Quasi-Randomized Algorithm for Nonlinear Substitution

ANATOLY BELETSKY*, ARSEN KOVALCHUK, DENYS NAVROTSKYI
Department of Electronics, Robotics, Monitoring & IoT Technologies,
Faculty of Aeronautics, Electronics, and Telecommunications,
National University "Kyiv Aviation Institute",
1, Avenue Lyubomir Guzar, Kyiv, 03058
UKRAINE

**Corresponding Author*

Abstract: - Classic cryptographic primitives of nonlinear cryptographic substitution perform a simple replacement of each character of the encrypted text with some character of the same alphabet, effectively implementing the transformation of a single-alphabet simple substitution cipher. As a result, the entropy of the text transformed by the nonlinear substitution operator is the same as the entropy of the original text. This paper examines one variant of constructing quasi-randomized nonlinear substitution algorithms using the so-called weak determinism scheme, which yields a significant increase in the entropy of the output text. We will refer to nonlinear substitution operators in which one or more transformation parameters are selected in a deterministic manner, but contain signs of almost random selection as quasi-randomized. With such transformations, the output text acquires properties that are pretty close to those of white noise.

Key-Words: - cryptographic transformations, criteria for cryptographic strength, symmetric block ciphers, cryptographic primitives, nonlinear cryptographic substitution, S-box, randomization, scatter diagrams.

Received: June 11, 2025. Revised: September 23, 2025. Accepted: December 27, 2025. Published: May 22, 2026.

1 Introduction

Modern cryptographic information protection algorithms are mathematical transformations of messages represented in computers as a specifically ordered set of binary numbers. Cryptographic transformations map "meaningful messages" (input or plaintext) to the domain of "meaningless messages" (output or ciphertext). From the perspective of signal theory, encrypting the original (redundant, compressible) text consists of "whitening" it. The process of message whitening involves transforming the encrypted text into an uncorrelated sequence of (0,1) elements of the ciphertext (practically incompressible), with the distribution density of the output alphabet elements as close to uniform as possible. For the purpose of whitening, messages are subjected to iterative multi-round transformations of the original text by a set of cryptographic primitives, as is done, for example, in symmetric block ciphers.

Currently, the established view is that cryptographically secure symmetric encryption algorithms should include at least one *nonlinear substitution primitive* (NSP), also known as a nonlinear substitution node or S-box. It is often the S-boxes that are the sole operators determining the resistance level of modern block ciphers (AES [1], Camellia [2], DES [3], etc.) to various cryptanalytic attacks, and primarily to linear [4], [5], [6] and differential attacks [7]. Indeed, if encryption is reduced to transforming the original text by an arbitrary number of linear operators only, then they can all be represented by a single equivalent linear transformation operator, which significantly simplifies the task of breaking the cipher, reducing its cryptographic strength.

Various optimality criteria for S-boxes are known. These include criteria such as nonlinearity and propagation [8], [9], the maximum of the autocorrelation spectrum [10], [11], correlation and algebraic immunity [12], [13], strict avalanche effect, balance and differential resistance [14], and others. It's worth noting, by the way, that the S-box of the AES cipher does not satisfy most of the optimality criteria listed above [15], [16], [17]. And yet, this doesn't raise any doubts about the cryptographic strength of both the S-box and the AES cipher as a whole.

Arbitrary nonlinear substitutions can be

represented in at least three different forms: algebraic normal form [18], over a Galois field [19], [20], and as substitution tables [21], [22]. Nonlinear substitution boxes in modern block ciphers are typically constructed based on this tabular representation. The justification for this approach to building an S-box lies not only in the simplicity of describing the transformation algorithm but also in the practically confirmed cryptographic strength of the tabular S-box [23] used, for example, in the most popular symmetric block cipher, AES.

The computer implementation of S-box assumes, first, that the substitution table contains $N = 2^m$ elements (m-bit numbers) taking decimal values in the range from 0 to N - 1. Specifically, for the AES cipher m = 8, i.e. a «byte-to-byte» substitution is performed. And secondly, the S-box performs a bijective mapping of the set N of input integers $x = \overline{0, N-1}$ to the set N of output integers $y = \overline{0, N-1}$. And, as a result, the tabular form of the S-transform does not lead to a change in the Shannon-Kolmogorov entropy [24], [25] of the output sequence H_{out} compared to the entropy of the input sequence H_{in} , i.e., the equality $H_{out} = H_{in}$ is satisfied.

2 Research problem

The main objective of this article is to develop methods for forming AES-like nonlinear substitution operators (table-based, 8x8 scheme) that, thru quasi-randomization, a type of dynamic (deterministic) chaos [26], [27], increase the entropy of the transformed message, i.e., ensure the inequality $H_{out} > H_{in}$. Chaos determinism guaranties the reversibility of the transformation, which is essential for information encryption algorithms, and its quasi-randomness enhances the system's cryptographic resistance to cracking.

We will classify as quasi-random operators those nonlinear substitution operators in which one or more transformation parameters, although chosen deterministically, exhibit signs of almost random selection. The proposed definition of a randomized operator is based on the definition of a randomized algorithm given in [28].

3 Preliminary remarks

One of the most important indicators of the quality of transformation $y = f(x)$ in S-boxes is the correlation dependence (correlation), which reflects the statistical relationship between the values x and y. It is generally accepted that the smaller this dependence, the better the bit, byte, or other component mixing properties the operator possesses for the input text. For a graphical representation of the correlation, it is convenient to use grids in a rectangular coordinate system with axles corresponding to both variables x and y. Each pair of variable values x, y is marked with a point. This type of graph is called a scatter plot or dot plot [29]. Figure 1 shows an example of the S-box scatter diagram for the Rijndael algorithm of the AES cipher.

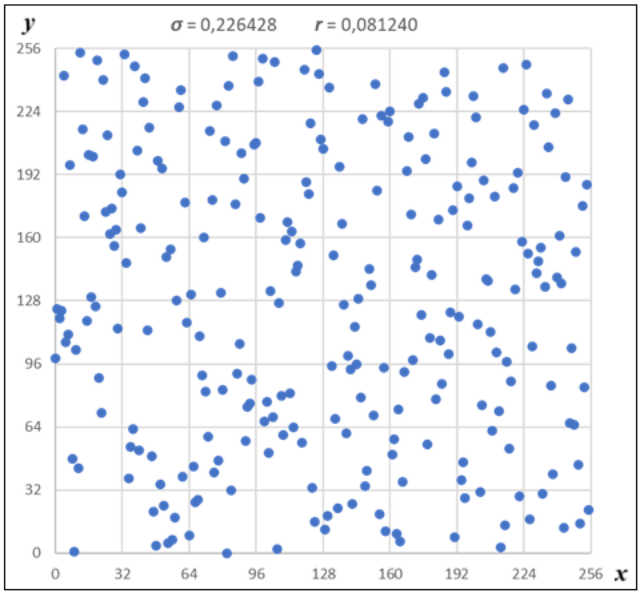

Fig. 1. Scatter diagram
Rijndael algorithm
Source: created by the authors

The mathematical measure of correlation between the values x and y in the NSP scatter diagram is the correlation coefficient r, determined by the ratio

$$r = \sum_{i=0}^{N-1} \dot{x}_i \cdot \dot{y}_i \Big/ \sqrt{\sum_{i=0}^{N-1} \dot{x}_i^2} \cdot \sqrt{\sum_{i=0}^{N-1} \dot{y}_i^2}\,, \qquad (1)$$

where $\dot{x}_i$ are centered and normalized variables x, whose average value for 8-bit substitutions ($N = 256$) is 127.5, i.e.

$$\dot{x}_i = (x_i - 127.5)/256, \quad i = \overline{0, 255}.$$

The variables $\dot{y}_i$ are calculated similarly.

Let's introduce an estimate of the quantitative measure of the density of the distribution of points (x, y) on the scatter plot. To this end, we will divide the diagram plane into 64 squares, as shown in Figure 1. Let's count the number $n_{i,j}$, ($i, j = \overline{0, 7}$) of points (x,

y) that fall into the (*i*, *j*)-th squares. If a point (*x*, *y*) is located on the bottom or left side of the square, we will consider it to belong to the square. A distribution of points within their existence area will be considered uniform if four points fall into each square of the scatter plot. As a mathematical measure of the uniformity of the scattering σ, we will take the normalized standard deviation of the values of the random variables $n_{i,j}$ relative to their mathematical expectation, which is equal to four, i.e.,

$$\sigma = \frac{1}{64}\sqrt{\sum_{i=0}^{7}\sum_{j=0}^{7}\left(n_{i,j}-4\right)^2}\,. \qquad (2)$$

Ideally, *r* and σ are equal to zero. For the Rijndael algorithm in the AES cipher, *r* = – 0.04381 and σ = 0.64044 (shown at the top of Figure 1).

The nonlinear substitution primitive of the Rijndael algorithm implements the following byte-to-byte transformation:

$$y = x_f^{-1}\cdot \boldsymbol{A} + \beta\,, \qquad (3)$$

where x_f^{-1} is the multiplicative inverse element of the field GF(2^8) over the irreducible polynomial $f = 100011011$ for a given element *x*; $\beta = 01100011$ is the additive component of the transformation, and A is a circulant matrix whose top row is the vector 10001111, and the subsequent rows (from top to bottom) are formed by cyclically shifting the previous rows one position to the right.

In a number of works, such as [30], doubt has been expressed as to whether the parameters *f*, ***A***, and β of the classical S-transform (3) are optimal, obtained as a result of careful and meticulous optimization. Confirmation of this assumption can be found in the fact that the diffusion properties of AES-like S-boxes, evaluated at least by the entropy of the ciphertexts they generate (or the correlation coefficient of the block's input/output variables), are not sensitive to the transformation parameters.

4 AES-like substitution primitives

The efficiency of nonlinear substitution primitives can be significantly increased by modifying transformation (3). Let's consider one possible substitution option.

$$y = (x+c)_f^{-1}\cdot \boldsymbol{G}_{\varphi,\theta}^{(8)} + \beta\,, \qquad (4)$$

where ***G*** is a generalized Galois matrix; *f* and φ are irreducible polynomials (IP) of degree eight; θ is a primitive element of the Galois field over IP φ; and c, β are the additive components of transformation (4). The order of the matrix, which is generally equal to n, will be denoted by a superscript on ***G***.

The terms *generalized Galois matrix* $\boldsymbol{G}_{\varphi,\theta}^{(n)}$, like the *Fibonacci matrix* $\boldsymbol{F}_{\varphi,\theta}^{(n)}$, are borrowed from cryptography theory and are not well-established in mathematics and technical applications [31]. Let's clarify these concepts by first presenting the previously known matrix, let's call it the classical ($\theta = 10$) Galois matrix, in this compact form:

$$\boldsymbol{G}_{\varphi,10}^{(n)} = \begin{pmatrix} \blacktriangleleft & f \\ \boldsymbol{E} & \boldsymbol{0} \end{pmatrix}, \qquad (5)$$

where ***E*** is the (*n* - 1)th-order identity matrix, **0** is the zero column-vector of dimension (*n* – 1), and ◀ is the index of the leading coefficient of the primitive generating polynomial f_n of degree *n*.

Fibonacci matrix $\boldsymbol{F}_{\varphi,10}^{(n)}$ and Galois matrix $\boldsymbol{G}_{\varphi,10}^{(n)}$ are related by the *right-sided transposition* operator (i.e., transposition relative to an auxiliary diagonal), denoted by $\perp$:

$$\boldsymbol{G}_{\varphi,10}^{(n)} = \begin{pmatrix} \blacktriangleleft & f \\ \boldsymbol{E} & \boldsymbol{0} \end{pmatrix} \longleftrightarrow \begin{pmatrix} \Theta & f \\ \boldsymbol{E} & \blacktriangledown \end{pmatrix} = \boldsymbol{F}_{\varphi,10}^{(n)}, \qquad (6)$$

where Θ is the zero vector-row of order $n-1$.

By left-transposing the matrices $\boldsymbol{G}_{\varphi,\theta}^{(n)}$ and $\boldsymbol{F}_{\varphi,10}^{(n)}$, we form another pair of matrices, which we will call the Galois and Fibonacci *conjugate matrices*. We will denote conjugate matrices with superscripts enclosed in square brackets, i.e., we will represent them as $\boldsymbol{G}_{\varphi,\theta}^{[n]}$ and $\boldsymbol{F}_{\varphi,\theta}^{[n]}$. Compact notation and the relationship of the introduced subset of matrices are shown in Figure 2.

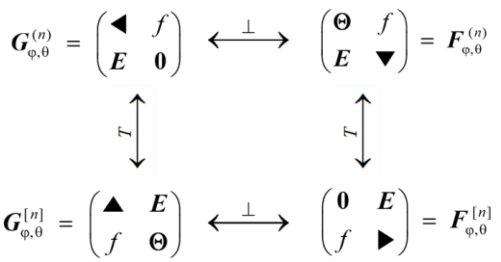

Fig. 2. Diagram of the relationship between Galois-Fibonacci matrices
Source: created by the authors

The synthesis of *generalized Galois matrices* (GGM) in image space format, where the matrix elements take values of 0 or 1, is performed according to the following empirically developed sequence of transformations.

GGM synthesis algorithm. Let a primitive element $\theta \geq 10$ of the Galois field over an irreducible

(not necessarily primitive) generating polynomial φ_n of degree *n* be chosen. We will place the element (let's call it the generating element of the GGM) in the rightmost digits of the bottom row of the matrix $\boldsymbol{G}_{\varphi,\theta}^{(n)}$ being formed. The remaining digits of the row are filled with zeros. Subsequent rows of the matrix (from bottom to top) are formed by shifting the previous row one digit to the left. In this case, a zero is written in the rightmost digit of the row that is freed up. If, at some iteration step, the senior unit of the row goes beyond the matrix boundary, then this (*n* +1)-bit row is reduced to the remainder modulo the irreducible polynomial φ_n, bringing it back within the matrix. Затем процесс продолжается в соответствии с описанной схемой, пока не будут заполнены все *n* строк матрицы. We arrive at the classical Galois-Fibonacci matrices (which we will also refer to as simple matrices) by setting the generator element in the GGM synthesis algorithm to $\theta = 10$, as indicated in (5) and (6). Such a value for the generator element θ in the formation of simple Galois-Fibonacci matrices belongs exclusively to extended Galois fields generated by primitive polynomials φ_n.

Transformation (4) can be given the property of quasi-randomization (*weak determinism*), by assuming that within the encrypted block, the displacement c_k of the *k*-th eight-bit element x_k changes according to the following rule

$$c_k = k \cdot h, \quad k = \overline{0, L-1}, \quad L = N/8, \qquad (7)$$

where h is the step for the block element offset; N is the block size (in bits).

Given (7), we can express the *j*-th byte y_k in (4) as

$$y_k = (x_k + k \cdot h)_f^{-1} \cdot \boldsymbol{G}_{\varphi,\theta}^{(8)} + \beta. \qquad (8)$$

Transformation (3) performs a simple substitution, for example, replacing the symbol 'a' from the original alphabet with another symbol 'b' from the same alphabet, while the frequency p_b of symbol 'b' remains equal to the frequency p_a of symbol 'a'. And for this reason, as we noted above, the classical S-transform (3) preserves the entropy of the input text. The picture changes significantly when the S-transformation is performed according to the weak determinacy scheme (8). Indeed, let $x_k = x$ there be some input byte, which corresponds to the offset $c_k = k \cdot h$. The byte $y_k = S(x + k \cdot h)$ is retrieved from the S-box table at the address $x + c_k$. Let's assume further that this or any other block of text to be converted also contains byte *x*, but the index *l* of byte is different from index *k*. In this case, the byte $y_l = S(x + l \cdot h)$ that does not match byte y_k is now retrieved from the S-box table at the address $x + c_l$. The consequence of such a transformation is an increase in the number of different symbols in the ciphertext compared to the number of symbols in the original text, which leads to an increase in the entropy of the transformed file, i.e., $H_{out} = H_{in}$.

The dynamics of the entropy change of the output text for three sizes of S-transformed blocks, depending on the shift step h, is shown in Table 1. A 12.5 MB fragment of the Dal dictionary [32] was used as the input file.

Table 1. Entropy of the text file
Source: created by the authors

h	S-box size (in bits)		
	128	192	25
0	4.707303	4.707303	4.707303
1	5.931931	6.741472	6.864060
2	6.612635	7.013791	7.332091
3	6.943560	7.342474	7.485984
4	7.186072	7.383172	7.556215
5	7.191	7.486439	7.640091
6	7.189903	7.481469	7.687300
7	7.25899	7.585280	7.745281
8	7.393023	7.612759	
9	7.354705	7.679003	
10	7.406647	7.653457	
11	7.385504	7.680380	
12	7.485629		
13	7.409907		
14	7.539308		
15	7.502134		

Generalized Galois matrices, when included in the PRS formation loop, provide the best values for the scattering diagram parameters σ and *r*, compared to the scattering parameters provided by the Rijndael algorithm's S-box.

As can be seen from the comparison of the data presented in Fig. 1, the mean square deviation (σ) and the correlation coefficient (r) of the input-output parameters (*x*, *y*) of the scatter diagrams of the S-box of the Rijndael algorithm are worse than the corresponding parameters of the NSP blocks based on GGM. Note, moreover, that the entropy (H) of the converted text file is invariant to the types of GGM used in quasi-randomized NSPs.

5 Results, Discussion, and Future

The main results of this work are as follows:

- Variants for constructing nonlinear substitution primitives based on so-called generalized Galois and Fibonacci matrices have been developed, thru which the same binary pseudorandom sequence (PRSs) can be calculated in software as those generated by corresponding hardware LFSR generators.
- It is shown that generalized matrices are synthesized not only based on primitive polynomials (the only possible polynomials used in the synthesis of classical Galois-Fibonacci matrices), but also based on polynomials that are not necessarily primitive at all. However, the condition must be met that the generating element of the generalized matrices can only be a primitive element of the Galois field over the irreducible polynomial that generates this field.
- The subset of both classical and generalized Galois-Fibonacci matrices, interconnected by the right-sided transpose operator, is augmented by so-called conjugate matrices, interconnected with the original matrices by the classical (left-sided) transpose operator.

Generalized Galois matrices of order *n* can serve as generators of PRSs of length $L = 2^n - 1$, whereby the sequences satisfy all three of Golomb's postulates. For this reason, it may seem that generalized Galois generators of PRSs do not introduce any new properties into sequences formed by classical generators, and since the latter are easier to implement in hardware and software, the use of generalized generators, for example in cryptographic applications, may not be practical. But that's not quite right. As established in [33], PRS generators built on generalized Galois matrices are immune to the Berlekamp-Massey (BM) attack. The noted feature of generalized generators arises for the following reason. For classical generators with a single feedback loop, the BM tester successfully solves the problem of determining only one unknown – the primitive polynomial f_n. When breaking generalized generators, in addition to f_n, the primitive generating element θ of the Galois matrix also turns out to be unknown. However, the classic BM algorithm is not designed to calculate two unknown parameters and therefore becomes unsuitable when organizing an attack on generalized generators. That's the first thing. And secondly, in any case, the processor implementing the BM algorithm always outputs the value of the primitive polynomial (PP) as a solution, while a generalized Galois LFSR can be constructed based on a polynomial that is not necessarily primitive.

As a promising direction for further research, we can suggest solving the well-known problem of constructing 16-bit S-boxes, supplemented by a quasi-randomization procedure for two-byte words based on a scheme of weak determinism, similar to transformation (8).

6 Conclusion

The development of nonlinear substitution primitives is one of the key tasks of modern symmetric cryptography. The proposed method for constructing quasi-random algorithms significantly increases the entropy of the transformed data, which, to a certain extent, is precisely what is responsible for ensuring the high cryptographic strength of symmetric ciphers.

Due to its structural flexibility, quasi-randomness, higher entropy, and better values of the parameters σ and r, the GGM-based NSP outperforms the classical S-box AES in a number of optimality criteria, including differential and linear robustness, avalanche effect, balance, etc.

Declaration of Generative AI and AI-assisted Technologies in the Writing Process

During the preparation of this work, the authors used Quillbot to check grammar. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

References:

[1] Daemen, J., Rijmen, V. The Design of Rijndael: The Advanced Encryption Standard (AES). *Springer-Verlag*, *Berlin*, 2002. **DOI:** 10.1007/978-3-662-04722-4

[2] Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T. Camellia: A 128-bit block cipher suitable for multiple platforms. [Online]. Available: https://info.isl.ntt.co.jp/crypt/camellia/dl/reference/sac_camellia.pdf (Accessed: Jan. 29, 2026).

[3] Coppersmith, D. The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, 1994, 38(3), pp. 243–250. **DOI:** 10.1147/rd.383.0243

[4] Biryukov, A., Shamir, A. Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers. *ASIACRYPT 2000.*, pp. 1–13. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-44448-3_1 (Accessed: Jan. 29, 2026).

[5] Lambin, A. Optimization of core components of block ciphers. *Cryptography and Security* [cs.CR]. Université de Rennes, 2019, pp. 145.

[6] Standaert, F.-X., Piret, G., Quisquater, J.-J., Cryptanalysis of Block Ciphers: A Survey. *UCL Crypto Group. Universite Catholique de Louvain, Belgium,* Technical Report CG–2003/2, pp.1-23.

[7] Dinur, I. Improved Differential Cryptanalysis of Round-Reduced peck. *Cryptology ePrint Archive*. Paper 2014/320, pp. 20. [Online]. Available: https://eprint.iacr.org/2014/320.pdf (Accessed: Jan. 29, 2026).

[8] Carlet C. A Wide Class of Boolean Functions Generalizing the Hidden Weight Bit Function. IEEE Trans. Inf. Theory 68(2): 1355-1368 (2022).

[9] Wu, B., Jin, Q., Liu, Z., Lin, D. Constructing Boolean Functions With Potential Optimal Algebraic Immunity Based on Additive Decompositions of Finite Fields. *arXiv:1401.6604v1 (cs)*, 2014, pp. 11. [Online]. Available: https://arxiv.org/pdf/1401.6604 (Accessed: Jan. 29, 2026).

[10] Carlet C. Boolean Functions for Cryptography and Error Correcting Codes. *LAGA, University of Paris*, 2007, pp. 186.

[11] Dupin A., Méaux P, Rossi M. On the Algebraic Immunity - Resiliency trade-off, implications for Goldreich's Pseudorandom Generator. *Cryptology ePr. Archive,* Paper 2021/649, pp. 51. [Online]. Available: https://eprint.iacr.org/2021/649 (Accessed: Jan. 29, 2026).

[12] Tang X., Tang D., Zeng X. and Hu L. Balanced Boolean Functions with (Almost) Optimal Algebraic Immunity and Very High Nonlinearity. *Cryptology ePr. Archive,* Paper 2010/443, pp. 24. [Online]. Available: https://eprint.iacr.org/2010/443.pdf (Accessed: Jan. 29, 2026). (Accessed: Jan. 29, 2026).

[13] Bogdanov A. Analysis and Design of Block Cipher Constructions. *Ruhr-Universitat Bochum,* 2009, pp. 213.

[14] Dey S. and Ghosh R. A review of cryptographic properties of S-boxes with Generation and Analysis of crypto secure S-boxes. *Cryptology ePrint Archive*, 2018, pp. 45. [Online]. Available: https://eprint.iacr.org/2018/405.pdf (Accessed: Jan. 29, 2026).

[15] Carlet, C. A method of construction of balanced functions with optimum algebraic immunity. *Cryptology ePrint Archive*, Paper 2006/149, 2005, pp. 18. [Online]. Available: https://eprint.iacr.org/2006/149.pdf (Accessed: Jan. 29, 2026).

[16] Lerman L., Markowitch O. and Veshchikov N. Comparing Sboxes of Ciphers from the *Cryptology ePrint Archive*, 2016, pp. 6. [Online]. Available: https://eprint.iacr.org/2016/993.pdf (Accessed: Jan. 29, 2026).

[17] Tokareva N. Algebraic normal form of a bent function: properties and restrictions. *Cryptology ePrint Archive*, 2018, pp. 17. [Online]. Available: https://eprint.iacr.org/2018/1160.pdf (Accessed: Jan. 29, 2026).

[18] Gomez G. S., Osuna O. P. A family of Boolean functions with good cryptographic properties. *Cryptology ePrint Archive*, 2019, pp. 9. [Online]. Available: https://eprint.iacr.org/2019/217.pdf (Accessed: Jan. 29, 2026).

[19] Bonnetain X., Perrin L. and Shizhu Tian. Anomalies and Vector Space Search: Tools for S-Box Analysis. *Cryptology ePrint Archive*, 2019, pp. 28. [Online]. Available: https://inria.hal.science/hal-02396738/file/paper.pdf (Accessed: Jan. 29, 2026).

[20] Kim H., Jeon Y., Kim G., Kim J., Sim B, Han D., Seo H., Kim S., Hong S., Sung J. and Hong D. A New Method for Designing Lightweight S-Boxes with High Differential and Linear Branch Numbers, and its Application. *Cryptology ePrint Archive*, Paper 2020/1582, pp. 62. [Online]. Available: https://eprint.iacr.org/2020/1582 (Accessed: Jan. 29, 2026).

[21] Clark J. A., Jacob J. L., Stepney S. The Design of S-Boxes by Simulated Annealing. *Cryptology ePrint Archive*, 2005, pp. 7. [Online]. Available: https://www-users.york.ac.uk/~ss44/bib/ss/nonstd/cec04a.pdf (Accessed: Jan. 29, 2026).

[22] Edmunds, D. E., Triebel, H. Recent advances in entropy numbers and ε-entropy: Applications to functional analysis and learning theory. *Entropy*, 24(3), 2022, pp. 407. **DOI:** 10.3390/e24030407

[23] Dicesar Lass Fernandez, Eduardo Brandani da Silva. Entropy numbers of bilinear operators. *Journal of Mathematical Analysis and Applications*, Vol. 497, Issue 1, 2021, pp. 1-23. **DOI:** 10.1016/j.jmaa.2020.124899

[24] Lawnik M., Moysis L., Volos C. Chaos-Based Cryptography: Text Encryption Using Image Algorithms. *Electronics*, 2022, 11(19), 3156 **DOI:** 10.3390/electronics11193156

[25] Jiang M., Yang H. Image Encryption Using a New Hybrid Chaotic Map and Spiral Transformation. *Entropy*. 2023, 25(11), 1516; **DOI:** 10.3390/e25111516

[26] Cormen, T. H., Leiserson, C. E., Rivest, R. L., Stein, C. Introduction to Algorithms (2rd ed.), *MIT Press*, Cambridge, Massachusetts, 2001, pp. 984.

[27] Engloner A. I, Podani J. A new statistical method for the comparison of biplots with the same objects and variables. *Ecological Indicators*, Volume 154, 2023 **DOI:** 10.1016/j.ecolind.2023.110802

[28] Martinez-Diaz I., Legon-Perez C.M., Sosa-Gomez G. Generation of Affine-Shifted S-Boxes with Constant Confusion Coefficient Variance and Application in the Partitioning of the S-Box Space. *Cryptography*, 2025, Vol. 9(2): 45.

[29] Beletsky A. Generalized Galois-Fibonacci Matrix Generators Pseudo-Random Sequences. *WSEAS Int. J. Computer Network and Information Security*, 6, 2021, pp. 57-69. **DOI:** 10.5815/ijcnis.2021.06.05

[30] Beletsky A. Generalized Galois and Fibonacci Matrices in Cryptographic Generalized Galois and Fibonacci Matrices in Cryptographic Applications. *WSEAS Transactions on Circuits and Systems*, 21, 2022, pp. 1-19. **DOI:** 10.37394/23201.2022.21.1

[31] Beletsky, A. Y. Synthesis of Cryptoresistant Generators of Pseudo-random Numbers Based on Generalized Galois and Fibonacci Matrixes. *Radio Electronics, Computer Science, Control*, (3), 2019, pp. 86–98. **DOI:** 10.15588/1607-3274-2019-3-10

[32] Dal, V. I. (1903–1909). Tolkovyi slovar' zhivogo velikorusskogo yazyka [Explanatory Dictionary of the Living Great Russian Language] (3rd edition by I. A. Baudouin de Courtenay). *Saint Petersburg & Moscow: M. O. Wolf*. [Online]. Available: https:// www.prlib.ru/en/node/457656 (Accessed: Jan. 29, 2026).

[33] Schneier, B.: Applied cryptography, Second Edition: Protocols, Algorithms, and Source Code in C. *John Wiley*; *Sons*, *New York*, 1996, pp. 792. **ISBN**-13: 978-0471117094

Contribution of Individual Authors to the Creation of a Scientific Article

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.