UDC 004

ALGORITHM FOR GENERATING S-BOX USING TRIGONOMETRIC FUNCTION

Abdurazzokov J.R. [1]

[1] Tashkent International University, Tashkent, Uzbekistan

javohirjon.1992@gmail.com

Abstract. Substitution boxes, commonly known as S-boxes, are one of the most important nonlinear components of modern symmetric-key block encryption algorithms. Their main task is to introduce confusion and nonlinear transformation into the encryption process so that the relationship between plaintext, ciphertext, and secret key becomes difficult to analyze. In Feistel networks and substitution–permutation networks, the S-box plays a central role in strengthening the resistance of a cipher against linear, differential, and algebraic cryptanalysis. This paper presents an algorithm for generating cryptographically strong 8×8 S-boxes using trigonometric transformation. The proposed approach is based on nonlinear numerical behavior produced by trigonometric functions and parameter-controlled transformations. By selecting different values of the control parameters, a large number of candidate S-boxes can be generated. These candidates are then evaluated according to standard cryptographic criteria, including nonlinearity, Strict Avalanche Criterion, Differential Probability, Linear Approximation Probability, and Fixed Point Analysis. The experimental results show that the generated S-box achieves a minimum nonlinearity of 100, a maximum nonlinearity of 112, and an average nonlinearity of 105.5. In addition, the proposed S-box obtains a SAC value of 0.4922, a DP value of 10/256, a LAP value of 0.1328, and zero fixed points. These results indicate that trigonometric transformations can be used as a promising mathematical tool for constructing substitution boxes for block cipher algorithms.

Keywords: block cipher, S-box, cryptography, nonlinear transformation, trigonometric function, nonlinearity, SAC, differential cryptanalysis, linear cryptanalysis.

1 INTRODUCTION

The development of modern information and communication technologies has significantly increased the need for reliable cryptographic protection mechanisms. Today, sensitive data is transmitted through open and heterogeneous networks in banking systems, e-government platforms, military communication, cloud computing, healthcare systems, and Internet of Things applications. In such environments, cryptographic algorithms are required to ensure confidentiality, integrity, and resistance against unauthorized analysis. Symmetric-key block ciphers remain one of the most widely used cryptographic mechanisms because of their efficiency, compactness, and applicability in both software and hardware environments [1, 2].

A symmetric-key block cipher transforms fixed-size plaintext blocks into ciphertext blocks using a secret key. Most modern block ciphers use a repeated round structure, where each round combines nonlinear substitution, linear diffusion, and key addition operations. In such constructions, the substitution box, or S-box, is usually the main nonlinear component. It is responsible for creating confusion in the sense of Shannon's cryptographic principles and helps reduce the statistical relationship between input and output data [1, 2].

An S-box is commonly represented as a mapping from an input vector space to an output vector space. In the case of an 8×8 S-box, the input and output are both 8-bit values. Therefore, the S-box can be interpreted as a permutation of integers from 0 to 255. If such a permutation is poorly designed, it may create exploitable weaknesses, including strong linear correlations, high-probability differential transitions, fixed points, and algebraic regularities. These weaknesses may be used by attackers to reduce the complexity of cryptanalysis [3, 12, 13].

The security of a cryptographic S-box is usually assessed using several mathematical and statistical criteria. Among the most important criteria are nonlinearity, differential probability, linear approximation probability, Strict Avalanche Criterion, and fixed point analysis. High nonlinearity is required to resist linear cryptanalysis, while low differential probability is necessary to resist differential cryptanalysis [12],

[13]. In addition, the Strict Avalanche Criterion measures whether a small change in the input causes a sufficiently large and unpredictable change in the output [12].

Traditional S-box construction methods are often based on algebraic structures, finite fields, Boolean functions, modular transformations, or manually designed permutations. For example, many well-known block ciphers use S-boxes constructed through carefully selected mathematical mappings. However, in recent years, the demand for dynamic, key-dependent, and algorithmically generated S-boxes has increased. This has motivated researchers to study alternative construction methods based on chaotic systems, genetic algorithms, reinforcement learning, neural networks, modular transformations, and trigonometric functions [4–11].

Among these methods, trigonometric transformation is an interesting direction because trigonometric functions naturally exhibit nonlinear, periodic, and parameter-sensitive behavior. These properties can be used to generate complex numerical sequences, which can then be converted into substitution tables. Zahid et al. proposed an efficient dynamic S-box generation method based on linear trigonometric transformation and demonstrated that such functions can be useful in cryptographic substitution design [8]. The present paper develops this idea and presents a trigonometric-transformation-based algorithm for generating 8×8 S-boxes.

The main purpose of this study is to construct an S-box generation algorithm that can produce bijective substitution tables with acceptable cryptographic characteristics. The proposed method randomly selects control parameters, generates candidate values using a trigonometric transformation, removes repeated values, forms a 256-element permutation, and evaluates the resulting S-box according to standard security criteria. If the generated S-box does not satisfy the required conditions, the algorithm repeats the generation process with new parameter values.

The remainder of the paper is organized as follows. Section II discusses related works and existing S-box construction methods. Section III explains the role of S-boxes in block cipher security. Section IV describes the use of trigonometric transformation in S-box generation. Section V presents the proposed algorithm. Section VI provides the mathematical evaluation criteria. Section VII discusses the experimental results. Section VIII analyzes the security implications of the obtained results. Finally, Section IX concludes the paper and outlines future research directions.

2 RELATED WORK

The construction of cryptographically strong S-boxes has been an active research problem for several decades. Since the introduction of classical block cipher structures, researchers have emphasized that the nonlinear layer is essential for resisting cryptanalytic attacks. Feistel, Notz, and Smith introduced important cryptographic techniques for machine-to-machine data communication, where substitution and permutation operations played an important role in secure transformation design [1]. Later, substitution–permutation networks became a fundamental model for constructing block ciphers with repeated nonlinear and linear layers [2].

Differential and linear cryptanalysis are among the most important attacks considered in S-box design. Differential cryptanalysis studies how input differences propagate through nonlinear components, while linear cryptanalysis searches for linear approximations between input, output, and key bits [12, 13]. Therefore, a secure S-box must be designed in such a way that no input difference produces an output difference with high probability and no linear approximation holds with significant bias.

Zhang and Pasalic proposed highly nonlinear balanced S-boxes with good differential properties, showing that nonlinearity and differential behavior should be considered jointly during S-box construction. Their work demonstrated that obtaining strong S-boxes requires a careful balance between algebraic, nonlinear, and differential characteristics [4].

Chaos-based methods have also been widely used for S-box design. Wang et al. proposed a method for designing S-boxes using chaotic maps and genetic algorithms, combining the unpredictability of chaotic systems with the search capability of evolutionary computation [5]. Later, Wang et al. introduced a genetic algorithm for constructing bijective substitution boxes with high nonlinearity, demonstrating that evolutionary algorithms can effectively search the large permutation space of 8×8 S-boxes [6].

Zhu et al. proposed an S-box generation method based on a combined chaotic system and advanced design strategy [7]. Their results showed that chaotic systems can generate candidate permutations with strong cryptographic properties when combined with suitable selection and optimization procedures [7]. Similarly, Jakimoski and Kocarev investigated the relationship between chaos and cryptography, including block encryption ciphers based on chaotic maps [11].

Artificial intelligence and machine learning techniques have also been explored for S-box generation. Kim et al. proposed a reinforcement learning approach for generating cryptographic S-boxes, showing that learning-based methods can search for useful transformation sequences in S-box construction [9]. Ahmad

and Malik proposed a chaotic neural-network-based method for designing cryptographic substitution boxes, demonstrating another direction where artificial intelligence and nonlinear dynamical systems can be applied to S-box design [10].

In addition to chaos and learning-based approaches, trigonometric functions have been used for dynamic S-box construction. Zahid et al. proposed an efficient dynamic S-box generation method using linear trigonometric transformation for security applications [8]. Their work showed that trigonometric functions may provide a flexible and efficient basis for generating nonlinear substitution boxes [8]. The present study follows this research direction and proposes a modified trigonometric-transformation-based algorithm for generating 8×8 S-boxes with measurable cryptographic properties.

3 ROLE OF S-BOXES IN BLOCK CIPHER SECURITY

An S-box is a nonlinear transformation that maps input bits to output bits. In an 8×8 S-box, the mapping can be represented as:

$$S : \mathbb{F}_2^8 \to \mathbb{F}_2^8.$$

Equivalently, it can be written as a permutation of the set:

$$\{0,1,2,\ldots,255\}.$$

For many block cipher designs, the S-box must be bijective. Bijectivity means that each input value has a unique output value and every output value appears exactly once. This property is important because it guarantees reversibility, which is required in decryption procedures of many symmetric-key block ciphers [2].

The S-box is primarily responsible for nonlinearity. If the S-box behaves like a linear or affine mapping, the entire cipher may become vulnerable to linear approximation attacks. Linear cryptanalysis attempts to approximate nonlinear transformations using linear expressions with probabilities different from one half. Therefore, an S-box must have high nonlinearity so that its output bits cannot be approximated by affine Boolean functions with high accuracy [13].

Another important property is resistance to differential cryptanalysis. Differential cryptanalysis examines how differences in input pairs influence differences in output pairs. If an S-box has certain input-output difference pairs with high probability, then an attacker may exploit these transitions to recover information about the secret key [12]. For this reason, an S-box should have low differential probability and good differential uniformity [4, 12].

The Strict Avalanche Criterion is also essential for S-box evaluation. According to this criterion, changing one input bit should change each output bit with probability close to 0.5. Webster and Tavares introduced this concept as an important design principle for cryptographic transformations [12]. If an S-box satisfies the avalanche property, then small input modifications produce large and unpredictable output changes.

Fixed points are another structural issue in S-box design. A fixed point occurs when S(x)=x. Such points are generally undesirable because they mean that some input values remain unchanged after substitution. In certain cipher structures, fixed points may create exploitable regularities. Therefore, a strong S-box should preferably have no fixed points or only a very small number of them.

Thus, the cryptographic quality of an S-box cannot be measured using only one criterion. A reliable S-box should simultaneously provide high nonlinearity, low differential probability, low linear approximation probability, good avalanche behavior, bijectivity, and minimal structural weaknesses [4, 6, 7, 12, 13].

4 TRIGONOMETRIC TRANSFORMATION FOR S-BOX GENERATION

Trigonometric functions are widely used in mathematics, physics, engineering, and signal processing because of their nonlinear and periodic properties. These functions can generate complex numerical patterns that are sensitive to parameter variations. In cryptography, such behavior is useful because parameter sensitivity and nonlinear output distribution may help construct unpredictable substitution mappings [8].

The proposed method uses a trigonometric transformation controlled by several parameters. These parameters influence the generated numerical sequence and allow the construction of many different candidate S-boxes. In general, the transformation may be represented as:

$$F(i) = G(A, B, C, x, y, i),$$

where i is the input index, and A, B, C, x, and y are control parameters. The function G includes trigonometric operations and produces numerical values that are later converted into integer values in the interval [0,255]. This idea is related to the trigonometric S-box generation approach proposed in [8].

The main advantage of this approach is the large solution space. By changing the parameters A, B, C, x, and y, many different numerical sequences can be produced. These sequences can then be processed to form candidate S-boxes. Since an 8×8 S-box must contain 256 distinct values, duplicate values must be removed during the construction process.

The use of trigonometric transformation provides several advantages. First, the transformation is nonlinear by nature. Second, it is sensitive to parameter changes. Third, it can generate a large number of candidate substitution tables. Fourth, it can be adapted for dynamic or key-dependent S-box generation. These properties make trigonometric transformations suitable for experimental cryptographic design [8].

However, trigonometric transformation alone does not guarantee cryptographic strength. A generated S-box must always be evaluated using formal criteria. Therefore, the proposed algorithm includes a testing phase in which nonlinearity, *SAC, DP, LAP*, and fixed point properties are computed. Only S-boxes satisfying the required conditions are accepted as valid outputs.

The proposed algorithm is designed to generate an 8×8 S-box using nonlinear trigonometric transformation. The algorithm is inspired by the dynamic S-box generation approach based on linear trigonometric transformation [8], but it introduces an additional value-combination and filtering procedure to obtain a complete 256-element bijective substitution table.

The generation process starts with random parameter selection. The values A, C, x, y_1, and y_2 are selected from predefined intervals. These parameters are then used in the trigonometric transformation function to generate two temporary values. The XOR operation is applied to these two values in order to obtain a new candidate value. The use of XOR helps combine two independently generated values and contributes to additional variation in the candidate sequence.

The generated value is then checked against the current output array d. If the value is already present in the array, it is rejected and the algorithm returns to the parameter selection step. If the value is not present, it is inserted into the array. This process continues until the array contains 256 unique elements. At that point, the array represents a bijective 8×8 S-box.

After constructing the candidate S-box, its nonlinearity is computed. If the nonlinearity does not satisfy the required threshold, the S-box is rejected and the generation process is restarted. If the nonlinearity is acceptable, the S-box is further evaluated according to SAC, DP, LAP, and fixed point analysis.

Table 1. The S-box generated using the proposed method

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

The proposed algorithm can be described as follows:

Step 1. Parameter selection - Randomly select the values of A, C, x, y_1, and y_2 from the predefined intervals;

Step 2. Trigonometric value generation - Use the selected parameters in the trigonometric transformation function to generate two temporary S-box values;

Step 3. XOR combination - Apply the XOR operation to the two generated values and obtain a new candidate value;

Step 4. Duplicate checking - Check whether the candidate value already exists in the array d. If it exists, return to Step 1. If it does not exist, add the value to the array;

Step 5. Completion of permutation - Repeat Steps 1-4 until the array ddd contains exactly 256 unique values;

Step 6. Nonlinearity testing - Compute the nonlinearity of the generated S-box. If the obtained value does not satisfy the cryptographic requirement, reject the candidate S-box and restart the generation process;

Step 7. Additional cryptographic evaluation - Evaluate the accepted S-box using SAC, DP, LAP, and fixed point analysis;

Step 8. Final output - If the S-box satisfies the required evaluation criteria, output it as the final substitution table.

This algorithm is suitable for generating both static and dynamic S-boxes. In static use, the algorithm is executed once and the resulting S-box is stored as a fixed substitution table. In dynamic use, the parameters may be derived from a secret key, round number, nonce, or initialization vector, allowing the S-box to change during encryption. The decimal values of the S-box generated using the proposed algorithm are presented in Table 1.

5 EXPERIMENTAL RESULTS AND DISCUSSION

The proposed trigonometric-transformation-based algorithm was implemented and tested for the generation of an 8×8 S-box. The obtained S-box was evaluated using nonlinearity, SAC, DP, LAP, and fixed point analysis. The results were also compared with several previously published S-boxes [6, 7], [10, 11]. The nonlinearity values of the eight coordinate Boolean functions of the proposed S-box are shown in Table 2.

Table 2. Nonlinearity values of the proposed S-box

Boolean function	1	2	3	4	5	6	7	8
Nonlinearity	106	104	104	104	100	110	104	112

As shown in Table I, the proposed S-box achieves a maximum nonlinearity of 112 and an average nonlinearity of 105.5. These values demonstrate that the generated S-box has a nonlinear structure and can reduce the effectiveness of linear approximation attacks [13]. Table 3 compares the nonlinearity values of the proposed S-box with several existing S-boxes reported in previous studies [6, 7, 10, 11].

Table 3. Comparison of nonlinearity scores of several 8×8 S-boxes

S-box	f1	f2	f3	f4	f5	f6	f7	f8
Proposed	106	104	104	104	100	110	104	112
In [6]	108	108	108	108	108	108	108	108
In [7]	108	108	106	102	108	102	108	104
In [10]	108	106	108	106	104	106	104	106
In [11]	98	100	100	104	104	106	106	108

The comparison shows that the proposed S-box has competitive nonlinearity values. Although some existing S-boxes, especially the S-box reported in [6], have more uniform nonlinearity, the proposed S-box reaches a maximum value of 112, which is an important positive result. Table 4 presents the minimum, maximum, and average nonlinearity values.

Table 4. Comparison of minimum, maximum, and mean nonlinearity

S-box	Minimum	Maximum	Mean
Proposed	100	112	105.5
In [6]	108	108	108
In [7]	102	108	105
In [10]	104	108	106
In [11]	98	108	103

From Table 4, it can be observed that the proposed S-box has a better maximum nonlinearity value than the compared S-boxes. However, its minimum value is lower than that of some optimized constructions. This means that future improvement should focus on increasing the minimum coordinate-function nonlinearity. The comparison of SAC, DP, LAP, and FPA values is presented in Table 5.

The SAC value of the proposed S-box is 0.4922, which is close to the ideal value of 0.5 [12]. This indicates that the proposed S-box provides good avalanche behavior. The DP value is 10/256, which is comparable with the results reported in [6, 7], and [10]. The LAP value is 0.1328, which is close to the

result in [10], but higher than the value reported in [7]. The fixed point value is zero, which means that the proposed S-box does not contain fixed points.

Table 5. Comparison of SAC, DP, LAP, and FPA values

S-box	SAC	DP	LAP	FPA
Proposed	0.4922	10/256	0.1328	0
In [6]	0.5781	10/256	0.1416	1
In [7]	0.5019	10/256	0.0629	0
In [10]	0.4987	10/256	0.1316	0
In [11]	0.4972	12/256	0.1181	0

The experimental results show that the proposed trigonometric-transformation-based algorithm can generate S-boxes with acceptable cryptographic properties. The obtained S-box has good avalanche behavior, no fixed points, and a competitive average nonlinearity value. These properties are important for resisting linear and differential cryptanalysis [12, 13].

The maximum nonlinearity value of 112 is a strong result for one of the coordinate Boolean functions. However, the minimum nonlinearity value of 100 indicates that the S-box is not fully optimized. In cryptographic design, the weakest coordinate function may influence the overall security of the S-box. Therefore, increasing the minimum nonlinearity should be one of the main goals of future research.

The DP value of 10/256 shows moderate resistance against differential cryptanalysis. Although this value is comparable with several existing S-boxes in the comparison table [6, 7, 10], it is still higher than the best-known highly optimized 8×8 S-boxes. Therefore, the trigonometric generation method may be combined with optimization algorithms such as genetic algorithms, hill climbing, simulated annealing, or reinforcement learning to reduce the differential probability [6, 9].

The LAP value of 0.1328 also suggests that the proposed method can be improved further. Since linear approximation probability is directly related to linear cryptanalysis, reducing the maximum linear bias is important for strengthening the proposed S-box [13]. A possible improvement is to apply affine transformations or local permutation modifications after the initial trigonometric construction.

One important advantage of the proposed algorithm is its flexibility. The parameter-controlled nature of the trigonometric function allows the generation of many different S-box candidates. This makes the method suitable for dynamic or key-dependent S-box construction. Dynamic S-boxes may be useful in block ciphers where the substitution layer changes according to secret key material or round-dependent parameters [8].

Another advantage is that the algorithm is relatively simple to implement. It does not require complex finite-field arithmetic or sophisticated algebraic structures. Instead, it relies on parameter selection, trigonometric computation, XOR combination, duplicate elimination, and cryptographic filtering. This simplicity makes the method suitable for experimental cryptographic research and educational purposes.

Nevertheless, the method has some limitations. First, because the algorithm depends on random parameter selection, it may require many iterations to obtain a strong S-box. Second, the current analysis considers only several basic cryptographic criteria. Additional metrics such as algebraic degree, algebraic immunity, transparency order, boomerang uniformity, and autocorrelation should be included in future studies. Third, the generated S-box should be tested inside a complete block cipher structure to determine its practical influence on encryption security.

The proposed trigonometric-transformation-based method has several advantages. First, it provides a large solution space because the control parameters can be varied over wide intervals. This increases the number of possible candidate S-boxes and allows the selection of strong variants through repeated testing [8].

Second, the method is nonlinear by construction. Since trigonometric functions naturally produce nonlinear numerical behavior, they can be used to generate complex substitution patterns. This property is important for reducing linear dependencies between input and output bits [13].

Third, the proposed method is suitable for dynamic S-box generation. If the parameters are derived from a secret key, initialization vector, nonce, or round number, the S-box can be changed dynamically during encryption. Such an approach may increase uncertainty for an attacker and make cryptanalysis more difficult [8].

Fourth, the algorithm can be combined with other optimization techniques. For example, genetic algorithms have been successfully applied to construct bijective S-boxes with high nonlinearity [6]. Reinforcement learning has also been used to generate cryptographic S-boxes [9]. Therefore, the proposed trigonometric method can serve as an initial generation mechanism, while optimization algorithms can be used to improve the generated candidates.

At the same time, several limitations must be considered. The current S-box has a minimum nonlinearity of 100, which is lower than that of some optimized S-boxes [6, 10]. The DP value of 10/256

is acceptable but not optimal. The LAP value of 0.1328 also leaves room for improvement. Therefore, future work should focus on improving the weakest cryptographic indicators while preserving the favorable properties of the proposed method.

6 CONCLUSION

This paper presented an algorithm for generating cryptographically strong 8×8 S-boxes using trigonometric transformation. The proposed method uses parameter-controlled nonlinear trigonometric functions to generate candidate substitution values. The XOR operation is applied to combine generated values, and duplicate checking is used to form a complete 256-element bijective S-box.

The generated S-box was evaluated according to standard cryptographic criteria, including nonlinearity, Strict Avalanche Criterion, Differential Probability, Linear Approximation Probability, and Fixed Point Analysis. The obtained results show that the proposed S-box has a minimum nonlinearity of 100, a maximum nonlinearity of 112, and an average nonlinearity of 105.5. The SAC value is 0.4922, which is close to the ideal value of 0.5. The DP value is 10/256, the LAP value is 0.1328, and the number of fixed points is zero.

The results demonstrate that trigonometric transformation can be used as a promising mathematical basis for S-box construction. Although the proposed S-box does not outperform the strongest optimized S-boxes in all metrics, it provides acceptable cryptographic properties and offers a flexible framework for generating many candidate S-boxes.

Future research should focus on improving the minimum nonlinearity, reducing differential probability and linear approximation probability, and integrating the proposed method with optimization techniques such as genetic algorithms, reinforcement learning, or local search. In addition, the generated S-boxes should be tested inside complete block cipher structures to evaluate their practical cryptographic effectiveness.

REFERENCES

[1] *Feistel, H., Notz, W. A., & Smith, J. L.* (1975). Some cryptographic techniques for machine-to-machine data communications. Proceedings of the IEEE, 63(11), 1545–1554. https://doi.org/10.1109/PROC.1975.10005.

[2] *Biryukov, A.* (2005). Substitution–Permutation (SP) network. In H. C. A. van Tilborg (Ed.), Encyclopedia of Cryptography and Security. Springer.

[3] *Abdurakhimov, B., Boykuziev, I., Khudoykulov, Z., & Allanov, O.* (2021). Application of the algebraic cryptanalysis method to the Kuznyechik encryption algorithm. In Proceedings of the IEEE International Conference on Science and Communications Technologies: Applications, Trends and Opportunities (ICISCT) (pp. 1–4). IEEE.

[4] *Zhang, W., & Pasalic, E.* (2014). Highly nonlinear balanced S-boxes with good differential properties. IEEE Transactions on Information Theory, 60(12), 7970–7979.

[5] *Wang, Y., Wong, K. W., Li, C., & Li, Y.* (2012). A novel method to design S-box based on chaotic map and genetic algorithm. Physics Letters A, 376(6–7), 827–833. https://doi.org/10.1016/j.physleta.2012.01.009.

[6] *Wang, Y., Zhang, Z., Zhang, L. Y., Feng, J., Gao, J., & Lei, P.* (2020). A genetic algorithm for constructing bijective substitution boxes with high nonlinearity. Information Sciences, 523, 152–166. https://doi.org/10.1016/j.ins.2020.03.025.

[7] *Zhu, D., Tong, X., Zhang, M., & Wang, Z.* (2020). A new S-box generation method and advanced design based on combined chaotic system. Symmetry, 12(12), 2087. https://doi.org/10.3390/sym12122087.

[8] *Zahid, A.H., Arshad, M.J., Ahmad, M., Alkhayyat, A., Alzahrani, A., & Raza, M.A.* (2021). Efficient dynamic S-box generation using linear trigonometric transformation for security applications. IEEE Access, 9, 98460–98475. https://doi.org/10.1109/ACCESS.2021.3095618.

[9] *Kim, G., Kim, H., Heo, Y., Jeon, Y., & Kim, J.* (2021). Generating cryptographic S-boxes using reinforcement learning. IEEE Access, 9, 83092–83104. https://doi.org/10.1109/ACCESS.2021.3085861.

[10] *Ahmad, M., & Malik, M.* (2016). Design of chaotic neural network based method for cryptographic substitution box. In Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) (pp. 864–868). IEEE. https://doi.org/10.1109/ICEEOT.2016.7754809.

[11] *Jakimoski, G., & Kocarev, L.* (2001). Chaos and cryptography: Block encryption ciphers based on chaotic maps. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48(2), 163–169.
[12] Webster, A. F., & Tavares, S. E. (1986). On the design of S-boxes. In Advances in Cryptology - CRYPTO'85 (Lecture Notes in Computer Science, Vol. 218, pp. 523–534). Springer.
[13] *Matsui, M.* (1994). Linear cryptanalysis method for DES cipher. In T. Helleseth (Ed.), Advances in Cryptology - EUROCRYPT '93 (Lecture Notes in Computer Science, Vol. 765, pp. 386–397). Springer. https://doi.org/10.1007/3-540-48285-7_33.

Received: January 19,2026

Citation: *Abdurazzokov J.R.* 2026. Algorithm for generating S-box using trigonometric function. *International journal of theoretical and applied issues of digital technologies*. Volume 9, Issue 2, pp. 78- 85. https://doi.org/10.62132/ijdt.v9i2.378.

АЛГОРИТМ ГЕНЕРАЦИИ S-БЛОКА С ИСПОЛЬЗОВАНИЕМ ТРИГОНОМЕТРИЧЕСКОЙ ФУНКЦИИ

Абдураззоков Ж.Р.[1]

[1] Ташкентский международный университет, Ташкент, Узбекистан

Аннотация. S-блоки, также известные как таблицы подстановок, являются одними из наиболее важных нелинейных компонентов современных блочных алгоритмов шифрования с симметричным ключом. Их основная задача заключается во внесении свойства запутывания и нелинейного преобразования в процесс шифрования, благодаря чему взаимосвязь между открытым текстом, шифртекстом и секретным ключом становится трудно поддающейся криптоаналитическому исследованию. В сетях Фейстеля и подстановочно-перестановочных сетях S-блок выполняет ключевую роль в повышении устойчивости шифра к линейному, дифференциальному и алгебраическому криптоанализу. В данной статье рассматривается алгоритм генерации криптографически стойких 8×8 S-блоков с использованием тригонометрического преобразования. Предлагаемый подход основан на нелинейном численном поведении тригонометрических функций и параметрически управляемых преобразованиях. За счет выбора различных значений управляющих параметров возможно формирование большого числа кандидатных S-блоков. Полученные кандидаты затем оцениваются по стандартным криптографическим критериям, включая нелинейность, строгий лавинный критерий, дифференциальную вероятность, вероятность линейной аппроксимации и анализ фиксированных точек. Экспериментальные результаты показывают, что сгенерированный S-блок достигает минимальной нелинейности 100, максимальной нелинейности 112 и средней нелинейности 105,5. Кроме того, предложенный S-блок имеет значение SAC, равное 0,4922, значение DP, равное 10/256, значение LAP, равное 0,1328, а также не содержит фиксированных точек. Полученные результаты свидетельствуют о том, что тригонометрические преобразования могут рассматриваться как перспективный математический инструмент для построения таблиц подстановок, применяемых в блочных алгоритмах шифрования.

Ключевые слова: блочный шифр, S-блок, криптография, нелинейное преобразование, тригонометрическая функция, нелинейность, строгий лавинный критерий, дифференциальный криптоанализ, линейный криптоанализ.