Access*, 2019, 7: 53079-53090. https://doi.org/10.1109/ACCESS.2019.291139
[41] ALZAIDI A A, AHMAD M, AHMED H S, & SOLAMI E A. Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map. *Complexity*, 2018, 1-16. https://doi.org/10.1155/2018/9389065.7.
[42] AL SOLAMI E, AHMAD M, VOLOS C, & BEG M M S. A new hyperchaotic system-based design for efficient bijective substitution-boxes. *Entropy*, 2018, 20(7): 525. https://doi.org/10.3390/e20070525

参考文:

[1] RAZAQ A、AHMAD M 和 EL-LATIF A A A。双 GF (27)结构和图像保护上强 S 盒的新颖代数构造。计算与应用数学，2023，42（2）：90。https://doi.org/10.1007/s40314-023-02215-y
[2] BELAZI A, ABD EL-LATIF A A, 和 BELGHITH S. 一种基于替换排列网络和混沌的新型图像加密方案。信号处理，2016，128：155-170。https://doi.org/10.1016/j.sigpro.2016.03.021
[3] BELAZI A, ABD El-LATIF A A, RHOUMA R, 和 BELGHITH S. 基于载重吨、AES S 盒和混沌排列的选择性图像加密方案。2015 年国际无线通信与移动计算大会（IWCMC）2015，606-610。IEEE。https://doi.org/10.1109/IWCMC.2015.7289152
[4] STANDARD D E. 国家标准局（美国）。联邦信息处理标准出版物 46。国家技术信息服务。弗吉尼亚州斯普林菲尔德，1977。
[5] RIJMEN V. 高级加密标准的密码分析。密码功能、算法和设备的设计和安全暑期学校，2013。
[6] CUI L, 和 CAO Y. 一种新的 S 盒结构，名为仿射-幂-仿射。国际创新计算、信息与控制杂志，2007，3(3)：751-759。
[7] BIHAM E 和 SHAMIR A. 类 DES 密码系统的差分密码分析。密码学杂志，1991，4：3-72。
[8] HAYAT U, 和 AZAM N A. 一种基于椭圆曲线的新型图像加密方案。信号处理，2019，155：391-402。https://doi.org/10.1016/j.sigpro.2018.10.011。
[9] ALTALEB A, SAEED M. S, HUSSAIN I, 和 ASLAM M. 基于射影一般线性群的分组密码替换盒构造算法。AIP 进展，2017，7(3)。https://doi.org/10.1063/1.4978264
[10] BLAKE I、SEROUSSI G 和 SMART N。密码学中的椭圆曲线（伦敦数学会讲座系列）。剑桥：剑桥大学出版社，1999。https://doi.org/10.1017/CBO9781107360211
[11] MILLER V S. 椭圆曲线在密码学中的使用。密码技术理论与应用会议，1985。
[12] CHEON J H、CHEE S 和 PARK C。具有可控非线性的 S 盒。柏林密码技术理论与应用国际会议论文集，海德堡：施普林格柏林海德堡，1999：286-294。
[13] KOBLITZ N. 椭圆曲线密码系统。计算数学，1987，48（177）：203-209。
[14] AMARA M 和 SIAD A. 椭圆曲线密码学及其应用。系统、信号处理及其应用国际研讨会论文集沃斯帕，2011：247-250 IEEE。https://doi.org/10.1109/WOSSPA.2011.5931464
[15] KOBLITZ N、MENEZES A 和 VANSTONE S。椭圆曲线密码学的状态。设计、代码和密码学，2000, 19：173-193。
[16] VANSTONE S.A. 椭圆曲线密码系统——用于保护受限环境的强大、快速的公钥密码学的答案。信息安全技术报告，1997，2(2)：78-87。
[17] ARTUGER F, 和 ÖZKAYNAK F. 一种基于随机选择的替换框生成方法。埃及信息学杂志，2022，23(1)：127-135。https://doi.org/10.1016/j.eij.2021.08.002
[18] CARLET C, 和 DING C. S 盒的非线性。有限域及其应用，2007，13(1)：121-135。https://doi.org/10.1016/j.ffa.2005.07.003
[19] LEVINSKAS M, 和 MIHALKOVICH A. 基于矩阵幂的完美安全香农密码的雪崩效应和位独立准则。工程数学模型, 2021, 7(3): 50-53.
[20] MOHAMED K、PAUZI M N M、ALI F H H M、ARIFFIN S 和 ZULKIPLI N H.N。分组密码中 S 盒特性的研究。2014 年计算机、通信和控制技术国际会议论文集，2014，362-366。
[21] SARKAR S, 和 SYED H. 排列的微分和线性分支数的界限。澳大利亚信息安全和隐私会议论文集，2018，207-224。查姆：施普林格国际出版社。
[22] ZHANG T, CHEN C P, CHEN L, XU X, 和 HU B。基于易经算子的高非线性替换盒设计。IEEE 控制论学报，2018，48(12)：3349-3358。

https://doi.org/10.1109/TCYB.2018.2846186。

[23] ALZAIDI A A、AHMAD M、DOJA M N、AL SOLAMI E 和 BEG M S。用于生成替换框的新一维混沌地图和$\贝塔$-爬山。IEEE 访问，2018，6：55405-55418。

[24] KHAN M, SHAH T, 和 BATOOL S I. 基于混沌布尔函数的 S 盒构建及其在图像加密中的应用。神经计算与应用，2016，27：677-685。https://doi.org/10.1007/s00521-015-1887-y

[25] YONG W, 和 PENG L. 一种基于混沌和遗传算法的改进 S 盒获取方法. 香港工程师学会学报，2012，19(4): 53-58. https://doi.org/10.1080/1023697X.2012.10669006

[26] GUESMI R、FARAH M A B、KACHOURI A 和 SAMET M。使用遗传算法技术的基于混沌的 S 盒的新颖设计。国际计算机系统与应用会议论文集，2014, 678-684 https://doi.org/10.1109/AICCSA.2014.7073265。

[27] AHMAD M、BHATIA D 和 HASSAN Y。一种基于蚁群优化的替换盒设计方案。计算机科学，2015，57：572-580。https://doi.org/10.1016/j.procs.2015.07.394

[28] TIAN Y, 和 LU Z. S 盒：六维复合超混沌映射和人工蜂群算法。系统工程与电子学报, 2016, 27(1): 232-241.

[29] AHMAD M、MITTAL N、GARG P 和 KHAN M M。利用旅行商问题和混沌进行高效密码替换盒设计。科学展望，2016，8：465-468。https://doi.org/10.1016/j.pisc.2016.06.001

[30] FARAH T, RHOUMA R, 和 BELGHITH S. 一种基于混沌映射和基于教学优化的 S 盒设计新方法。非线性动力学，2017，88(2)：1059-1074。https://doi.org/10.1007/s11071-016-3295-y。

[31] AHMED H A, ZOLKIPLI M F, 和 AHMAD M. 一种基于萤火虫算法和离散混沌映射的新型高效替换盒设计。神经计算与应用，2019，31：72017210。https://doi.org/10.1007/s00521-018-3557-3

[32] KHAN M、SHAH T、MAHMOOD H 和 GONDAL M A。一种构建多混沌系统分组密码的有效方法。非线性动力学，2013，71：489-492。https://doi.org/10.1007/s11071-012-0675-9

[33] LAMBIC D. 一种基于混沌映射和合成方法的 S 盒设计新方法。混沌、孤子和分形，2014，58：16-21。https://doi.org/10.1016/j.chaos.2013.11.001。

[34] LAMBIC D. 一种基于离散混沌映射的 S 盒设计新方法。非线性动力学，2017，8：2407-2413。https://doi.org/10.1007/s11071-016-3199-x。

[35] ULLAH A、JAMAL S S 和 SHAH T。一种新颖的替换盒结构，使用混沌映射和改进的混沌范围的组合。非线性动力学，2017，88：2757-2769。https://doi.org/10.1007/s11071-017-3409-1

[36] ATTAULLAH, JAMAL, S. S, 和 SHAH, T. 一种用于构造强替换框的新颖代数技术。无线个人通信 99, 2018: 213-226 https://doi.org/10.1007/s11277-017-5054-x

[37] ÖZKAYNAK F. 基于混沌系统的稳健替换盒的构建。神经计算与应用，2019, 31(8): 3317-3326。https://doi.org/10.1007/s00521-017-3287-y

[38] YE T, 和 ZHIMAO L. 混沌 S 盒：六维分数阶洛伦兹-达芬混沌系统和氧型路径置乱。非线性动力学，2018，94：2115-2126。https://doi.org/10.1007/s11071-018-4478-5。

[39] SILVA-GARCIA V M、FLORES-CARAPIA R、RENTERIA-MARQUEZ C、LUNA-BENOSO B 和 ALDAPE-PEREZ M。使用混沌生成替换框：图像加密应用程序。应用数学与计算，2018，332：123-135。https://doi.org/10.1016/j.amc.2018.03.019

[40] YI L, TONG X, WANG Z, 等。一种基于混沌 S 盒的无线传感器网络分组加密算法 IEEE 访问，2019，7：53079-53090。https://doi.org/10.1109/ACCESS.2019.291139

[41] ALZAIDI A A、AHMAD M、AHMED H S 和 SOLAMI E A。使用增强的混沌映射动力学构建基于正余弦优化的双射替换框。复杂性，2018，1-16。https://doi.org/10.1155/2018/9389065.7。

[42] AL SOLAMI E、AHMAD M、VOLOS C 和 BEG M M S。一种基于超混沌系统的高效双射替换盒设计。熵，2018，20（7）：525。https://doi.org/10.3390/e20070525