MixColumns Transformation in AES

PhD Nguyen Ngoc Tu

March 23, 2025

Introduction

- AES (Advanced Encryption Standard) uses a MixColumns transformation.
- Operates in $GF(2^8)$ using the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.
- Strengthens diffusion in AES encryption.

Given Matrices in AES

MixColumns Matrix M:

$$M = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Inverse MixColumns Matrix M^{-1}:

$$M^{-1} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix}$$

Polynomial Representation in $GF(2^8)$

Element Representation in $GF(2^8)$:

- $1 = 00000001_2 \rightarrow x^0$;
- $2 = 00000010_2 \rightarrow x$
- $3 = 00000011_2 \rightarrow x + 1$;
- $9 = 00001001_2 \rightarrow x^3 + 1$
- $11 = 00001011_2 \rightarrow x^3 + x + 1$
- $13 = 00001101_2 \rightarrow x^3 + x^2 + 1$
- $14 = 00001110_2 \rightarrow x^3 + x^2 + x$

MixColumns Matrix M in Polynomial Form:

$$M = \begin{bmatrix} x & x+1 & x^0 & x^0 \\ x^0 & x & x+1 & x^0 \\ x^0 & x^0 & x & x+1 \\ x+1 & x^0 & x^0 & x \end{bmatrix}$$

Inverse MixColumns Matrix M^{-1} in Polynomial Form:

$$M^{-1} = \begin{bmatrix} x^3+x^2+x & x^3+x+1 & x^3+x^2+1 & x^3+1 \\ x^3+1 & x^3+x^2+x & x^3+x+1 & x^3+x^2+1 \\ x^3+x^2+1 & x^3+1 & x^3+x^2+x & x^3+x+1 \\ x^3+x+1 & x^3+x^2+1 & x^3+1 & x^3+x^2+x \end{bmatrix}$$

In $GF(2^8)$, calculations follow modular arithmetic using $x^8 + x^4 + x^3 + x + 1$.

Verification: $M \cdot M^{-1}$

Matrix Multiplication in $GF(2^8)$:

$$(M \cdot M^{-1})_{ij} = \sum_{k=0}^{3} M_{ik} \cdot M^{-1}_{kj} \mod (x^8 + x^4 + x^3 + x + 1)$$

Performing computations in $GF(2^8)$, we obtain:

$$M \cdot M^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

This confirms that M^{-1} is indeed the correct inverse of M.

Conclusion

- MixColumns and its inverse enhance AES security through diffusion.
- Operations occur in $GF(2^8)$ with modular arithmetic.
- Essential for both encryption and decryption phases.