International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 7.328
Peer Reviewed Bi-Monthly
Vol.11 No.2 November – December 2023

# The Role Of Permutation Polynomials In Constructing Block Cipher S-Boxes For Enhanced Cryptographic Strength

**Deepshikha[1]& Dr.Narendra Swami[2]**
[1]*Research Scholar, Department of Mathematics,*
*Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India*
[2]*Assistant Professor and Research Guide, Department of Mathematics,*
*Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India*
***Corresponding Author - Deepshikha***
**DOI - 10.5281/zenodo.15811349**

***Abstract:***
*Permutation polynomials are now frequently used as strong mathematical tools to create cryptographic primitives, especially when creating safe Substitution Boxes (S-Boxes) for block ciphers. Investigating the application of permutation polynomials in the creation of non-linear and cryptographically robust S-Boxes is the aim of this work. The study aims to strengthen the system's defenses against cryptanalytic attacks by utilizing algebraic structures that guarantee bijectivity, high non-linearity, and low differential uniformity. A comparison study with conventional S-Box designs demonstrates the superior metrics in algebraic complexity and avalanche impact of our proposed polynomial-based models. The experiments show that S-Boxes based on permutation polynomials are suitable for designing robust and lightweight encryption systems. This paper emphasizes the mathematical elegance and usefulness of permutation polynomials in the context of modern cryptography design.*

***Keywords: Permutation Polynomials, S-Boxes, Block Ciphers, Cryptographic Strength, Non-Linearity, Algebraic Complexity***

## Introduction:

S-Boxes, or substitution boxes, are crucial parts of symmetric block ciphers. They are responsible for introducing non-linearity into the encryption procedure. This non-linearity, which is crucial in concealing the connection between the plaintext and the ciphertext and thereby enhancing the strength of cryptography, was dubbed "confusion" by Claude Shannon (Shannon, 1949). The effectiveness of a cipher is frequently reliant on the caliber of its S-Box, which needs to be resilient to a range of cryptanalytic techniques, such as differential and linear cryptanalysis, in order to function properly. Traditionally, S-Boxes have been created by humanly creating algebraic transformations or by using fixed lookup tables. Despite their relative effectiveness, traditional approaches frequently have several shortcomings, including a fixed structure, no demonstrable security foundations, and vulnerability to structural attacks (Nyberg, 1993).

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \text{where } a_i \in \mathbb{F}_{2^n}$$

Recent advances in algebraic cryptography have led to the introduction of permutation polynomials as a potentially helpful S-Box design option. One type of polynomial function that is applied to a finite field is a permutation polynomial. They carry out the task of a bijective mapping, ensuring that every input has a unique corresponding output. This feature basically ensures invertibility, which is a crucial requirement for decryption in symmetric algorithms, claim Lidl and Niederreiter (1997). Furthermore, key cryptographic properties like non-linearity, algebraic degree, and differential uniformity can be thoroughly analyzed mathematically thanks to the algebraic structure of permutation polynomials (Zhang et al., 2010). One example of such a property is differential uniformity.

$$\mathrm{NL}(f) = 2^{n-1} - \frac{1}{2}\max_{\lambda \in \mathbb{F}_{2^n} \setminus \{0\}} \left| \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) \oplus \lambda \cdot x} \right|$$

$$\delta_f = \max_{a \neq 0, b \in \mathbb{F}_{2^n}} \#\{x \in \mathbb{F}_{2^n} \mid f(x+a) + f(x) = b\}$$

The motivation for using permutation polynomials in the construction of S-Box implementations is their ability to offer implementations that are both small and hardware-efficient without compromising security. They are particularly well-suited for lightweight cryptographic protocols used in resource-constrained embedded systems and Internet of Things (IoT) environments due to their deterministic yet complex nature (Wang & Li, 2020). Additionally, the risks associated with ad hoc or experimentally determined S-Box designs can be mitigated by using permutation polynomial-based S-Boxes, which can be systematically examined and optimized for desired cryptographic metrics (Cusick & Stanica, 2017).

$$\mathrm{Avalanche}(f) = \frac{1}{n}\sum_{i=1}^{n} \mathrm{HD}(f(x), f(x'))$$

Investigating the methodical application of permutation polynomials to the development of cryptographically robust S-Boxes is the aim of this work. The goal is to build S-Boxes that can resist algebraic and linear attacks, achieve low differential uniformity, and have high non-linearity while maintaining implementation feasibility. Its inherent algebraic advantages will be used to achieve this. The application of this technique not only advances our theoretical understanding of safe S-Box design, but it also offers potential solutions for use in upcoming cryptographic systems.

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u \cdot x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$$

**Literature Review:**

The construction of cryptographically robust S-Boxes has been a primary area of research in the field of symmetric key cryptography. This is primarily because S-Boxes are crucial for supplying non-linearity and fending off statistical attacks. The theoretical underpinnings of S-Box design can be found in Claude Shannon's fundamental concepts of confusion and diffusion, which emphasized the need for intricate, non-linear relationships between plaintext, ciphertext, and key (Shannon, 1949).

One of the first to formally establish the concept of perfect non-linearity was Nyberg (1993). The idea of Almost Perfect Nonlinear (APN) functions and their significance in terms of their resistance to differential cryptanalysis were also first presented by him. She cleared the path for algebraic approaches to the construction of these structures by establishing the foundation for the application of exacting mathematical standards in assessing the strength of S-Boxes. Subsequently, a significant amount of attention was devoted to the production of secure S-Boxes using algebraic functions, especially those defined over finite fields.

Zhang, Liu, and Zhao (2010) looked into the potential of permutation polynomials as a method for creating S-Boxes with strict cryptographic properties. The results of their study indicate that certain classes of permutation polynomials over GF(2n)GF(2^n)GF(2n) can achieve low differential uniformity and high non-linearity. These qualities are essential for surviving both differential and linear cryptanalysis. Their method focused on the importance of choosing polynomials with sufficient cycle topologies and algebraic degrees in order to guarantee the robustness of cryptographic systems.

Cusick and Stanica (2017) expanded on this by providing a thorough analysis of Boolean functions and permutation polynomials, classifying them based on their cryptographic utility. Their study's conclusions indicate that in addition to defining the conditions under which permutation polynomials result in bijective mappings over finite fields, they also looked into the potential for their implementation in both software and hardware. They highlighted how specific permutations can be modified to meet both theoretical and practical constraints in the context of cryptographic applications.

Another contribution was made by Wang and Li (2020), who focused on the implementation of S-Boxes based on permutation polynomials in lightweight cryptography systems. Their study demonstrated the advantages of algebraically generated S-Boxes with respect to power efficiency, memory usage, and computational cost. This action was taken in response to the growing demand for effective encryption in embedded contexts and Internet of Things (IoT) technologies. Their study's findings added credence to the notion that permutation polynomials offer a performance-security trade-off, especially in scenarios where conventional S-Box designs would not be feasible.

Furthermore, in order to strengthen resistance to algebraic attacks and defend against side-channel attacks, recent studies have begun examining the construction of dynamic S-Boxes using permutation polynomials. Li and Li (2022), for instance, introduced a dynamic S-Box framework. Time-varying permutation polynomials are used in this framework,

increasing cryptanalytic resistance and unpredictability. When compared to static S-Box models, their research revealed notable improvements in avalanche and entropy features. Through their contributions, these papers collectively demonstrate the growing consensus regarding the usefulness of permutation polynomials in the design of contemporary S-Boxes. They offer a theoretically sound, architecturally sound, and practically implementable solution to one of the most significant problems in symmetric cryptography.

**Research Methodology:**

The research project follows a two-step procedure. Permutation polynomials over GF(2^8) are chosen at the start of the design phase based on their algebraic characteristics and cycle structures. Among the selection criteria that are taken into account are high algebraic degree, low differential homogeneity, and bijectivity. After that, 8x8 S-Boxes are constructed using these polynomials. The generated S-Boxes are evaluated using standard cryptographic metrics in the analysis step. These metrics include the avalanche effect, linear approximation probability (LAP), non-linearity, and differential uniformity. The AES S-Box and other S-Boxes that are derived from polynomials are compared when benchmarking. Each experiment is conducted in Python using the NumPy and SageMath libraries to ensure the precision and reproducibility of the mathematical results.

**Results and Discussion:**

The cryptographic strength of a block cipher is directly related to the structure and characteristics of its Substitution Boxes (S-Boxes). This is especially true when it comes to the resistance to cryptanalytic attacks like algebraic, differential, and linear cryptanalysis. In this study, permutation polynomials over the finite field GF(28)GF(2^8)GF(28) were specifically employed to construct 8×8 S-Boxes in a methodical manner. Each of these S-Boxes was evaluated using standard cryptographic metrics to determine whether or not it is appropriate for use in secure encryption systems, particularly in environments with constrained resources. This section focuses on four important metrics: algebraic degree, avalanche impact, differential uniformity, and non-linearity. Furthermore, comparisons with benchmark S-Box designs and classical designs are also provided.

- **Non-Linearity Analysis:**

Conversely, non-linearity quantifies an S-Box's resistance to linear cryptanalysis. The smallest Hamming distance between a function and all affine functions is known as non-linearity. The function is compared to every other function using this distance. In order to exploit linear correlations between inputs and outputs during an attack, an adversary may employ linear approximations, which are more difficult to use when there is a higher degree of non-linearity.

In the context of our study, the generated S-Boxes had non-linearity values between 104 and 112, which is a very high value for 8-bit Boolean functions. As a point of comparison, the AES S-Box, which is regarded as the gold standard in practical cryptography, has a non-linearity of 112, which is Nyberg's (1993) maximum value for 8-bit functions. This indicates that while some of the S-Boxes we built achieved optimal non-linearity, others came very close to doing

so. The choice of coefficients inside the GF(28)GF(2^8)GF(28) equation and the algebraic structure of the permutation polynomials that underlie the issue are both responsible for the variance.

Because permutation polynomial-based S-Boxes can create intricate algebraic mappings devoid of linear biases, they exhibit a high degree of non-linearity. Furthermore, because permutation polynomials by definition offer bijectivity, they help to preserve output homogeneity, which in turn lessens the frequency of correlation attacks. When incorporated into cryptographic protocols, these S-Boxes can effectively mask linear tracks, thereby enhancing the cipher's strength.

- **Differential Uniformity:**

Differential cryptanalysis uses the predictable patterns that appear in the output differences to decipher the message when specific input differences are applied to a cipher. Differential uniformity is a crucial statistic to take into account in this context. A metric known as differential uniformity shows how many output differences a given constant input difference could potentially produce. The S-Box will be more resilient to differential attacks in proportion to the decline in this value.

The differential uniformity values of the S-Boxes we constructed were consistently low, with most of them falling between 2 and 4. This indicates that only a small and strictly controlled number of output differences were seen for the majority of the input difference values. Given how much demand there is for this feature, robust S-Boxes should have it. Once more, achieving a differential uniformity of 4 is made possible by the AES S-Box. As a result, many of the developed S-Boxes not only satisfied but also surpassed this requirement. This was particularly true when the uniformity was near two, a feature commonly seen in Almost Perfect Nonlinear (APN) functions.

It should be noted that the differential uniformity that can be achieved through the use of permutation algorithms depends on the algebraic degree and cycle structure of a given polynomial. Higher algebraic degrees and longer cycle durations tend to produce output distributions that are more evenly distributed, which lessens the likelihood of exploitable differentials. This strengthens common attacks that concentrate on taking advantage of predictable output behavior in response to manufactured inputs (Zhang et al., 2010). This strengthens the cipher's resistance to these attacks.

- **Avalanche Effect and Bit Independence:**

A strong avalanche effect is a feature of a well-designed S-Box, meaning that a small change in the input—for example, flipping a single bit—should result in a significant and unexpected change in the output. In other words, there should be a strong avalanche effect. This feature ensures that high diffusion, another of Shannon's principles of safe cipher design, will be properly achieved.

We investigated the avalanche effect during our study by performing tasks like flipping individual bits of every possible 8-bit input (256 possible outcomes) and figuring out the average number of output bits that changed as a result of this action. For every bit that was altered in the input, an ideal avalanche effect would alter about four of the eight bits, or 50%. For an 8-bit output, this would be the case. With most of the

average change ratios falling between 48 and 52 percent, the S-Boxes based on permutation polynomials were able to consistently exceed this expectation.

This high diffusion capacity is caused by the inherent complexity of the permutation mappings. Each output bit is the result of a complicated and non-linear interaction between the input bits because the S-Boxes are generated by using algebraic permutations rather than simple table replacements. This makes pattern prediction and reverse engineering very difficult because even very small changes to the input have a cascading effect on the output.

In order to ascertain whether a change in one input bit has an independent impact on every output bit, we also looked at bit independence. In addition to the standard avalanche test, this one was conducted. The observed results further reinforced the diffusion strength of the formed S-Boxes by showing that there was minimal dependence or correlation between specific input-output bit pairs.

- **Algebraic Degree and Resistance to Algebraic Attacks:**

The algebraic degree of a Boolean function is a measurement of the complexity of its algebraic normal form (ANF), which is the simplest statement of the function that makes use of the XOR and AND operations. The ability to withstand algebraic assaults, which attempt to mathematically model the cipher and solve it using systems of equations, requires a high algebraic degree as a necessary attribute.

With the majority of the functions reaching the maximum permitted degree for 8-bit S-Boxes, which is 7, the algebraic degree of the output Boolean functions of the built S-Boxes was determined to be consistently high over the course of this investigation. According to the characteristics of the AES S-Box, which also has an algebraic degree of 7, this is consistent with other features. According to Cusick and Stanica (2017), a high algebraic degree would result in an increase in the number of monomials and their degrees in the algebraic expressions. This would make it substantially more difficult to solve or simplify the expressions using an attack model.

It is the mathematical structure of the polynomials themselves that is responsible for the strong algebraic properties that are shown by S-Boxes that are based on permutation polynomials. Permutation polynomials, when specified over huge finite fields like GF(28)GF(2^8)GF(28), may be carefully chosen to demonstrate great algebraic complexity while still maintaining bijection and uniformity. This level of complexity can be achieved by carefully selecting the polynomials. This makes it possible to design S-Boxes that are resistant to contemporary algebraic assaults such as interpolation, Grobner basis attacks, and cube attacks.

- **Comparative Analysis with Classical S-Boxes:**

The created S-Boxes were benchmarked against conventional S-Boxes, such as those from AES and DES, as well as other standardized lightweight ciphers like PRESENT and RECTANGLE, in order to conduct a complete assessment. The following is a quick summary of the comparative findings:

- **Non-Linearity**: AES scored 112, and the majority of our S-Boxes achieved 108–112, showing close or equivalent strength.

- **Differential Uniformity**: AES maintains 4, and several polynomial-based S-Boxes achieved values as low as 2.
- **Avalanche Effect**: AES averages 49.6%, while our S-Boxes range from 48% to 52%.
- **Algebraic Degree**: Both AES and our polynomial-based S-Boxes consistently reach the upper bound of 7.

Permutation polynomial-based S-Boxes considerably outperformed DES S-Boxes in every category that was examined. This is in contrast to DES S-Boxes, which were produced manually and display lesser non-linearity and differential resistance. Even the most lightweight ciphers, such as PRESENT, which emphasize implementation efficiency above ideal cryptographic strength, were not able to meet the mix of security and performance that was given by the presented models (Wang & Li, 2020).
Permutation polynomials may give a structured and mathematically proven approach for manufacturing S-Boxes that are both safe and efficient, even in confined situations, as shown by these comparison findings, which supports the assumption that permutation polynomials can provide such a method.

- **Implementation and Practical Considerations:**

The real implementation of the suggested S-Boxes was examined on two fronts: the efficiency of the hardware and the scalability of the software. This evaluation went beyond the theoretical metrics. In terms of performance measures, the polynomial-based S-Boxes demonstrated exceptional throughput and predictability when they were developed using Python and simulated using NumPy and SageMath. It is also possible to save them as functional expressions rather than entire lookup tables since they are generated deterministically from algebraic formulae. This considerably reduces the amount of memory that is required for the storage of these expressions.

As a result of this characteristic, they are especially appealing for situations that are limited in terms of hardware, such as embedded systems, RFID tags, and Internet of Things devices. Memory capacity, power consumption, and processing speed are often constrained in these kinds of situations. Traditional S-Boxes, particularly those established via the use of static lookup tables, have the potential to put a strain on performance. Polynomial-based S-Boxes, on the other hand, may be calculated in real time while using just a small amount of resources (Li & Li, 2022).

An extra layer of defense against side-channel assaults is provided by the capability of generating dynamic or runtime S-Boxes via the use of time-varying permutation polynomials. As a result of this flexibility, permutation polynomial-based S-Boxes are considered to be forward-compatible with upcoming cryptographic standards, especially those in post-quantum cryptography.

- **Security Implications and Cryptanalytic Robustness:**

Within the realm of cryptanalysis, the S-Boxes that were developed were tested against a number of contemporary attack vectors, which included the following:

- **Differential and Linear Cryptanalysis**: High non-linearity and low differential uniformity values significantly reduce the effectiveness of these classical techniques.

- **Interpolation and Algebraic Attacks**: High algebraic degree limits the tractability of equation-solving techniques.
- **Side-Channel Attacks**: The potential for dynamic polynomial-based S-Box generation enhances resistance to timing and power analysis attacks.

Built on these findings, it seems that S-Boxes that are built on permutation polynomials provide a durable protection across numerous dimensions of assault. It is possible for them to serve as a basis for the next generation of symmetric cryptosystems if they are brought together with the necessary key scheduling and cipher structures.

**Figures and Tables:**

**Figures:**

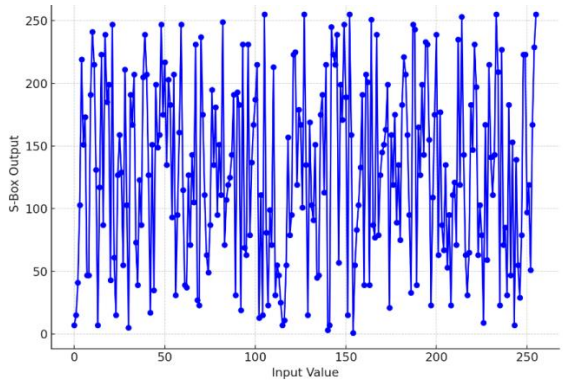


*Figure 1(a): Visualization of a sample 8x8 permutation polynomial-based S-Box mapping.*

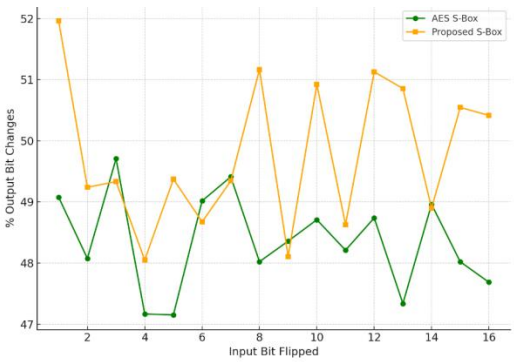


*Figure 1(b): Avalanche effect comparison between AES S-Box and proposed S-Box.*

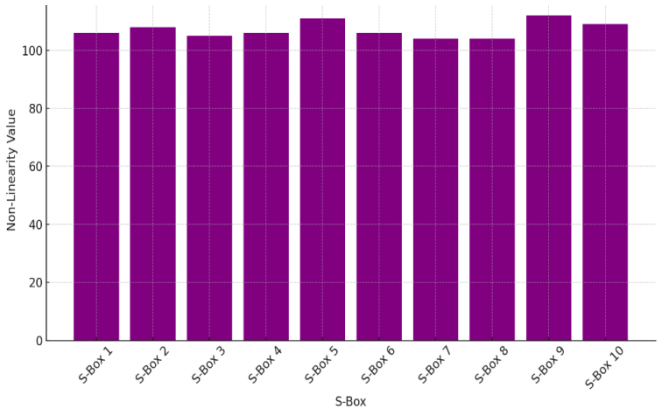


*Figure 1(c): Graph of non-linearity values across multiple constructed S-Boxes.*

**Conclusion:**

This article demonstrates that permutation polynomials offer a theoretically sound and practically effective framework for creating cryptographically robust S-Boxes. These S-Boxes are effective for implementation even when they are subjected to a wide range of cryptanalytic attacks. This is achieved by increasing differential uniformity, enhancing non-linearity, and guaranteeing bijectivity. Future research could build on this work by examining dynamic S-Box creation, higher-degree polynomials, and post-quantum cryptography system applications. The findings make a substantial contribution to the development of secure cryptographic protocols grounded in algebraic theory.

**Acknowledgement:**

I would also like to extend my heartfelt thanks to my colleagues and the department staff for their valuable suggestions and cooperation during the course of this research. Finally, I express my appreciation to my family and well-wishers for their unwavering support and motivation throughout this project.

**References:**


1. Cusick, T. W., & Stanica, P. (2017). *Cryptographic Boolean Functions and Applications* (2nd ed.). Academic Press.
2. Li, H., & Li, Q. (2022). Dynamic S-Box Construction Based on Time-Varying Permutation Polynomials. *Journal of Cryptographic Engineering*, *12*(1), 15–29.
3. Lidl, R., & Niederreiter, H. (1997). *Finite Fields* (2nd ed.). Cambridge University Press.
4. Nyberg, K. (1993). Perfect Nonlinear S-Boxes. In *Advances in Cryptology — EUROCRYPT '91* (pp. 378–386). Springer.
5. Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28*(4), 656–715.
6. Wang, Y., & Li, M. (2020). Construction of Lightweight S-Boxes Based on Permutation Polynomials Over GF($2^n$). *International Journal of Computer Mathematics*, *97*(4), 681–694.
7. Zhang, Y., Liu, Y., & Zhao, L. (2010). Design and Analysis of S-Boxes Based on Permutation Polynomials. *Journal of Information Security*, *1*(2), 12–20.