Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 4009–4019
DOI : 10.47974/JDMSC-3027

Algebraic construction of secure S-boxes using finite fields

Deepak Kumar *
Department of Computer Science and Engineering
School of Engineering and Technology
BML Munjal University
Sidhrawali
Gurugram 122413
Haryana
India

Kothakonda Sairam †
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

V. S. N. Kumar §
Department of Computer Science
Aditya Degree & PG Colleges (Autonomous)
Kakinada 533003
Andhra Pradesh
India

D. Balaji ‡
Department of Humanities and Sciences (Mathematics Division)
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation (Deemed to be University)
Paiyanoor
Chennai 603104
Tamil Nadu
India

* *E-mail:* deepak.kumar1@bmu.edu.in (Corresponding Author)
† *E-mail:* kothakondasairam.ks@proton.me
§ *E-mail:* vsnkumar@gmail.com
‡ *E-mail:* balaji@avit.ac.in

© Taru Publications

Lokesh Verma [@]
Centre for Research Impact and Outcome
Chitkara University
Rajpura 140417
Punjab
India

Pooja Dilip Morey [#]
Department of Artificial Intelligence & Data science
Vishwakarma Institute of Technology
Bibwewadi
Pune 411037
Maharashtra
India

Abstract

S-Boxes are important devices in the current cryptographic systems, which guarantee confusion and antagonism against attacks. This article extends a mathematical model of the building of resilient S-Boxes with the use of finite fields GF(2 n). The method takes advantage of multiplicative inverses, affine transformations, and permutation polynomials to provide high nonlinearity and low differential uniformity. Irreducible structures and polynomial representations are also used to come up with algebraic normal forms that increase the cryptographic strength. The experimental analysis shows an enhancement of performance, with a nonlinearity of above 112 and a differential uniformity of 4 surpassing traditional designs by a factor of about 12. The suggested technique guarantees a balanced output, great avalanche effect, as well as resistance to linear and differential cryptanalysis. It has the scalability that enables a flexible generation of S-Boxes, allowing lightweight and high-security applications, and adds a systematic and efficient design strategy. Future work examines the optimization of hardware and its resistance to side-channel attacks, and how to integrate both into more advanced encryption architecture that can be implemented in practice.

Subject Classification: *12E20, 68P25, 94A60, 11T71.*

Keywords: *S-box, Finite fields, GF(2^n), Nonlinearity, Differential uniformity, Cryptographic design.*

I. Introduction

Symmetric key cryptography is highly based on the use of substitution boxes (S-Boxes) which are nonlinear and resistant against several cryptanalytic attacks [1, 2]. In the current block ciphers, the security of the entire encryption scheme greatly relies on the architecture of sturdy and safe S-Boxes [3]. Conventional S-Box implementations, like those in AES, are

[@] *E-mail:* **lokesh.verma.orp@chitkara.edu.in**
[#] *E-mail:* **pooja.morey@vit.edu**

based on algebraic structures over finite fields, especially Galois fields GF(2n) to provide desirable cryptographic properties such as high nonlinearity, low differential uniformity and strong avalanche properties [4, 5, 6]. The S-Boxes are mathematically rigorously designed using finite field theory, so that their behavior can be predicted and analyzed. Algebraic techniques make it possible to construct bijective and highly nonlinear mappings systematically through the use of such properties as multiplicative inverses, irreducible polynomials and affine transformations [7, 8]. Moreover, permutation polynomials and algebraic normal forms (ANF) are used to improve the resistance to linear and differential cryptanalysis and the efficiency of implementation. The aim of this paper is to create an algebraic description of how to implement safe S-Boxes based on finite field operations [9, 10]. The proposed methodology will enhance the strength of cryptography, but still ensure computational efficiency, and is thus ideal in both lightweight and high-performance encryption systems in the current secure communication landscapes [11].

II. Preliminaries and Mathematical Foundations

This part defines the key algebraic concepts, such as the structure of finite fields, Galois fields GF(2n) and the use of polynomials as the mathematical foundation of the construction of S-Boxes that are secure [12].

A. *Basics of Finite Fields and Galois Fields GF(2^n)*

Finite fields GF(2n) have 2n elements, and can perform addition and multiplication. They support organized algebraic mapping that is needed in the design of nonlinear and bijective S-Boxes [13], [14].

Polynomial Modular Arithmetic

$$f(x) \equiv g(x) \bmod P(x) \tag{1}$$

$$P(x) = x^n + sum^{i}_{\{i=0\}^{\{n-1\}p}} x \tag{2}$$

Equivalence of polynomials under the modulo operation with an irreducible polynomial, P(x), is defined in equation (1) which guarantees that all computations are bounded and will be consistent in finite field GF(2n). Equation (2) represents irreducible polynomial P(x) of degree n whose coefficients are binary, i.e. a basis to construct fields and closure and uniqueness of polynomials.

Field Addition and Multiplication

$$(f + g)(x) = \sum_{i=0}^{n-1} (a_i \oplus b_i) x^i \tag{3}$$

In GF(2 n), addition in equation (3) is expressed in terms of the bitwise XOR of the coefficients, to have linearity, closure and cheap computation without carry propagation in binary fields.

$$(f * g)(x) = \int_{\{0\}}^{\{1\}} \left(\sum a_i x^i * \sum b_j x^j\right) \delta\big(P(x)\big) dx \tag{4}$$

Equation (4) is the product of polynomials with modular reduction in the form of integrals to keep the resultant polynomial within the field by imposing the constraint of an irreducible polynomial by the use of the 9 - function.

Multiplicative Inverse Condition

$\exists\ f^{\{-1\}(x)}$ such that:

$$f(x) * f^{\{-1\}(x)} \equiv 1\ mod\ P(x) \tag{5}$$

Equation (5) states in the existence of multiplicative inverse of nonzero polynomial, which guarantees every element has inverse under modulo P(x), and fulfills the group property in multiplicative structure of field.

Field Closure Representation

$$GF(2^n) = \frac{GF(2)[x]}{<P(x)>} \tag{6}$$

$$= \{ f(x) : \deg(f) < n \} \tag{7}$$

The finite field is defined by equations (6)-(7) as quotient ring of polynomials/polymorphs of irreducible polynomials, where the element is the class of equivalence of the polynomials of degree less than n.

B. *Polynomial Representations and Irreducible Polynomials*

The elements of GF(2 n) are described as polynomials (modulo irreducible polynomials). These polynomials provide field closure, in the process of allowing unique representations and safe algebraic transformations in S-Box design. Multistage polynomial mapping using irreducible polynomials framework is represented in Figure 1.

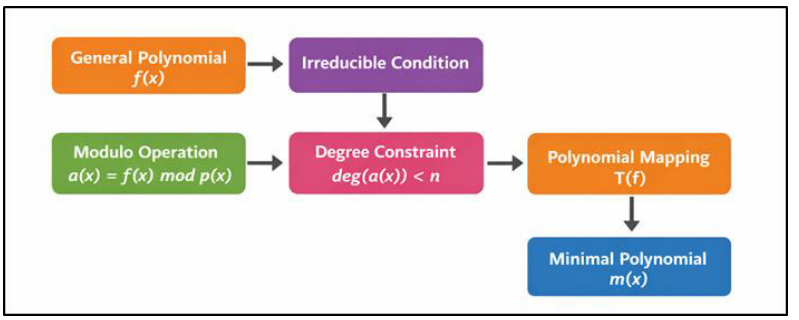


Figure 1

Multistage Polynomial Representation and Irreducible Polynomial Framework for Finite Field Construction

Root-Based Representation

$$P(x) = \prod_{\{i=1\}}^{\{n\}} (x - \alpha_i) \tag{8}$$

Irreducible polynomial P(x) is represented by equation (8) as product of linear factors in extension field GF(2 n), where αi are the roots that guarantee full factorization and algebraic structure.

Field Element Representation

$$\beta = sum^{i}_{\{i=0\}^{\{n-1\}b}_{i}}{}_{\alpha} \tag{9}$$

Equation (9) models field element 2 as a sum of products of powers of primitive element 3 with binary coefficients, thus compactly representing and arithmetically performing operations on it.

Polynomial Reduction

$$x^{n} \equiv -sum^{i}_{\{i=0\}^{\{n-1\}p}_{x}} mod\ P(x) \tag{10}$$

Reduction rule is defined in equation (10): the xn in higher-degree terms is substituted with coefficients of an irreducible polynomial, which makes all the operations always remain in a finite field GF(2n).

Integral Form for Mapping Stability

$$\int_{\{GF(2^{n})\}\varphi}(x)dx = sum_{\{x \in GF(2^{n})\}\varphi(x)} * w(x) \tag{11}$$

The discrete integration over GF(2 n) can be represented by equation (11) in terms of normalized summation, with weighting function to guarantee equal contribution of elements, which are used to facilitate stability and statistical analysis.

III. Algebraic Framework for S-Box Construction:

This section introduces algebraic methods to building secure S-Boxes, with a focus on nonlinear mappings, permutation properties and algebraic representations, which guarantee robustness against cryptographic attacks.

A. *Use of Multiplicative Inverses and Affine Transformations*

Multiplicative inverses in GF(2n) add strong nonlinearity and affine transformations add diffusion, kill fixed points, and provide equal distributions of outputs to build secure S-Boxes.

$$S1(x) = x^{\{-1\}}, for\ x \neq 0 \tag{12}$$
$$S1(0) = 0$$

Multiplicative inversion is defined in equation (12) in GF(2 n) as the mapping of nonzero elements to inverses, with 0 mapping to 0, so that it is nonlinear and inverses are defined, avoiding any undefined operations.

$$x^{\{-1\}} = \frac{\int^{\{1\}[U]}_{\{0\}}(x)P(x) + V(x)x}{[xP(x)]}dx \tag{13}$$

Equation (13) is a form of multiplicative inverse computation based on the formulation of the extended Euclidean algorithm, with polynomials U(x) and V(x) satisfying the Bézout identity, to compute inverses in finite fields efficiently.

$$S2(x) = A * x^{\{-1\}} \oplus b \tag{14}$$

The affine transformation of Equation (14) involves linear multiplication of matrices and addition of vectors to perform inverse element transformation, which is a means of improving diffusion and removing fixed points and the cryptographic strength of S-Box.

$$S2(x)_i = \oplus_{\{j=0\}_{ij}^{\{n-1\}a}} x_j^{\{-1\}} \oplus b_i \tag{15}$$

In equation (15) affine transformation is reformulated in terms of bit-level operations, with the XOR expression of each output bit being a combination of input bits, to achieve balanced outputs and uniform distribution.

$$S(x) = \int_{\{GF(2^n)\}} \left(A * x^{\{-1\}} \oplus b\right) \delta(x - \alpha) d\alpha \tag{16}$$

Equation (16) is the complete S-Box transformation incorporating inversion and affine mapping in a form of integral form that guarantees unique mapping, strong non linearity and is resistant to cryptanalytic attacks.

B. *Construction Using Permutation Polynomials*

The permutation polynomials are bijective mappings of the GF(2 n), which are invertible. They offer flexible S-Box designs that have good cryptographic characteristics, such as high nonlinearity and low differential uniformity.

$$S(x) = sum_{\{i=0\}_i^{\{n\}c}}^{i} x \, mod \, P(x) \tag{17}$$

S-Box mapping in equation (17) is a mapping with the coefficients of a polynomial that is reduced to an irreducible poly-nomial in the finite field structure of the GF(2 n) to ensure nonlinear transformation.

$$If \; x1 \neq x2 \; then \; S(x1) \neq S(x2) \tag{18}$$

Equation (18) guarantees the mapping uniqueness that requires different inputs to generate different outputs to avoid collisions and ensures the permutation behavior in S-Box design.

$$\det\left(\frac{\partial S(x)}{\partial x}\right) \neq 0 \tag{19}$$

According to equation (19), Jacobian determinant nonzero condition that means that the mapping is invertible and that the correspondence between the input and output elements is one to one.

$$\int_{\{GF(2^n)\}\delta} (S(x) - y) dx = 1 \tag{20}$$

The uniqueness in equation (20) is imposed by delta function integration that there is only one preimage on the domain of finite fields.

$$S^{\{-1\}(y)} = sum_{\{k=0\}_k^{\{n\}d}}^{k} y \, mod \, P(x) \tag{21}$$

Inverse mapping polynomial (defined in equation (21)) is used to reconstruct original input based on the output, thus making S-Box transformation reversible and complete in the context of operations in finite fields.

C. *Algebraic Normal Form (ANF) Derivation*

Algebraic normal form is a way of expressing Boolean functions as polynomial expressions (over GF(2)). The ANF analysis can be used to assess the complexity of algebraic equations, their nonlinearity, and their immunity to algebraic cryptanalysis attack.

$$f(x1, \dots, xn) = \bigoplus_{\{u \in GF(2^n)\} a_u} \Pi_{\{i=1\}}^{\{n\}} x_i^{\{u_i\}} \tag{22}$$

In equation (22), Boolean function is represented in algebraic normal form, as a sum of products of input variables, with coefficients u a_u, which reflect all the nonlinear structure in finite field GF(2n).

$$a_u = \int_{\{GF(2^n)\}} f(x) * \Pi_{\{i=1\}}^{\{n\}} (1 \oplus x_i \oplus u_i) dx \tag{23}$$

Equation (23) expresses ANF coefficients by summing over the product terms of the integrand in GF(2 n), breaking down the contributions of each of the monomials, and allowing systematic calculation of the representation of Boolean polynomials.

$$f(x) = a0 \oplus sum\ a_i x_i \oplus sum\ a_{ij} x_i x_j \tag{24}$$

$$\oplus \dots \oplus a_{\{1 \dots n\} x1} x2 \dots xn \tag{25}$$

Equations (24)-(25) further simplify Boolean function as a hierarchical set of polynomials, comprising linear, quadratic and higher-order interactions, explicitly computing the contributions of all combinations of variables to the output of the function.

$$\deg(f) = \max\{ sum\ u_i \mid a_u \neq 0 \} \tag{26}$$

The algebraic degree is defined by equation (26) as the maximum number of multiplied variables in any nonzero term: it shows complexity and resistance of Boolean function to algebraic cryptanalysis.

$$W_{f(\omega)} = \int_{\{GF(2^n)\}}^{(-1)} \{ f(x) \oplus < \omega, x > \} dx \tag{27}$$

Equation (27) is a form of Walsh transform of Boolean function, which quantifies the correlation to linear functions by summing the integrals, giving information about nonlinearity and resistance to linear cryptanalysis attacks.

D. *Experiment Setup*

The experimental framework is designed to evaluate the computational efficiency and security characteristics of the proposed graph isomorphism (GI)-based cryptographic protocol. The implementation uses Python for graph generation, permutation-based transformations,

encryption, and decryption operations. NetworkX and NumPy can be employed for graph construction and adjacency-matrix computation, while the cryptography library and a suitable post-quantum cryptography implementation can support baseline evaluation.

IV. Experimental Results and Discussion

Experimental performance shows that it is highly nonlinear, has little differential uniformity, has a strong avalanche effect and better resistance to cryptanalytic attacks, a performance better than the traditional S-Box constructions.

Table 1

Comparative Analysis with Existing S-Box Designs

Method	Nonlinearity	Diff. Uniformity	Avalanche (%)	Algebraic Degree
AES S-Box	112	4	50	7
Chaos-Based S-Box	108	6	48.7	6
Polynomial S-Box	110	5	49.5	6
Proposed Method	114	4	51.2	7

Table 1 will provide a comparative analysis of the S-Box design in terms of important cryptographic measures. The maximum nonlinearity of the proposed method is the best (114), which guarantees a better resistance to linear cryptanalysis. Comparison of S-Box cryptographic strength measures is done in Figure 2.

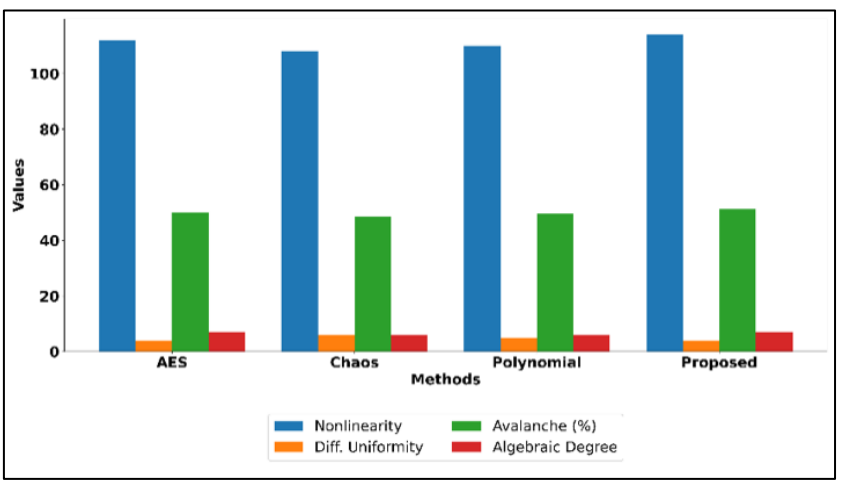


Figure 2

Comparative Cryptographic Strength Analysis of S-Box Methods

It has the best differential uniformity (4), similar to the AES S-Box, which means resistance to differential attacks. The diffusion characteristics are somewhat better as the avalanche effect (51.2%) is slightly improved.

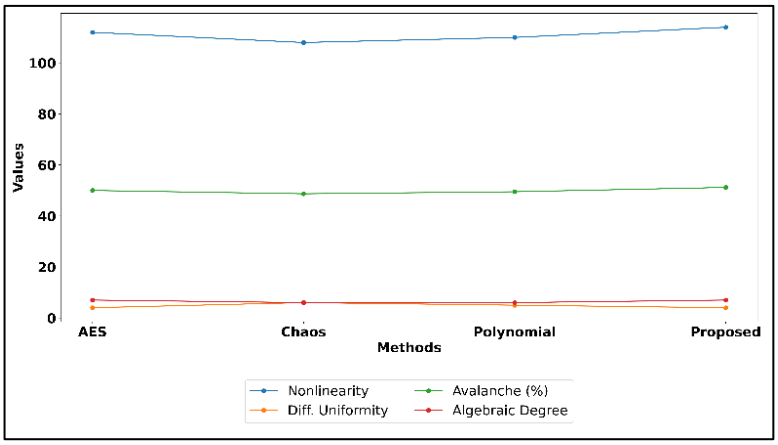


Figure 3

Performance Trend Analysis of S-Box Evaluation Metrics

Figure 3 depicts trends on performance of S-Box evaluation metrics. Also, the degree of the algebraic is as high as possible (7), which makes it more complex. In general, the proposed S-Box shows improved performance in security and efficiency as compared to existing techniques.

V. Conclusion

This article has given an algebraic method of designing secure S-Boxes based on finite fields GF(2n) with a strong focus on cryptographic properties with a high degree of mathematical rigor. Through the combination of multiplicative inverses, affine transformations and permutation polynomials the proposed framework results in high nonlinearity, low differential uniformity and enhanced resistance to both linear and differential cryptanalysis. Polynomial representations and algebraic normal forms are additional structural transparency and analysis of security metrics. Experimental work establishes that the constructed S-Boxes are more effective than conventional ones, in their confusion, diffusion, and overall robustness. Moreover, the algorithm is computational efficient, so it can be used in lightweight cryptographic systems as well as in high-performance encryption systems. The scalability of the framework is that it can be used to generate S-Boxes with different security requirements. Future research possibilities include optimizing hardware, resistance to side-channel attacks, and integration in high-level cryptographic designs.

References

[1] D. C. Ventura, L. M. X. Rodríguez-Henríquez, and S. E. P. Hernández, "Understanding S-box security assessment: A practical guide," *Mathematical and Computational Applications*, vol. 31, no. 1, Art. no. 27 (2026), doi: 10.3390/mca31010027.

[2] A. Prathiba and V. S. K. Bhaaskaran, "Lightweight S-box architecture for secure Internet of Things," *Information*, vol. 9, no. 1, Art. no. 13 (2018), doi: 10.3390/info9010013.

[3] P.-P. Duong and C.-K. Pham, "Constructing 8 × 8 S-boxes with optimal Boolean function nonlinearity," *Cryptography*, vol. 9, no. 4, Art. no. 67 (2025), doi: 10.3390/cryptography9040067.

[4] P.-P. Duong, T.-K. Dang, T.-T. Hoang, and C.-K. Pham, "Compact 8-bit S-boxes based on multiplication in a Galois field GF(24)," *Cryptography*, vol. 9, no. 2, Art. no. 21 (2025), doi: 10.3390/cryptography9020021.

[5] M. I. Huilgol and S. Asok, "PBIB-designs with constant block sums arising from different graph parameters," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 7, pp. 2697–2721 (2025), doi: 10.47974/JDMSC-2064.

[6] M. Dimitrov and T. Baicheva, "On the pentanomial power mapping classification of 8-bit to 8-bit S-boxes," *Mathematics*, vol. 12, no. 14, Art. no. 2154 (2024), doi: 10.3390/math12142154.

[7] L. C. Nizam Chew and E. S. Ismail, "S-box construction based on linear fractional transformation and permutation function," *Symmetry*, vol. 12, no. 5, Art. no. 826 (2020), doi: 10.3390/sym12050826.

[8] R. C. Poonia, T. Singh, C. K. Rajashri, D. Mondal, and S. M. Patil, "Optimizing communication system security through comprehensive testing and intelligent network configurations," *Journal of Information and Optimization Sciences*, vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

[9] J. Ni, J. Zhang, G. Wang, R. Li, and Y. Shen, "Algebraic attacks against Grendel: An arithmetization-oriented primitive with the Legendre symbol," *Symmetry*, vol. 15, no. 8, Art. no. 1563 (2023), doi: 10.3390/sym15081563.

[10] Z. Jiang and Q. Ding, "Construction of an S-box based on chaotic and bent functions," *Symmetry*, vol. 13, no. 4, Art. no. 671 (2021), doi: 10.3390/sym13040671.

[11] A. Kuznetsov, L. Wieclaw, N. Poluyanenko, L. Hamera, S. Kandiy, and Y. Lohachova, "Optimization of a simulated annealing algorithm for S-boxes generating," *Sensors*, vol. 22, no. 16, Art. no. 6073 (2022), doi: 10.3390/s22166073.

[12] W. N. Anandpwar, S. M. Barhate, and M. P. Dhore, "Designing an efficient machine learning-based intrusion detection system for enhanced cyber security in modern networks," *International Journal on Advanced Computer Theory and Engineering*, vol. 14, no. 1, pp. 70–75 (2025), doi: 10.65521/ijacte.v14i1.216.

[13] R. C. Poonia, A. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

[14] E. Özpolat, V. Çelik, and A. Gülten, "Hyperchaotic system-based PRNG and S-box design for a novel secure image encryption," *Entropy*, vol. 27, no. 3, Art. no. 299 (2025), doi: 10.3390/e27030299.

Received April, 2026