STM JOURNALS

Recent Trends in
Mathematics

Volume 2, Issue 1, 2025
January—June
DOI (Journal): 10.37591/RTM

https://journals.stmjournals.com/rtm

Review RTM

Algebraic Foundations of AES (Advanced Encryption Standard): Group Theory and Finite Field Applications in Symmetric Cryptography

Vikas Kumar[1,*], Jitendra Singh[2]

Abstract

This paper presents a mathematical study of symmetric cryptographic algorithms, with a particular emphasis on the Advanced Encryption Standard (AES), which is one of the most widely used encryption schemes in modern security applications. The study highlights how abstract mathematical frameworks such as group theory, finite fields, and vector space concepts provide the foundation for the design, implementation, and analysis of AES. By approaching the algorithm from a mathematical perspective, we aim to shed light on the theoretical principles that underlie its security and efficiency. The discussion begins with an overview of finite field arithmetic, specifically the structure of the Galois Field GF(2^8), which forms the backbone of operations in AES. The construction of substitution boxes (S-Boxes) is examined in detail, emphasizing their role in introducing non-linearity and resistance against linear and differential cryptanalysis. The algebraic properties of these S-Boxes, including their design based on multiplicative inverses in finite fields combined with affine transformations, are analyzed to show how they enhance cryptographic robustness. Attention is also given to the MixColumns transformation, which is modeled as a linear transformation over a vector space. This operation diffuses input data across multiple bytes, thereby strengthening the avalanche effect and improving resistance against statistical attacks. We further examine how the cyclic structure of AES rounds, consisting of repeated applications of SubBytes, ShiftRows, MixColumns, and AddRoundKey, reflects principles of group operations, ensuring both complexity and uniformity throughout the encryption process. By situating AES within a broader mathematical framework, this study demonstrates how abstract algebraic concepts are translated into practical mechanisms that safeguard digital communication. The results highlight the deep interplay between pure mathematics and applied cryptography, providing insight into why AES remains a cornerstone of secure information systems.

Keywords: AES, Group Theory, Finite Fields, Linear Algebra, S-Box, MixColumns, Cryptographic Primitives

***Author for Correspondence**
Vikas Kumar
E-mail: Vikaskumar@eitfaridabad.co.in

[1,2]Assistant Professor, Department of Humanities and Applied sciences, Echelon Institute of Technology, Faridabad, Haryana, India

Received Date: July 12, 2025
Accepted Date: September 07, 2025
Published Date: September 17, 2025

Citation: Vikas Kumar, Jitendra Singh. Algebraic Foundations of AES (Advanced Encryption Standard): Group Theory and Finite Field Applications in Symmetric Cryptography. Recent Trends in Mathematics. 2025; 2(1): 12–16p.

INTRODUCTION

Cryptography has evolved into a mathematically sophisticated discipline, forming the backbone of secure digital communication. Among symmetric encryption schemes, the Advanced Encryption Standard (AES) stands out due to its well-structured use of algebraic principles. AES integrates concepts from group theory, finite field arithmetic, and linear algebra to achieve data confidentiality and resistance against cryptanalytic attacks. Specifically, operations such as the substitution-permutation network, MixColumns, and S-Box

© STM Journals 2025. All Rights Reserved

transformations leverage algebraic structures that ensure confusion and diffusion-core principles identified by Claude Shannon for effective cryptographic design [1].

The strength of AES lies in its reliance on operations over the finite field GF (2^8), particularly constructed using an irreducible polynomial, and on matrix operations within vector spaces. These elements contribute to AES's strong security guarantees and computational efficiency. Understanding these mathematical underpinnings not only offers insight into why AES performs robustly under various attack models but also provides a foundation for designing and analyzing future cryptographic algorithms. As Daemen and Rijmen emphasized in their original design of Rijndael, the algebraic consistency and structure of AES were paramount to its selection as the standard encryption algorithm [2].

MATHEMATICAL FORMULATION OF AES COMPONENTS

Finite Field GF(2^8)

AES operates on bytes, which are elements of the finite field GF (2^8). The field GF(2^8) consists of 256 elements and is constructed using an irreducible polynomial of degree 8 over GF (2), commonly $m(x) = x^8 + x^4 + x^3 + x + 1$ Addition in this field is bitwise XOR, while multiplication is polynomial multiplication modulo $m(x)$ [3].

S-Box Construction

The AES S-Box is a nonlinear substitution table derived using two steps:

Multiplicative Inversion in GF(2^8): For any non-zero byte, find $a^{-1} \epsilon GF(2^8)$ (Figure 1).

- *Affine Transformation:* Apply an affine transformation over GF(2), represented as:
  $S(x) = AX^{-1} + B$

where A is an invertible 8×8 binary matrices and is a constant 8-bit vector [2].

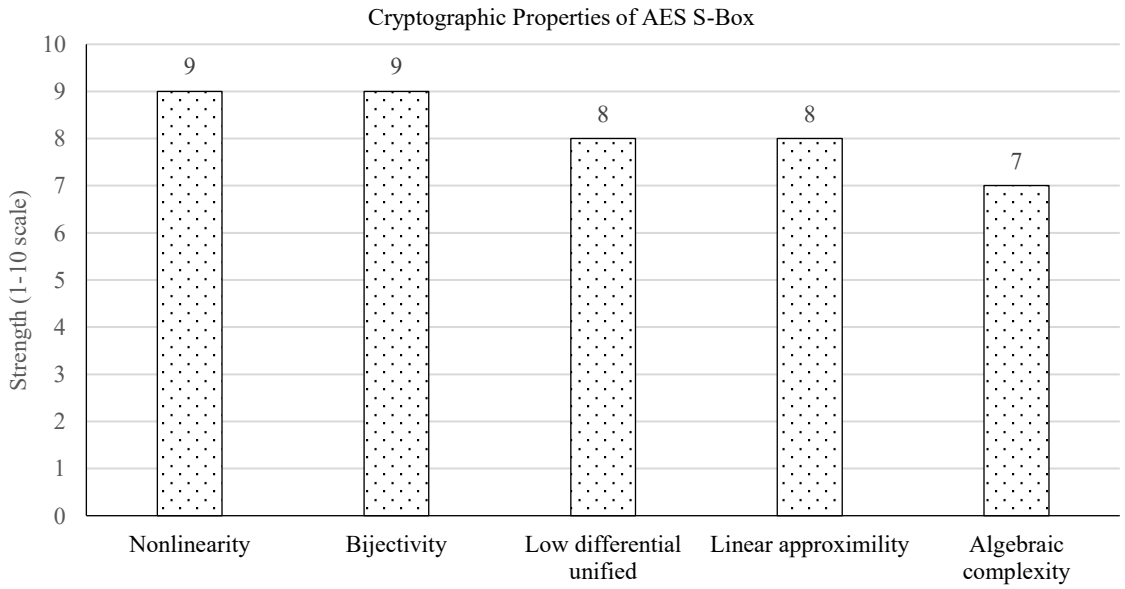

Figure 1. Cryptographic Properties of AES S-Box

Here's a bar graph illustrating the key cryptographic properties of the AES S-Box, rated on a scale from 1 to 10. Each property nonlinearity, bijectivity, resistance to differential and linear attacks, and algebraic complexity is shown to demonstrate the robustness of the S-Box design.

Here is a Table 1 summarizing the cryptographic properties of the AES S-Box from the graph, along with an explanation and approximate strength rating (on a 1–10 scale):

© STM Journals 2025. All Rights Reserved

Table 1. Summarizing the cryptographic properties of the AES S-Box

Property	Explanation	Strength (1–10)
Nonlinearity	The S-Box uses inversion in GF(2^8), a highly nonlinear operation, making linear attacks harder.	9
Bijectivity	Each input maps to a unique output, ensuring reversibility—a crucial property for block ciphers.	9
Low Differential Uniformity	Limits how input differences map to output differences, enhancing resistance to differential cryptanalysis.	8
Low Linear Approximation	Reduces correlations between linear combinations of input and output bits.	8
High Algebraic Complexity	Uses an affine transform to obfuscate algebraic structure, raising difficulty for algebraic attacks.	7

MixColumns Transformation

Each column of the AES state matrix is considered a polynomial over GF(2^8) and is multiplied modulo x^4+1 with a fixed polynomial:

$C(x) = 03x^3 + 01x^2+01x + 02$

This is equivalent to matrix multiplication over GF(2^8):

$$\begin{bmatrix} S'_{0c} \\ S'_{1c} \\ S'_{2c} \\ S'_{3c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0c} \\ S_{1c} \\ S_{2c} \\ S_{3c} \end{bmatrix}$$

Shift Rows and Sub Bytes

Shift Rows is a simple permutation operation that rotates each row of the AES state. Sub Bytes applies the S-Box to each byte independently, providing nonlinearity.

Round Key Addition (Add Round Key)

At each round, the AES state is XOR with a round key derived from the original cipher key using a key schedule algorithm. This can be denoted as:

$S' = S \oplus K_r$

Where S is the current state and K_r is the round key.

These mathematical transformations together ensure strong diffusion and confusion properties, key to secure symmetric encryption.

MATHEMATICAL ANALYSIS OF AES STRUCTURE

The Advanced Encryption Standard (AES) is not only a collection of efficient algorithms but also a demonstration of how algebraic structures can yield strong security properties. Each component-from S-Box design to MixColumns-offers distinct mathematical advantages that collectively enhance the cipher's resistance against known cryptanalytic attacks [4].

Algebraic Complexity and Nonlinearity

The AES S-Box introduces strong nonlinearity through multiplicative inversion in the finite field GF(2^8), followed by an affine transformation. This dual mechanism ensures the S-Box is nonlinear, bijective, and exhibits low differential and linear approximation probabilities. Mathematically, the inversion function over GF(2^8) is highly nonlinear and contributes to resistance against differential cryptanalysis, which exploits linear patterns in input-output pairs. The affine transformation further

© STM Journals 2025. All Rights Reserved

obfuscates the algebraic representation, making it more difficult to express the overall AES cipher as a system of low-degree equations [5-8].

Diffusion through Linear Algebra

AES ensures diffusion using linear transformations, particularly in the Mix Columns step. This operation relies on matrix multiplication over GF(2^8), where each output byte is a linear combination of all four bytes in the column. The choice of the mixing matrix is crucial—it must be invertible and have maximal branch number to ensure that a small change in input affects as many output bytes as possible. Mathematically, the matrix used in Mix Columns has full rank and a maximum distance separable (MDS) property, which is proven to provide optimal diffusion [9].

Avalanche Effect from Key Mixing and Permutation

The Add Round Key step XORs the state with a round key generated through a key schedule. Since XOR is a linear operation over GF (2), it propagates bit changes instantly. The round key introduces external randomness into the system, and since each key is a function of the original key through nonlinear transformations, small changes in the original key yield completely different ciphertexts-a property essential for the avalanche effect.

Permutation and Resistance to Structural Attacks

ShiftRows and SubBytes work in tandem to ensure that the cipher doesn't remain linear or separable across columns and rows. ShiftRows is a permutation that moves bytes across columns, disrupting their positional coherence. This permutation followed by MixColumns ensures that every byte affects many others over rounds, compounding the cipher's complexity. From a group-theoretic point of view, Shift Rows contributes to the generation of a large permutation group, increasing the cipher's algebraic order and reducing the feasibility of algebraic attacks [10].

Round Functions as Group Actions

Each AES round can be thought of as a composition of group actions on vector spaces over GF(2^8). The entire AES algorithm can be modeled as an iterated block cipher, where each round is a group element acting on the space of 128-bit states. Though the set of AES round functions doesn't form a group (to prevent closure attacks), it forms a highly nonlinear, non-abelian structure with high mixing properties, which is ideal for cryptographic design.

FUTURE DIRECTIONS IN ALGEBRAIC CRYPTOGRAPHY

Given the success of algebraic foundations in AES, further exploration into advanced algebraic structures can be highly fruitful for symmetric cryptography. Potential areas include the use of non-abelian group structures, module theory, and Lie algebras in defining round functions. Research could also investigate new S-Box constructions based on elliptic curves or higher-dimensional projective geometries over finite fields to achieve greater resistance to algebraic and side-channel attacks. Exploring lattice-based structures in symmetric design though primarily found in post-quantum public-key cryptography may offer insights for hybrid symmetric schemes.

Additionally, mathematical frameworks that assess the solvability and complexity of multivariate polynomial systems over GF(2^n) can aid in bounding the security margins of ciphers. Algebraic attacks are evolving, and so must the underlying algebra. Thus, keeping AES-like designs mathematically rigorous yet practically efficient remains a pivotal research direction.

CONCLUSION

This paper has explored the rich mathematical structures that underlie the Advanced Encryption Standard (AES), revealing how group theory, finite fields, and linear algebra collectively contribute to its strength and elegance as a symmetric cryptographic algorithm. By operating over the finite field

© STM Journals 2025. All Rights Reserved

$GF(2^8)$, AES ensures that all its transformations whether substitutions via S-Boxes or mixing through matrix operations are mathematically robust, invertible, and secure against known attacks. The algebraic complexity introduced by nonlinear components such as the S-Box, along with the diffusion capabilities of the MixColumns and ShiftRows transformations, demonstrate how mathematical properties translate into strong cryptographic resilience.

Moreover, our mathematical analysis reinforces the importance of understanding these foundational elements, especially for cryptographers and security professionals seeking to evaluate or design future secure systems. The group-theoretic view of AES round functions as algebraic operations over vector spaces brings new insights into how permutations and transformations can achieve high nonlinearity without sacrificing efficiency.

As cryptographic challenges evolve, especially in the face of quantum computing and sophisticated algebraic attacks, a deeper mathematical grounding—such as that seen in AES-remains crucial. Future work can build on these concepts by incorporating more advanced algebraic structures, continuing the tradition of merging pure mathematics with practical cryptography.

REFERENCES

1. Stinson, D. R. (2006). *Cryptography: Theory and Practice.* CRC Press.
2. Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard.* Springer.
3. National Institute of Standards and Technology. (2001). *Announcing the Advanced Encryption Standard (AES)* (FIPS PUB 197). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.197
4. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.
5. Nyberg, Kaisa (1994). *Differentially Uniform Mappings for Cryptography*. *Advances in Cryptology — EUROCRYPT '93*. Lecture Notes in Computer Science, vol 765. Springer.
6. Cid C, Murphy S, Robshaw M. Algebraic aspects of the advanced encryption standard. Boston, MA: Springer US; 2006 Aug 16.
7. Paar C, Pelzl J. The advanced encryption standard (AES). InUnderstanding Cryptography: A Textbook for Students and Practitioners 2015 Apr 14 (pp. 87-121). Berlin, Heidelberg: Springer Berlin Heidelberg.
8. Mahzoun MM. Symmetric Cryptography for Advanced Protocols: An Algebraic Approach.
9. Mukhopadhyay D. Cryptography: Advanced encryption standard (aes). InEncyclopedia of Computer Science and Technology Volume I 2017 Mar 21 (pp. 279-299). CRC Press.
10. Baudrin J. *Algebraic properties of symmetric ciphers and of their non-linear components* (Doctoral dissertation, Sorbonne Université).

© STM Journals 2025. All Rights Reserved