The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering and Mathematics (EPSTEM), 2025

Volume 36, Pages 102-109

ICBAST 2025: International Conference on Basic Sciences and Technology

# Design of S-Boxes Based on Alternative Irreducible Polynomials

**Zhanat Saukhanova**
L.N. Gumilyov Eurasian National University

**Gulmira Shakhmetova**
L.N. Gumilyov Eurasian National University

**Altynbek Sharipbay**
L.N. Gumilyov Eurasian National University

**Alibek Barlybayev**
L.N. Gumilyov Eurasian National University

**Sayat Raykul**
L.N. Gumilyov Eurasian National University

**Altay Khassenov**
L.N. Gumilyov Eurasian National University

**Abstract**: In the era of rapid digital technology development, the volume of information transmitted in cyberspace is significantly increasing, thereby intensifying the need to ensure confidentiality and the protection of personal data. Modern cryptographic methods are used for such purposes. One of the most widely used encryption algorithms is Advanced Encryption Standard (AES), which employs substitution box (S-box) to enhance the security of the encryption process. S-box is one of the important components of the block algorithm. The robustness of an S-box is largely determined by its architecture and algebraic basis. In this paper, a method for constructing S-boxes is proposed based on various alternative irreducible polynomials with the addition of a constant 8-bit vector, different from that used in the AES standard. A total of 16 S-boxes were constructed and their performance was evaluated using standard cryptographic criteria, including nonlinearity, strict avalanche effect, etc. The results demonstrated that the proposed S-boxes exhibit performance comparable to that of the standard AES S-box. This study is conducted within the framework of grant funding from the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (grant No. AP19677422).

**Keywords:** Cryptography, Advanced encryption standard (AES), Substitution box (S-box), Irreducible polynomial

## Introduction

AES is a widely used block symmetric encryption cryptosystem. The Rijndael algorithm was declared the AES standard in 2002 by the US National Institute of Standards and Technology (NIST). This algorithm provides encryption of 128 bits of plaintext using a key of 128, 192, or 256 bits. For encryption in each round of the algorithm, transformations such as ByteSub, ShiftRows, MixColumns, AddRoundKey are used (Dworkin et al., 2021). One of the important nonlinear components in the structure of the Rijndael algorithm is the cryptographic substitution table (or S-Box), which is applied at the ByteSub stage.

A cryptographic S-box is used to transform input bits into output bits to ensure their randomization and increase cryptographic strength (El Gaabouri et. al., 2024). In standard AES, the irreducible polynomial $t(x) = x^8 + x^4 + x^3 + x + 1$ and the constant $63_{16}$ are used to generate the S-box (Nitaj et.al., 2020). This combination is known to potential attackers. Therefore, the generation of new S-boxes with the same cryptographic properties as the traditional one expands the capabilities of block algorithms.

The use of alternative S-boxes increases the security of the cryptographic algorithm. In this paper, various irreducible polynomials and constants were considered, on the basis of which 16 new S-boxes were constructed. The proposed S-boxes were tested for cryptographic criteria such as balance, bijective, nonlinearity, Strict avalanche criterion (SAC), differential uniformity, fixed points and periods. The results showed that the proposed S-boxes have performance indicators comparable to those of the original AES S-box.

## Method

### Traditional S-box in Rijndael Algorithm

In the symmetric block cipher Rijndael (AES), the replacement byte (S-box) function $S$ is represented as a composition of two mappings $S(x) = f(x) \circ g$ , where $x \in \mathbb{F}_{2^8}$, defined over the Galois field $GF(2^8)$ (Daemen, 2002).

The first transformation $f(x): GF(2^8) \to GF(2^8)$ implements the calculation of the multiplicative inverse element using the formula:

$$f(x) = \begin{cases} 0, if\ x = 0, \\ x^{-1}, if\ x \neq 0. \end{cases} \quad (1)$$

Where $x^{-1}$ denotes the multiplicative inverse in the field $GF(2^8)$, while zero remains unchanged. The multiplication operation is performed modulo the irreducible polynomial $t(x) = x^8 + x^4 + x^3 + x + 1$.

The second transformation $g: GF(2^8) \to GF(2^8)$ is an affine mapping implemented through a bitwise operation. The affine function $g(x)$ is defined by the following equation:

$$g(x) = Ax + b, \quad (2)$$

where $A$ is an $8 \times 8$ bit matrix and $b$ is a constant. For an element $x = (x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0)$ of the field, the mapping $(x) = y$ is computed as follows:

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \\ 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

As an example, consider the element $x = 45 = 0010\ 1101 = 0x2d$.

Let us compute the transformation of the input element $S(0x2d) = 0xd8$:

1) $0x2d = (0,0,1,0,1,1,0,1)$ has a polynomial representation $x^5 + x^3 + x^2 + 1$

2) The inverse transform of the polynomial $x^5 + x^3 + x^2 + 1$ modulo the irreducible polynomial $t(x) = x^8 + x^4 + x^3 + x + 1$ is $f(x^5 + x^3 + x^2 + 1) = x^6 + x^2$, which has the form $(0,1,0,0,0,1,0,0)$ in binary representation.

3) Apply an affine transformation:

$$\begin{pmatrix}10001111\\11000111\\11100011\\11110001\\11111000\\01111100\\00111110\\00011111\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\\0\\0\\1\\0\end{pmatrix}+\begin{pmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\\1\\0\\1\\1\end{pmatrix}$$

4) Thus, the output of element $0x2d$ will be element (1,1,0,1,1,0,0,0) or $0xd8$.

**Proposed S-boxes**

This section of the article describes the proposed method for constructing 16 cryptographically strong 8×8 S-boxes, based on the use of some irreducible polynomials selected from the list of 30 irreducible polynomials of degree 8 (Planteen, 2019) and the affine transformation employed in the AES standard. As noted in the work (Ospanov et.al., 2022), by varying the selection of specific irreducible polynomials, the choice of the initial transformation from a set of alternative transformations, the selection of a particular affine transformation matrix, and a specific shift constant, it is possible to construct various optimal S-boxes. Table 1 shows the set of components used in constructing the proposed S-boxes.

Table 1. A set of components for constructing S-boxes

| S-boxes | Irreducible polynomial | Affine matrices | Constants |
|---|---|---|---|
| Sbox0 | $x^8+x^7+x^2+x+1$ | 11011001 | a3 |
| Sbox1 | | 11010110 | 72 |
| Sbox2 | | 01101101 | 18 |
| Sbox3 | | 01101101 | a0 |
| SBox4 | | 00011111 | 3d |
| Sbox5 | | 01001010 | 79 |
| Sbox6 | $x^8+x^4+x^3+x+1$ | 11101001 | dc |
| SBox7 | | 11010011 | e7 |
| SBox8 | | 00011100 | 3e |
| Sbox9 | | 11111000 | 5a |
| Sbox10 | $x^8+x^6+x^5+x+1$ | 00001000 | 22 |
| SBox11 | | 11110001 | eb |
| Sbox12 | | 00000001 | fb |
| SBox13 | $x^8+x^6+x^5+x^2+1$ | 10010001 | 2b |
| SBox14 | | 10000000 | f8 |
| SBox15 | $x^8+x^5+x^3+x^2+1$ | 11110111 | da |

As an example, Table 2 presents one of the sixteen S-boxes, namely Sbox14, which was constructed using the irreducible polynomial $t(x)=x^8+x^6+x^5+x^2+1$. The values obtained as a result of the multiplicative inverse transformation (1) are fed into the affine mapping as a bitwise vector $x=(x_7,x_6,x_5,x_4,x_3,x_2,x_1,x_0)$, corresponding to equation (2).

$$\begin{pmatrix}y_0\\y_1\\y_2\\y_3\\y_4\\y_5\\y_6\\y_7\end{pmatrix}=\begin{pmatrix}10000000\\01000000\\00100000\\00010000\\00001000\\00000100\\00000010\\00000001\end{pmatrix}\begin{pmatrix}x_0\\x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\end{pmatrix}+\begin{pmatrix}0\\0\\0\\1\\1\\1\\1\\1\end{pmatrix}$$

Table 2. Proposed SBox14

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

## Results and Discussion

For efficient encryption, the S-box must have strong algebraic properties that establish nonlinear relationships between its input and output values (Mahboob, 2023). This section presents the results of the analysis of the cryptographic characteristics of the 16 S-boxes we proposed. For the evaluation of S-boxes, the generally accepted tests described in the sources (Nizam Chew & Ismail, 2020), (Zahid, 2019) were used: the strict avalanche criterion (SAC), nonlinearity (NL), balanced, differential uniformity, algebraic degree, fixed points and period. The results of the comparative performance of our S-boxes with the standard AES S-box are presented in Table 3. In addition, this section includes a SageMath code listing developed to compute and verify several of the cryptographic criteria employed in the evaluation of the proposed S-boxes.

### Balanced Boolean Function

A Boolean function $f(x)$ is defined as *balanced* if it satisfies the condition given in formula (3):

$$H_W\big(f(x)\big) = \sum_{x=0}^{2n-1} f(x) = 2^{n-1} \qquad (3)$$

where $H_W$ is Hamming weight, and n is the number of Boolean variables. According to (Bejo & Adji, 2017), the Hamming weight indicates how balanced the output values are distributed, so it is one of the important cryptographic properties in the analysis of Boolean functions. In other words, the Boolean function is balanced if number of input values for which $f(x)$ =0 is equal to the number of input values for which $f(x)$ =1. This property ensures that the output values are uniform between 0 and 1, which avoids statistical bias that can be exploited in attacks. The balanced nature of the function confirms its cryptographic strength. All component Boolean functions of the proposed 16 S-box are balanced (number of 1's = number of 0's) (Table 3).

### Bijectivity

An $n \times n$ S-box is bijective when it acts as a permutation: every input maps to a unique output, yielding all $2^n$ distinct values within $[0, 2^{n-1}]$. The all 16 proposed $8 \times 8$ S-box produces 256 unique outputs over $[0,255]$, and thus meets the bijectivity criterion (Mahboob, 2023).

### Nonlinearity(NL)

The nonlinearity of an S-box is a fundamental cryptographic parameter that characterizes its resistance to linear cryptanalysis. It is defined as the Hamming distance between each component Boolean function of the S-box and the set of all affine functions. This characteristic is formally expressed as (Esa, 2022):

$$NL_f = 2^{n-1}(1 - 2^{-n}\max\ |W_f(z)|), \qquad (4)$$

where $W_f(z)$ denotes the Walish spectrum of the Boolean function, defined by:

$$W_f(z) = \sum(-1)^{f(x)\oplus x\cdot z}, \quad x, z \in \mathbb{F}(2^n).$$

Higher nonlinearity values indicate a reduced correlation between input and output bits under linear approximations, thereby enhancing the cryptographic strength of the substitution box. The theoretical upper bound for the nonlinearity of a Boolean function over the field $\mathbb{F}(2^n)$ is known to be 120, as established in (Carlet & Ding, 2007). The16 S-boxes developed in this work demonstrates an average nonlinearity of 112, which is comparable to that of the AES S-box (Table 3). The observed nonlinearity suggests that the designed S-box possesses strong resistance to linear cryptanalysis by minimizing linear correlations.

**Differential Uniformity**

Differential cryptanalysis is one of the most widely used cryptanalysis methods aimed at recovering plaintext or key information. The method is based on the analysis of differences between pairs of plaintexts and corresponding ciphertexts. Identifying stable dependencies between input and output differences can allow the cryptanalyst to draw conclusions about parts of the secret key. To ensure resistance to differential cryptanalysis, the S-box must have a low value of Differential Uniformity (DU). This characteristic is calculated using the following formula (Zahid, 2019):

$$DU = \max_{A_x \neq 0, B_x}[\#\{x \in Z | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}] \qquad (5)$$

where, $A_x$ and $B_x$ – input and output masks, respectively and $Z = \{0,1, \dots, 255\}$, are $\Delta x$ and $\Delta y$ the input and output differentials, respectively.

For example, for 8-bit substitutions, the optimal values of differential uniformity are values no greater than 8. According to Theorem 4.1 in work (Cui et. al., 2011) AES S-box has DU = 4. All S-boxes can be considered differentially 4-unitary, which is allowed in the practice of designing secure substitutions.

**Algebraic Degree**

The algebraic degree of an S-box is a fundamental cryptographic metric, defined as the maximum algebraic degree among its component Boolean functions when represented in Algebraic Normal Form (ANF) (Prévost & Martin, 2025). Formally, given a vectorial Boolean function $F: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the algebraic degree is:

$$\deg(F) = \max \deg(f_i), 1 \leq i \leq n \qquad (6)$$

where each $f_i$ denotes a single-bit output coordinate of the S-box. A high algebraic degree hinders attackers' ability to express or approximate the S-box using low-degree polynomial equations, thereby strengthening its resistance to algebraic attacks and interpolation methods. In the context of 8-bit S-boxes, a degree of 7-seen, for example, in the AES S-box—is considered optimal.

**Fixed Points**

Fixed points are important structural properties of substitution boxes that may reveal exploitable symmetries if not properly avoided. A fixed point is an input value $x \in \mathbb{F}(2^n)$ for which the S-box returns the same value as output, i.e., $S(x) = x$. In the presented results (Table 3), all S-boxes exhibit no fixed points, indicating that for every $x$, $S(x) \neq x$, thereby eliminating trivial self-mappings and enhancing resistance to iterative attacks.

**Periodicity of S-box**

Another cryptographic property of the S-box is its periodicity. Periodicity shows how many times the S-box needs to be used to return the initial input value to its original value. Periodicity analysis allows to estimate how resistant

the S-box is to repeated attacks (Cui et. al., 2011). Formally, for a function $F$, that maps elements from a field $\mathbb{F}_{2^n}$ to the same field $\mathbb{F}_{2^n}$, the period of an element $x$ is the smallest positive number p, for which $F^p(x) = x$.

The proposed S-boxes show a good result of periodicity. According to the results demonstrated in Table 3, the minimum period of cycle lengths is in the range from 2 to 10, and maximum varies from 88 to 215. The best result was shown by SBox14, in this S-box, to obtain each initial value, it is necessary to go through a period of 256 times, which indicates a single cycle of permutation. This property is highly desirable in cryptographic design because it maximizes diffusion and minimizes the risk of short cycle vulnerabilities that can be exploited in iterative attacks.

**StrictAvalancheCriterion (SAC)**

Another important cryptographic property of Boolean functions is the strong avalanche effect (SAC). This criterion was introduced by Webster and Tavares (Webster & Tavares, 1985) as a definition of strong S-boxes. According to SAC, changing one bit in the input of a strong S-box should change the output bit with probability close to 0.5. In formal terms, SAC is characterized by the following relation (Bejo & Adji, 2017):

$$\delta(x) = (\frac{1}{2^n}\sum_{i=1}^{n} f(x) \oplus f(x \oplus c_i^n)) \qquad (5)$$

Where $c_i^n$ denote an $n$-dimensional vector with Hamming weight equal to 1 at the $i$-th position. A cryptographic function is said to satisfy the Strict Avalanche Criterion (SAC) if all entries in the resulting output matrix are approximately equal to 0.5. For the 16 proposed S-boxes, the SAC values were computed using the built-in by Python. Each S-box was evaluated across all 8 input bits, and the resulting average output change probabilities were recorded. The results for all S-boxes fall within the range of [0.45, 0.55], with two instances—SBox4 and SBox10—exhibiting slightly higher symmetry with values closer to [0.47, 0.53].

**S-box Cryptographic Criterias Coded in Sage**

To analyze such cryptographic properties as: balanced, nonlinearity, differential uniformity, algebraic degree and fixed points, the mathematical tool SageMath was used. SageMath is a free open-source mathematical platform that provides an integrated environment for performing calculations and conducting scientific research (Esslinger, 2023). Within the framework of cryptographic tasks, SageMath offers a specialized module S-Boxes and Their Algebraic Representations, which allows calculating a wide range of cryptographic characteristics, including linear and differential parameters. Listing 1 is presented below, which shows the code for determining the cryptographic criteria of the presented S-boxes. SageMath code for cryptographic evaluation of the proposed S-box:

```
from sage.crypto.sbox import SBox
from sage.crypto.boolean_function import BooleanFunction
S = SBox([
0x8c, 0x90, 0xd9, 0xc1, 0x46, 0x63, 0x53, 0xf1, 0x61, 0x32, 0x15, 0x3e, ...
# ])
# Evaluation of cryptographic criteria
S.is_balanced()                                  # Balanced (should return True)
S.maximal_difference_probability_absolute()      # Differential uniformity
S.nonlinearity()                                 # Nonlinearity
S.max_degree()                                   # Algebraic degree
S.fixed_points()                                 # Fixed points
```

**Analysis of Cryptographic Properties of the Proposed S-boxes**

To evaluate the strength of the proposed S-boxes, their cryptographic properties were compared with those of the AES S-box, which is widely regarded as a benchmark in symmetric key cryptography. As mentioned in work (Seitkulov et.al., 2021) the AES S-box demonstrates high cryptographic robustness, with a nonlinearity of 112, algebraic degree of 7, and differential uniformity of 4. These values are essential for ensuring resistance against linear and differential cryptanalysis.

Table 3. Cryptographic properties of the proposed 16 S-boxes

| | Balanced | Nonlinearity | Differential uniformity | Algebraic degree | Fixed points | Periodicity | SAC |
|---|---|---|---|---|---|---|---|
| Sbox0 | True | 112 | 4 | 7 | [] | [6, 154] | [0.45, 0.55] |
| Sbox1 | True | 112 | 4 | 7 | [] | [2, 195] | [0.45, 0.55] |
| Sbox2 | True | 112 | 4 | 7 | [] | [2, 61] | [0.45, 0.55] |
| Sbox3 | True | 112 | 4 | 7 | [] | [2, 138] | [0.45, 0.55] |
| Sbox4 | True | 112 | 4 | 7 | [] | [3, 213] | [0.47, 0.53] |
| Sbox5 | True | 112 | 4 | 7 | [] | [2, 215] | [0.45, 0.55] |
| Sbox6 | True | 112 | 4 | 7 | [] | [4, 166] | [0.45, 0.55] |
| Sbox7 | True | 112 | 4 | 7 | [] | [2, 88] | [0.45, 0.55] |
| SBox8 | True | 112 | 4 | 7 | [] | [10, 109] | [0.45, 0.55] |
| Sbox9 | True | 112 | 4 | 7 | [] | [8, 166] | [0.45, 0.55] |
| SBox10 | True | 112 | 4 | 7 | [] | [2, 123] | [0.47, 0.53] |
| SBox11 | True | 112 | 4 | 7 | [] | [5, 133] | [0.45, 0.55] |
| SBox12 | True | 112 | 4 | 7 | [] | [3, 198] | [0.45, 0.55] |
| SBox13 | True | 112 | 4 | 7 | [] | [5, 210] | [0.45, 0.55] |
| SBox14 | True | 112 | 4 | 7 | [] | [256,256] | [0.45, 0.55] |
| SBox15 | True | 112 | 4 | 7 | [] | [3, 150] | [0.45, 0.55] |

It should be noted that all constructed S-boxes, in terms of the main cryptographic parameters, correspond to the AES S-box. They preserve the same optimal nonlinearity and algebraic degree, and exhibit minimal differential uniformity, which is essential for secure substitution. It is also worth mentioning that the SAC values lie within the acceptable cryptographic range [0.45, 0.55], indicating a well-balanced avalanche effect. Each of the proposed S-boxes has no fixed points and satisfies the periodicity conditions. This consistency across all cryptographic criteria confirms that the our S-boxes meet the level of cryptographic strength of the s-box used in the AES standard.

## Conclusion

The authors of this paper conducted a study of the construction of alternative S-boxes. A method for generating 16 new S-boxes was proposed, which consisted in using irreducible polynomials over a finite Galois field different from the standard. From the list of 30 irreducible polynomials, 5 were taken, for each of them their own unique affine matrices and individual constants were used. The use of such a set of components led to the structural diversity of the obtained S-boxes. The cryptographic resistance of the obtained S-boxes was tested according to the established criteria, such as bijectivity, balance, nonlinearity, strict avalanche criterion (SAC), differential homogeneity, algebraic degree, fixed points, and periodicity. Analysis of cryptographic metrics showed that all the proposed S-boxes meet the necessary conditions for their use as an alternative to the standard AES S-box.

## Scientific Ethics Declaration

*The authors declares that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

## Conflict of Interest

*The authors declare that they have no conflicts of interest

## Funding

*This research is funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP19677422).

## Acknowledgements or Notes

*This article was presented as an oral presentation at the International Conference on Basic Sciences and Technology ( www.icbast.net ) held in Budapest/Hungary on August 28-31, 2025.

## References

Bejo, A., & Adji, T. B. (2017, August). AES S-box construction using different irreducible polynomial and constant 8-bit vector. *2017 IEEE Conference on Dependable and Secure Computing* (pp. 366-369). IEEE.

Carlet, C., & Ding, C. (2007). Nonlinearities of S-boxes. *Finite Fields and Their Applications*, *13*(1), 121-135.

Cui, J., Huang, L., Zhong, H., Chang, C., & Yang, W. (2011). An improved AES S-box and its performance analysis. *International Journal of Innovative Computing, Information and Control*, *7*(5), 2291-2302.

Daemen, J., & Rijmen, V. (2002). *The design of Rijndael* (Vol. 2). New York: Springer-verlag.

Dworkin, M. J., Barker, E., Nechvatal, J. R., Foti, J., Bassham, L. E., Roback, E., & Dray Jr, J. F. (2001). *Advanced encryption standard* (AES). National Institute of Standards and Technology.

El Gaabouri, I., Senhadji, M., Belkasmi, M., & El Bhiri, B. (2024). A new S-box pattern generation based on chaotic enhanced logistic map: Case of 5-bit S-box. *Cybersecurity, 7*(1), 59.

Esa, N. F., Abdul-Latip, S. F., & Abu, N. A. (2022). A new design of substitution box with ıdeal strict avalanche criterion. *Malaysian Journal of Mathematical Sciences*, *16*(4).

Esslinger, B. (2023). *Learning and experiencing cryptography with cryptool and sagemath*. Artech House.

Mahboob, A., Nadeem, M., & Rasheed, M. W. (2023). A study of text-theoretical approach to S-box construction with image encryption applications. *Scientific Reports*, *13*(1), 21081.

Nitaj, A., Susilo, W., & Tonien, J. (2020). A new improved AES S-box with enhanced properties. *Australasian Conference on Information Security and Privacy* (pp. 125-141). Springer International Publishing.

Nizam Chew, L. C., & Ismail, E. S. (2020). S-box construction based on linear fractional transformation and permutation function. *Symmetry*, *12*(5), 826.

Ospanov, R., Seitkulov, E., & Ergalieva, B. (2022). A generalized algebraic method for constructing 8-bit rijndael S-boxes. *Bulletin of KazATK, 120*(1), 156-163.

Planteen, C. (2019). *Primitive elements and irreducible polynomials of GF (256)*. Cody Planteen.

Prévost, T., & Martin, B. (2025). A 10-bit S-box generated by Feistel construction from cellular automata. *arXiv preprint arXiv:2507.02489*.

Seitkulov, Y. N., Ospanov, R. M., & Yergaliyeva, B. B. (2021). On the cryptographic properties of S-boxes. *Engineering Journal of Satbayev University*, *143*(4), 96-103.

Webster, A. F., & Tavares, S. E. (1985). On the design of S-boxes. *Conference on the Theory and Application of Cryptographic Techniques* (pp. 523-534). Berlin, Heidelberg.

Zahid, A. H., Arshad, M. J., & Ahmad, M. (2019). A novel construction of efficient substitution-boxes using cubic fractional transformation. *Entropy*, *21*(3), 245.

## Author(s) Information

**Zhanat Saukhanova**
L.N. Gumilyov Eurasian National University
Pushkin street 11, Astana, Kazakhstan

**Gulmira Shakhmetova**
L.N. Gumilyov Eurasian National University
Pushkin street 11, Astana, Kazakhstan
Contact e-mail: *sh_mira2004@mail.ru*

**Altynbek Sharipbay**
L.N. Gumilyov Eurasian National University
Pushkin street 11, Astana, Kazakhstan

**Alibek Barlybayev**
L.N. Gumilyov Eurasian National University
Pushkin street 11, Astana, Kazakhstan

**Sayat Raykul**
L.N. Gumilyov Eurasian National University
Pushkin street 11, Astana, Kazakhstan

**Altay Khassenov**
L.N. Gumilyov Eurasian National University
Pushkin street 11, Astana, Kazakhstan

**To cite this article:**

Saukhanova, Z., Shakhmetova G., Sharipbay A., Barlybayev A., Raykul S., & Khassenov A. (2025). Design of S-boxes based on alternative irreducible polynomials. *The Eurasia Proceedings of Science, Technology, Engineering and Mathematics (EPSTEM), 36,* 102-109.