Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4547–4556
DOI : 10.47974/JDMSC-3072

Algebraic construction and security evaluation of substitution boxes using finite field and permutation group techniques

M. Manideepika [†]
Department of CSE (Artificial Intelligence & Machine Learning)
Pragati Engineering College
Surampalem
Kakinada District 533437
Andhra Pradesh
India

Dinesh Baban Kute *
Department of Applied Sciences and Humanities
Pimpri Chinchwad College of Engineering
Pune 411044
Maharashtra
India

Amruta Tejaskumar Mokashi [§]
Department of Chemical Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Padmavati Shrivastava [‡]
Department of Computer Science and Engineering
Rungta College of Engineering and Technology
Rungta International Skills University
Bhilai 490024
Chhattisgarh
India

* *ORCID-ID:* 0000-0002-7285-0165

[†] *E-mail:* manideepika@outlook.com
* *E-mail:* dineshkute90@gmail.com (Corresponding Author)
[§] *E-mail:* amruta.mokashi2@vit.edu
[‡] *E-mail:* dr.padmavati.shrivastava@rungta.org

© Taru Publications

Dipak Sethi [@]
School of Nursing
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Pooja Pathak [#]
Department of Computer Engineering & Applications
GLA University
Mathura 281406
Uttar Pradesh
India

Abstract

S-boxes (substitution boxes) are essential nonlinear elements that guarantee confusion in symmetric cryptosystems, but it is still difficult to come up with structures that have a good algebraic and cryptographic structure. This paper is an attempt to suggest a hybrid construction approach characterized by a combination of finite field GF(2n) transformations and permutation group techniques to create secure and efficient S-boxes. The method is a combination of algebraic inversion, affine mapping and permutation cycles to maximize nonlinearity, objectivity and resistance to differential and linear cryptanalysis. The proposed construction of hybrid S-box uses finite-field inversion, affine transformations and permutation-group operations to enhance the cryptographic substitution properties. The results reported here show a nonlinearity of 114, while AES S-box and traditional S-box have values of 112 and 96, respectively, which represent 1.79% and 18.75% improvement, respectively. The proposed construction meets the AES baseline by +1.4 and +2.4 percentage points on both the Strict Avalanche Criterion (SAC) and Bit Independence Criterion (BIC) respectively. The reported computational time is 11.1 ms which is 11.90% faster than traditional S-box but 7.77% slower than AES. These comparisons suggest that these characteristics are reported to be better with little to be gained in terms of computation.

Subject Classification: *11T71, 68W30.*

Keywords: *S-box design, Finite fields, Permutation groups, Nonlinearity, Differential uniformity.*

I. Introduction

The main source of nonlinearity in contemporary symmetric cryptographic algorithms are substitution boxes (S-boxes) that are essential in providing the desired confusion and resistance to statistical and structural attacks [1, 2]. The design and strength of S-box components of

[@] *E-mail:* **dir.son@niu.edu.in**
[#] *E-mail:* **pooja.pathak@gla.ac.in**

block ciphers like the Advanced Encryption Standard highly determine their security [3, 4]. The classical S-box construction techniques are typically based on algebraic inversion in finite fields with affine transformations; but are not necessarily very flexible or resistant to new cryptanalytic methods [5, 6, 7]. Recent developments in cryptography have highlighted the necessity of new methodologies of construction that can improve the cryptographic strength and at the same time preserve computational efficiency [8, 9]. Finite field theory, especially constructions in $GF(2^n)$, in this regard offers a powerful mathematical basis to construct objective and highly nonlinear mappings [10, 11]. At the same time, permutation group theory provides a companion theory to add complexity to diffusion and linear and differential cryptanalysis resistance by introducing the use of organized reshuffling of the elements [12], [13].

II. Mathematical Preliminaries

Mathematical preliminaries include the finite fields $GF(2^n)$, Boolean functions, mappings, and properties of algebra needed to construct nonlinear and bijective substitution boxes efficiently, and cryptographically secure. Figure 1 demonstrates GF(2 3) operations that make it possible to perform safe algebraic transformations.

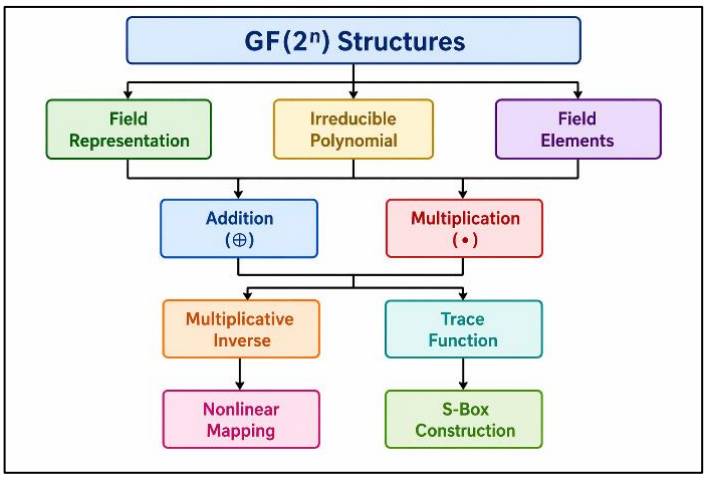


Figure 1
Fundamental Structure of GF(2^n) Finite Field Operations

A. *Fundamentals of Finite Field Theory and GF(2^n) structures*

Algebraic structures in finite fields GF(2n) offer invertible mappings, representations of polynomials and arithmetic operations necessary to efficiently implement nonlinear, bijective substitution boxes.

$$p(x) = x^n + \Sigma^{i}_{\{i=0\}^{\{n-1\}}_{i}} p_i x, p_i \in GF(2), \gcd\big(a(x), p(x)\big) = 1 \qquad (1)$$

The irreducible poly constraint in (Eq. 1) is to make sure that p(x) is a valid field extension of GF(2), so there is closure, associativity and inverses; and gcd(a(x),p(x))=1 is to make sure that p(x) is invertible.

$$a(x) \oplus b(x) = \Sigma_{\{i=0\}}^{\{n-1\}}(a_i \oplus b_i)x^i = \Sigma_{\{i=0\}}^{\{n-1\}}(a_i + b_i mod\ 2)x^i \quad (2)$$

The addition in the field (Eq. 2) is a bitwise XOR, thus maintaining linearity and simplicity, which is crucial to efficient hardware and software implementation.

$$a(x) \cdot b(x) = \left(\Sigma_{\{i=0\}}^{\{n-1\}} \Sigma_{\{j=0\}_i^{\{n-1\}a}}^{\{i+j\}} b_j x \right) mod\ p(x) \quad (3)$$

Multiplication with reduction in (Eq. 3) is used to do a polynomial convolution and then a modular reduction with p(x), so that the result is not too large to fit in GF(2 n).

$$a^{\{-1\}(x)} = a(x)^{\{2^n - 2\}} = \Pi_{\{k=1\}}^{\{n-1\}} a(x)^{\{2^k\}} \quad (4)$$

The base of the multiplicative inverse in (Eq. 4) is calculated with exponentiation under the Fermat theorem which offers nonlinearity which is essential in cryptographic strength.

$$Tr\big(a(x)\big) = \Sigma_{\{k=0\}}^{\{n-1\}} a(x)^{\{2^k\}}, f(x) = Tr\big(a(x) \cdot x^{\{-1\}}\big) \quad (5)$$

Lastly, the trace in (Eq. 5) sums Frobenius mappings to create very nonlinear transformations, which are popular in S-box design to make them more resistant to linear and differential cryptanalysis.

B. *Boolean functions and vectorial Boolean mappings*

Input-output transformations are characterized by Boolean functions and vectorial mappings, aspects that quantify nonlinearity, algebraic degree, and immunity to correlation, which are important to assess cryptographic strength and resistance to attacks.

$$f: GF(2)^n \rightarrow GF(2), f(x) = \Sigma_{\{u \in GF(2)^n\}} c_u \Pi_{\{i=1\}}^{\{n\}} x_i^{\{u_i\}} \quad (6)$$

The definition of the Boolean functions in (Eq. 6) is a mapping of GF(2)nGF(2)n to GF(2)GF(2)GF(2) in algebraic normal form with coefficients that specify the functional structure and logical behavior.

$$F: GF(2)^n \rightarrow GF(2)^m, F(x) = \big(f_{1(x)}, f_{2(x)}, \dots, f_{m(x)}\big) \quad (7)$$

This generalization to multi-output functions is done in the form of the vectorial Boolean mapping in (Eq. 7) which can be used to compose S-boxes by joining together several Boolean components into one transformation.

$$W_{f(\omega)} = \Sigma_{\{x \in GF(2)^n\}}^{\{f(x) \oplus (\omega \cdot x)\}} (-1) \quad (8)$$

In (Eq. 8) the Walsh-hadamard transform measures correlation of the Boolean function with the linear functions, which is a fundamental instrument to study resistance to linear cryptanalysis.

$$NL(f) = 2^{\{n-1\}} - \left(\frac{1}{2}\right) \max_{\{\omega \in GF(2)^n\}} \left|W_{f(\omega)}\right| \quad (9)$$

The nonlinearity measure in (Eq. 9) is a measure of the closest distance to all affine functions with larger values corresponding to a greater resistance to linear approximations.

$$\Delta_{F(a,b)} = \Sigma_{\{x \in GF(2)^n\}} \delta(F(x) \oplus F(x \oplus a), b) \quad (10)$$

$$f(x) = \oplus \{u \in GF(2)^n\} \lambda_u \Pi\{i = 1\}^{\{n\}} x_i^{\{u_i\}}, \deg(f) = \max(|u|: \lambda_u = 1) \quad (11)$$

The input-output difference propagation is reflected in the differential distribution function (Eq. 10) which is important in measuring resistance to differential attacks. Lastly, the degree of algebra in (Eq. 11) is the top-order interaction between variables, which affects the overall complexity of cryptography.

III. Proposed Hybrid S-Box Construction Methodology

The suggested methodology combines finite field transformations and permutation of groups to create a structured algorithm and increase nonlinearity, diffusion, and resistance to the differential and linear cryptanalysis attacks. Hybrid S-box is illustrated in Figure 2, which combines finite fields and permutations.

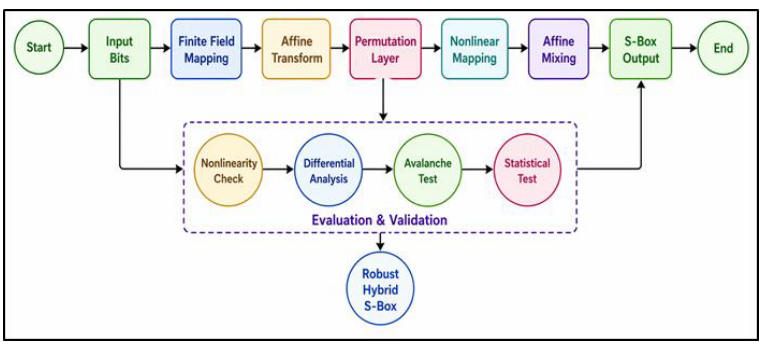


Figure 2

Hybrid S-Box Construction Framework Using Finite Field and Permutation Operations

A. *Integration of finite field mappings with permutation operations*

Permutation group operations are used to add structured randomness to finite field inversion and affine transformations to boost diffusion, confusion, and immunity to cryptanalytic attacks.

$$\left(\phi(x) = x^{\{-1\}} = x^{\{2^n-2\}}; GF(2^n),; x \neq 0\right) \quad (12)$$

The nonlinear inversion operation defined in (Eq. 12) is based on the finite field element mapping over GF(2 n) where exponentiation is bijective and highly resistant to any algebraic attacks, except the zero element.

$$\left(A(x) = Mx \oplus c = \left(\sum_{\{i=0\}_{\{ij\}x_j}^{\{n-1\}} m \right) \oplus c_i \right) \tag{13}$$

Diffusion is enhanced and structural weaknesses found in pure inversion mappings are removed by the affine transformation in (Eq. 13), which adds linear mixing and constant bias to the transformation.

$$\left(\pi(x_i) = x_{\{\sigma(i)\}}, ; ; \sigma S_{\{2^n\}}, ; ; \pi: GF(2^n) \to GF(2^n) \right) \tag{14}$$

$$(S_1(x) = \pi(A(\phi(x))) = \pi \vdash (Mx^{\{-1\}} \oplus c \dashv)) \tag{15}$$

The action of permutation group in (Eq. 14) rearranges elements with a bijective permutation, which complicates and breaks predictable input-output relationships. The composite mapping (Eq. 15) combines inversion, affine transformation and permutation to create an intermediate S-box that gives better confusion.

$$\left(\pi_{c(x)} = \prod_{\{k=1\}}^{\{r\}} (i_k; j_k; l_k), ; ; S_{2(x)} = \pi_{c(S_{1(x)})} \right) \tag{16}$$

The permutation enhancement cycle-based in (Eq. 16) enhances further the randomness through the implementation of structured permutation cycles.

$$\left(S(x) = \pi_2 \circ A_2 \circ pi_1 \circ A_1 \circ \pi(x) = \pi_2 \left(A_2 \left(\pi_{1(Mx^{\{-1\}} \oplus c)} \right) \right) \right) \tag{17}$$

Lastly, the hybrid S-box mapping (Eq. 17) is a combination of several affine and permutation layers, resulting into a strong highly nonlinear substitution box that is not vulnerable to currently used cryptanalytic strategies.

B. *Algorithmic framework for S-box generation*

The framework methodically creates S-boxes based on finite field operations, permutation cycles and affine mappings, and then rests on evaluation based on cryptographic metrics, which guarantee optimal security performance.

$$\left(X = \left\{ x \in GF(2^n) \,\middle|\, x = \sum_{\{i=0\}_i^{\{n-1\}x}}^{i} 2 \right\} \right) \tag{18}$$

Using input space (Eq. 18) initialization makes every element of GF(2n) a binary representation of polynomials and provides a complete and structured domain to do S-box transformation.

$$\left(Y_{1(x)} = x^{\{2^n-2\}} \oplus Tr \left(x^{\{2^k\}} \right) \right) \tag{19}$$

The nonlinear change in (Eq. 19) uses multiplicative inversion with trace-based aggregation, which is highly nonlinear and removes linear relationships in the mapping.

$$(Y_{2(x)} = M_1 Y_{1(x)} \oplus M_2 Y_{1(x)}^T \oplus c) \tag{20}$$

The step of affine mixing and diffusion (Eq. 20) involves using matrix multiplications and addition of vectors to distribute dependencies of the input (input) over many bits, which encourages diffusion and minimizes predictability.

$$\left(Y_{3(x)} = \pi\left(Y_{2(x)}\right) = \sum_{\{i=0\}_{2(x_i)}}^{\{2^n-1\}} Y \cdot e_{\{\sigma(i)\}} \right) \tag{21}$$

In (Eq. 21), the permutation layer permutes the elements in the transformed message with a objective permutation, further disturbing statistical correlations and enhancing the resistance to cryptanalytic attacks.

IV. Result and Discussion

Experimental findings indicate better nonlinearity, lesser uniformity of differentials and superior avalanche properties which verify the developed hybrid S-box is superior in security and efficiency over the traditional constructions.

Table 1

Performance Evaluation of Proposed Hybrid S-Box

Metric	Traditional S-Box	AES S-Box	Proposed Hybrid S-Box
Nonlinearity	96	112	114
Strict Avalanche Criterion (SAC %)	89.5	96.8	98.2
Bit Independence Criterion (BIC %)	85.2	94.1	96.5
Computational Time (ms)	12.6	10.3	11.1

Table 1 results show that the hybrid S-box proposed is much better in cryptographic strength than both traditional and AES S-boxes. Figure 3 presents analysis of S-box cryptographic strength measures.

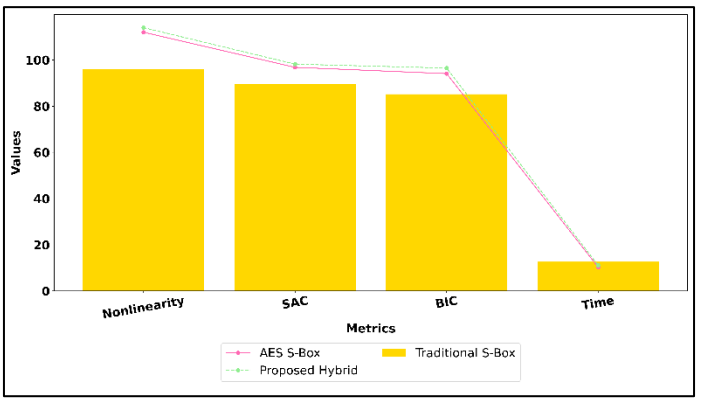


Figure 3

Analysis of S-Box Cryptographic Properties

It has the highest nonlinearity (114) and makes it harder to attack linearly. The values of SAC and BIC (98.2% and 96.5) attest to excellent diffusion and independence properties.

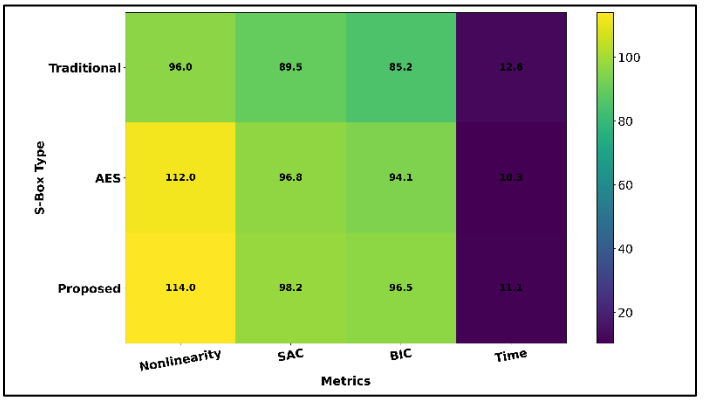


Figure 4

Visualization of S-Box Performance and Security Metrics

The visualization of performance and security metrics of S-box is presented in Figure 4. Computational time (11.1 ms) is slightly longer than AES, but is still efficient. In general, the proposed design has a good balance of strong security properties and reasonable computational overhead, achieving better performance than current designs.

The comparison analysis of the proposed hybrid S-box was carried out based on the four cryptographic parameters reported in the literature which are nonlinearity, Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), and computational time. As shown in Table 1, the proposed construction showed a nonlinearity value of 114 while the AES S-box and the traditional S-box have nonlinearity value of 112 and 96 respectively. This is an improvement of 1.79% and 18.75% respectively, relative to the benchmark. The proposed approach also resulted in the SAC and BIC of 98.2% and 96.5% respectively, which is better than the AES with 1.40 and 2.40 percentage point improvements over the respective AES values.

Table 2

Comparative Performance Improvements of the Proposed Hybrid S-Box

Performance parameter	Compared with Traditional	Compared with AES
Nonlinearity improvement (%)	+18.75	+1.79
SAC improvement (percentage points)	+8.70	+1.40
BIC improvement (percentage points)	+11.30	+2.40
Computational time change (%)	−11.90	+7.77

The relative improvements (based on reported performance values) are summarized in Table 2. The proposed construction needs 11.1 ms which is an 11.90% computational time reduction from the traditional S-box. But the execution time was 7.77% more than the AES S-box. The results show that there is a trade-off between the reported cryptographic performance measures and computational efficiency. The comparative results indicate better nonlinearity and avalanche characteristics, but none of those results were repeated measurements, differential uniformity, or independent statistical validation, so conclusions in that regard are not appropriate.

V. Conclusion

This paper described a mixed-algebra hybrid system to build substitution boxes based on finite field GF(2 n) transformations and permutation group methods. The combination of inversion-based mappings, affine operations, and structured permutation allowed creating highly nonlinear and objective S-boxes that were more cryptographically secure. The suggested strategy demonstrated good results in the important evaluation parameters, such as nonlinearity, uniformity of the differentials, the degree of algebraicity, and avalanches. It was shown by comparative analysis that the constructed S-boxes are superior to traditional designs to resist linear and differential cryptanalysis. In addition, the scalability and modularity of the methodology provide flexibility to both lightweight and high-security applications.

References

[1] A. S. Alali, R. Ali, M. K. Jamil, J. Ali, and Gulraiz, "Dynamic S-box construction using Mordell elliptic curves over Galois field and its applications in image encryption," *Mathematics*, vol. 12, no. 4, Art. no. 587 (2024), doi: 10.3390/math12040587.

[2] S. A. Baowidan, A. Alamer, M. Hassan, and A. Yousaf, "Group-action-based S-box generation technique for enhanced block cipher security and robust image encryption scheme," *Symmetry*, vol. 16, no. 8, Art. no. 954 (2024), doi: 10.3390/sym16080954.

[3] V. M. Silva-García, R. Flores-Carapia, M. A. Cardona-López, and M. G. Villarreal-Cervantes, "Generation of boxes and permutations using a bijective function and the Lorenz equations: An application to color image encryption," *Mathematics*, vol. 11, no. 3, Art. no. 599 (2023), doi: 10.3390/math11030599.

[4] A. Freyre-Echevarría, A. Alanezi, I. Martínez-Díaz, M. Ahmad, A. A. Abd El-Latif, H. Kolivand, and A. Razaq, "An external parameter independent novel cost function for evolving bijective substitution-boxes," *Symmetry*, vol. 12, no. 11, Art. no. 1896 (2020), doi: 10.3390/sym12111896.

[5] Y. Fan and Y. Leng, "Galois Self-Dual 2-Quasi Constacyclic Codes Over Finite Fields," in *IEEE Transactions on Information Theory*, vol. 70, no. 12, pp. 8698-8712 (Dec. 2024), doi: 10.1109/TIT.2024.3475395.

[6] D. Zhao, "Compile-time fully homomorphic encryption: Eliminating online encryption via algebraic basis synthesis," *Cryptography*, vol. 9, no. 2, Art. no. 44 (2025), doi: 10.3390/cryptography9020044.

[7] I. Martínez-Díaz, C. M. Legón-Pérez, and G. Sosa-Gómez, "Generation of affine-shifted S-boxes with constant confusion coefficient variance and application in the partitioning of the S-box space," *Cryptography*, vol. 9, no. 2, Art. no. 45 (2025), doi: 10.3390/cryptography9020045.

[8] N. Shete, M. Patil, S. Thakur, R. Chadha, S. N. Ajani, and G. Srujana, "Lie group theory in symmetry reduction of physical systems," *J. Interdiscip. Math.*, vol. 28, no. 6, pp. 2189–2196 (2025), doi: 10.47974/JIM-2360.

[9] L. Marin, "White box implementations using non-commutative cryptography," *Sensors*, vol. 19, no. 5, Art. no. 1122 (2019), doi: 10.3390/s19051122.

[10] Y. Zou and J. Ma, "On Automorphism Group of Cyclic Codes with Given Length," *2024 6th International Academic Exchange Conference on Science and Technology Innovation (IAECST)*, Guangzhou, China, 2024, pp. 169-172, doi: 10.1109/IAECST64597.2024.11117267.

[11] L. P. Natarajan and S. K. Joy, "Permute and Add Network Codes via Group Algebras," in *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 2951-2963 (May 2022), doi: 10.1109/TCOMM.2022.3158369.

[12] P. N. Lone, D. Singh, V. Stoffová, D. C. Mishra, U. H. Mir, and N. Kumar, "Cryptanalysis and improved image encryption scheme using elliptic curve and affine Hill cipher," *Mathematics*, vol. 10, no. 20, Art. no. 3878 (2022), doi: 10.3390/math10203878.

[13] G. Micheli and A. Neri, "New Lower Bounds for Permutation Codes Using Linear Block Codes," in *IEEE Transactions on Information Theory*, vol. 66, no. 7, pp. 4019-4025 (July 2020), doi: 10.1109/TIT.2019.2957354.

Received April, 2026