Giả sử ma trận trạng thái trước khi bước vào phép tính Mix Column của AES là

$$\begin{pmatrix} c_0 & c_1 & c_2 & c_3 \\ c_4 & c_5 & c_6 & c_7 \\ c_8 & c_9 & c_{10} & c_{11} \\ c_{12} & c_{13} & c_{14} & c_{15} \end{pmatrix} \tag{1}$$

Phép tính Mix Column lấy mỗi cột của ma trận trạng thái trên làm tham số cho đa thức với hệ số trong $GF(2^8)$ và nhân với đa thức $c(z) = 2 + z + z^2 + 3z^3$ rồi modulo cho $z^4 + 1$.

Giả sử với cột đầu tiên, ta viết hệ số theo thứ tự bậc tăng dần $d(z) = c_0 + c_4 z + c_8 z^2 + c_{12} z^3$.

Tính (trong $GF(2^8)$)

$$\begin{aligned} c(z) \cdot d(z) =& (2 + z + z^2 + 3z^3) \cdot (c_0 + c_4 z + c_8 z^2 + c_{12} z^3) \\ =& 2c_0 + 2c_4 z + 2c_8 z^2 + 2c_{12} z^3 \\ &+ c_0 z + c_4 z^2 + c_8 z^3 + c_{12} z^4 \\ &+ c_0 z^2 + c_4 z^3 + c_8 z^4 + c_{12} z^5 \\ &+ 3c_0 z^3 + 3c_4 z^4 + 3c_8 z^5 + 3c_{12} z^6 \\ =& 2c_0 + (2c_4 + c_0) z + (2c_8 + c_4 + c_0) z^2 \\ &+ (2c_{12} + c_8 + c_4 + 3c_0) z^3 + (c_{12} + c_8 + 3c_4) z^4 \\ &+ (c_{12} + 3c_8) z^5 + 3c_{12} z^6 \end{aligned}$$

Trong $GF(2^8)$ thì mọi phần tử đều có tính chất $2x^n = 0$, tương đương với $x^n = -x^n$. Do đó

$$\begin{aligned} z^6 &\pmod{z^4 + 1} \equiv -z^2 \equiv z^2 \\ z^5 &\pmod{z^4 + 1} \equiv -z \equiv z \\ z^4 &\pmod{z^4 + 1} \equiv -1 \equiv 1 \end{aligned}$$

Suy ra

$$
\begin{aligned}
c(z)\cdot d(z) =& 2c_0 + (2c_4 + c_0)z + (2c_8 + c_4 + c_0)z^2 \\
&+ (2c_{12} + c_8 + c_4 + 3c_0)z^3 + (c_{12} + c_8 + 3c_4) \\
&+ (c_{12} + 3c_8)z + 3c_{12}z^2 \\
=& (c_{12} + c_8 + 3c_4 + 2c_0) + (c_{12} + 3c_8 + 2c_4 + c_0)z \\
&+ (3c_{12} + 2c_8 + c_4 + c_0)z^2 + (2c_{12} + c_8 + c_4 + 3c_0)z^3
\end{aligned}
$$

Như vậy xét hệ số lần lượt trước 1, z, z^2 và z^3 thì tương đương với phép nhân ma trận

$$
\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_4 \\ c_8 \\ c_{12} \end{pmatrix} \tag{2}
$$