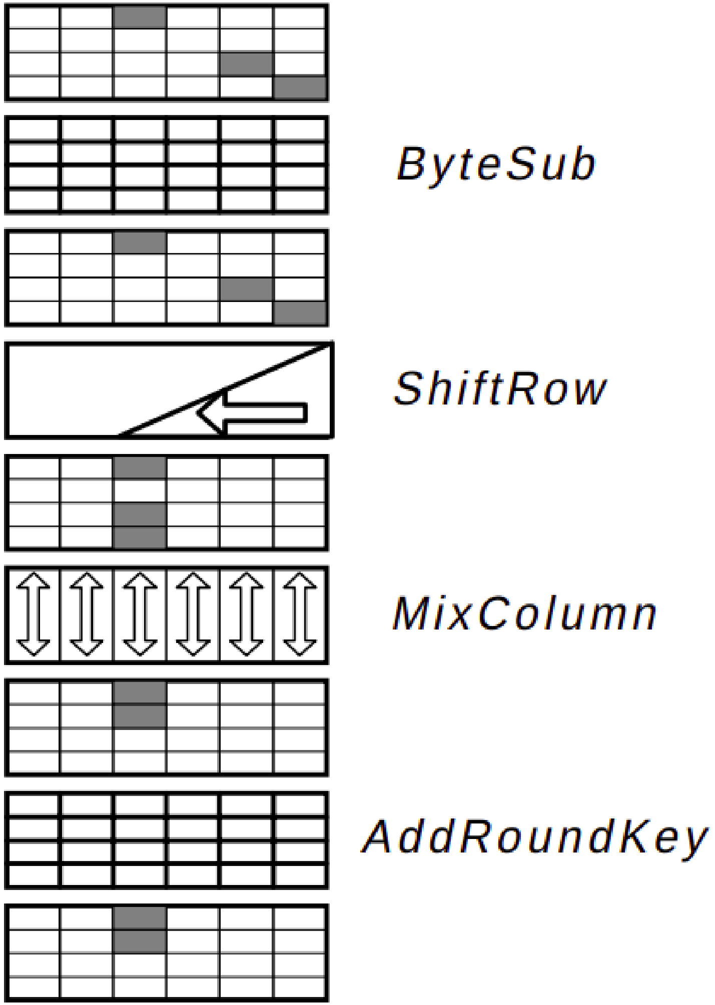
More notes on AES…

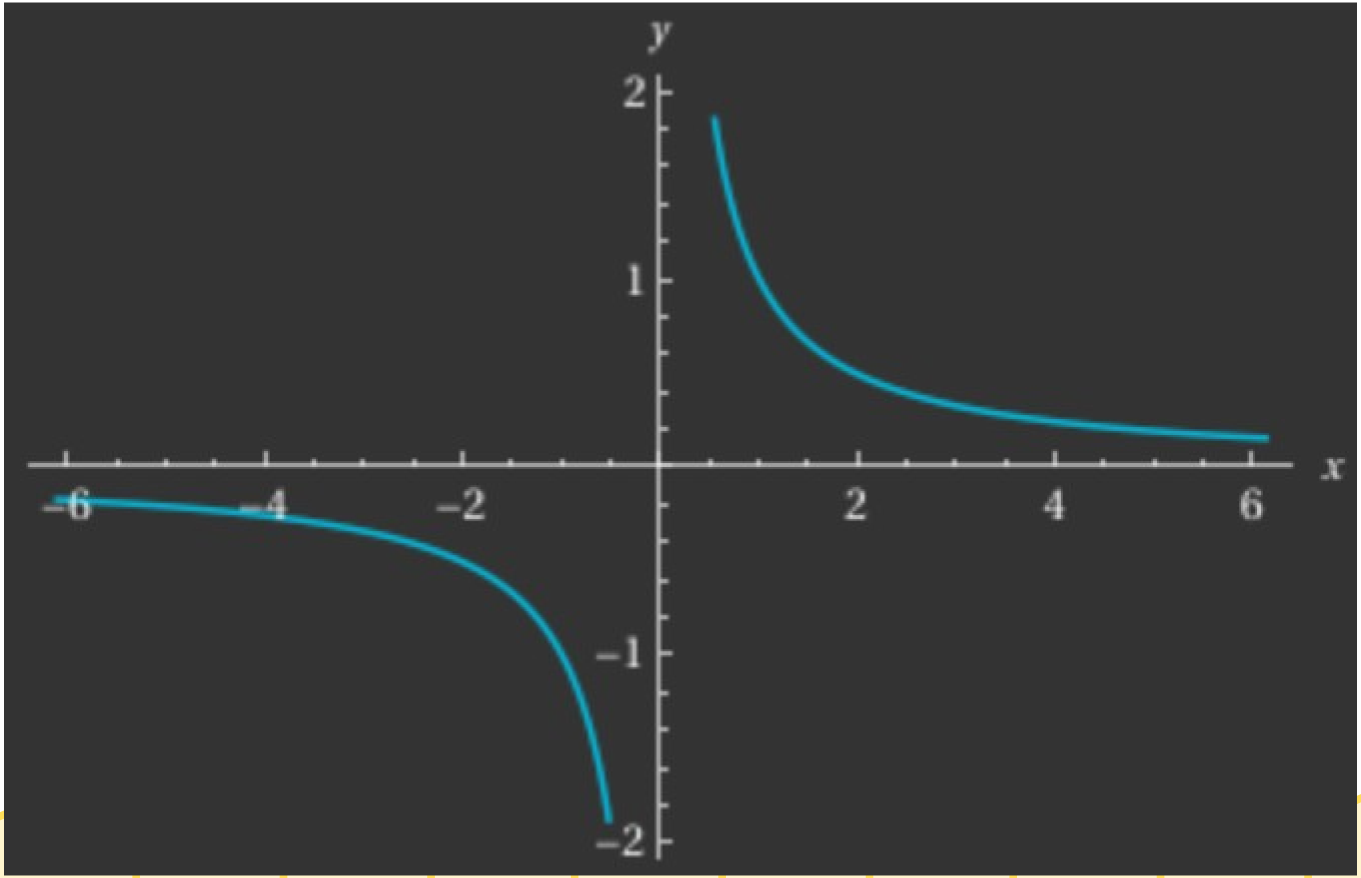
CSE548 Spring 2026
jedimaestro@asu.edu

https://www.cs.miami.edu/home/burt/learning/Csc688.012/rijndael/rijndael_doc_V2.pdf


ByteSub
ShiftRow
MixColumn
AddRoundKey

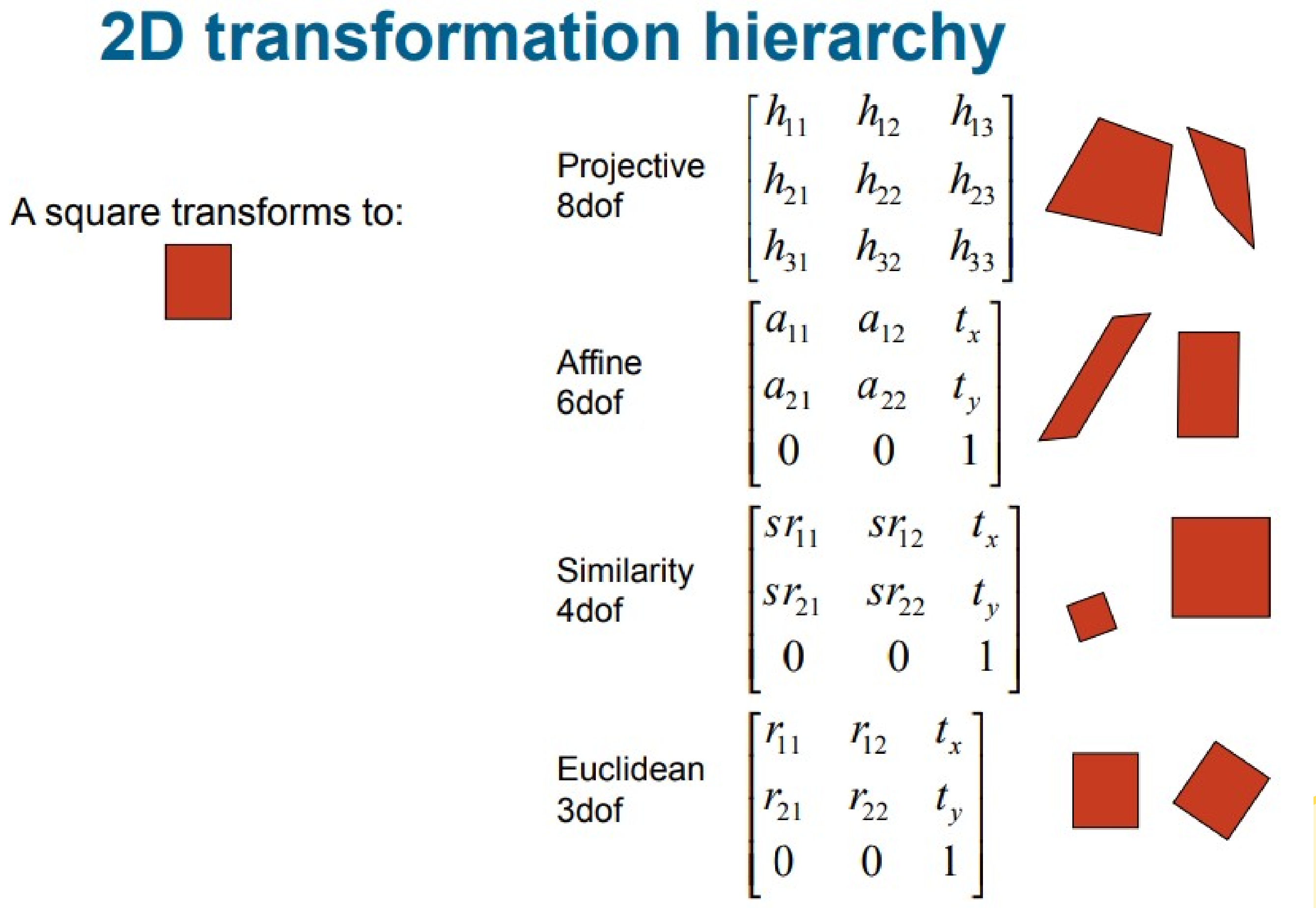
ByteSub gives non-linearity...

f(x) = 1/x



Affine transformation

https://math.stackexchange.com/questions/2717306/math-background-for-approximating-a-projective-transformation-by-an-affine-trans



2D transformation hierarchy

A square transforms to:

Projective
8dof

$$\begin{bmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \\ h_{31} & h_{32} & h_{33} \end{bmatrix}$$

Affine
6dof

$$\begin{bmatrix} a_{11} & a_{12} & t_x \\ a_{21} & a_{22} & t_y \\ 0 & 0 & 1 \end{bmatrix}$$

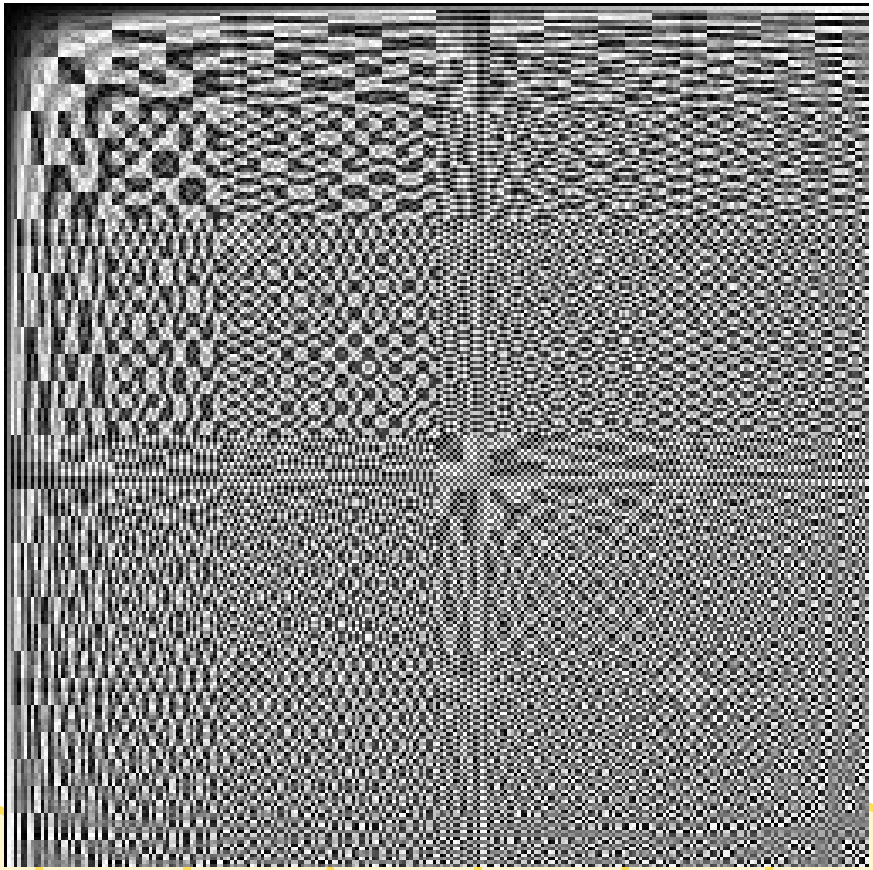
Similarity
4dof

$$\begin{bmatrix} sr_{11} & sr_{12} & t_x \\ sr_{21} & sr_{22} & t_y \\ 0 & 0 & 1 \end{bmatrix}$$

Euclidean
3dof

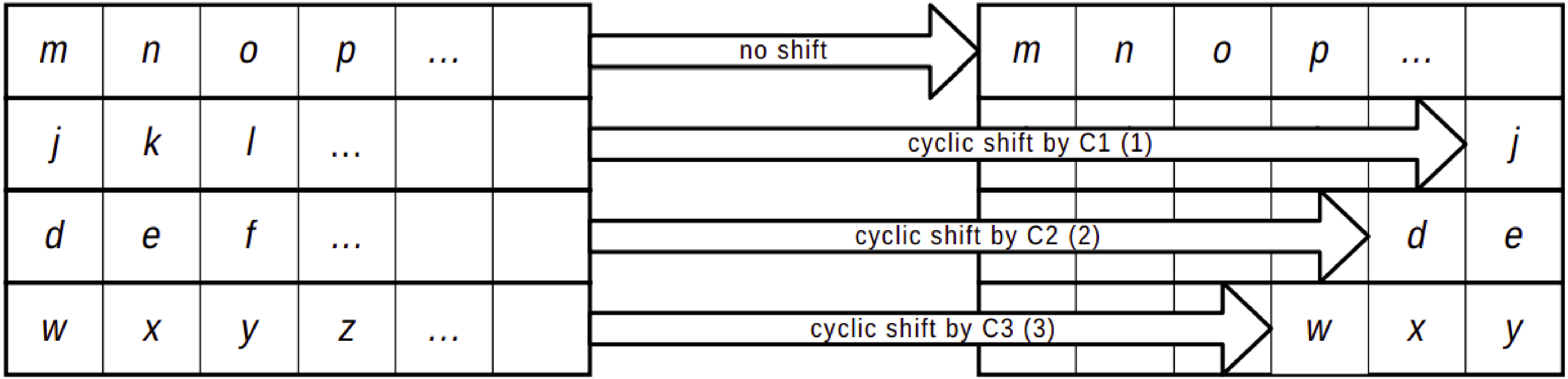
$$\begin{bmatrix} r_{11} & r_{12} & t_x \\ r_{21} & r_{22} & t_y \\ 0 & 0 & 1 \end{bmatrix}$$

https://www.cs.uaf.edu/2015/spring/cs463/lecture/03_23_AES.html



ShiftRow and MixColumn give diffusion...

ShiftRow



m	*n*	*o*	*p*	…	
j	*k*	*l*	…		
d	*e*	*f*	…		
w	*x*	*y*	*z*	…	

no shift

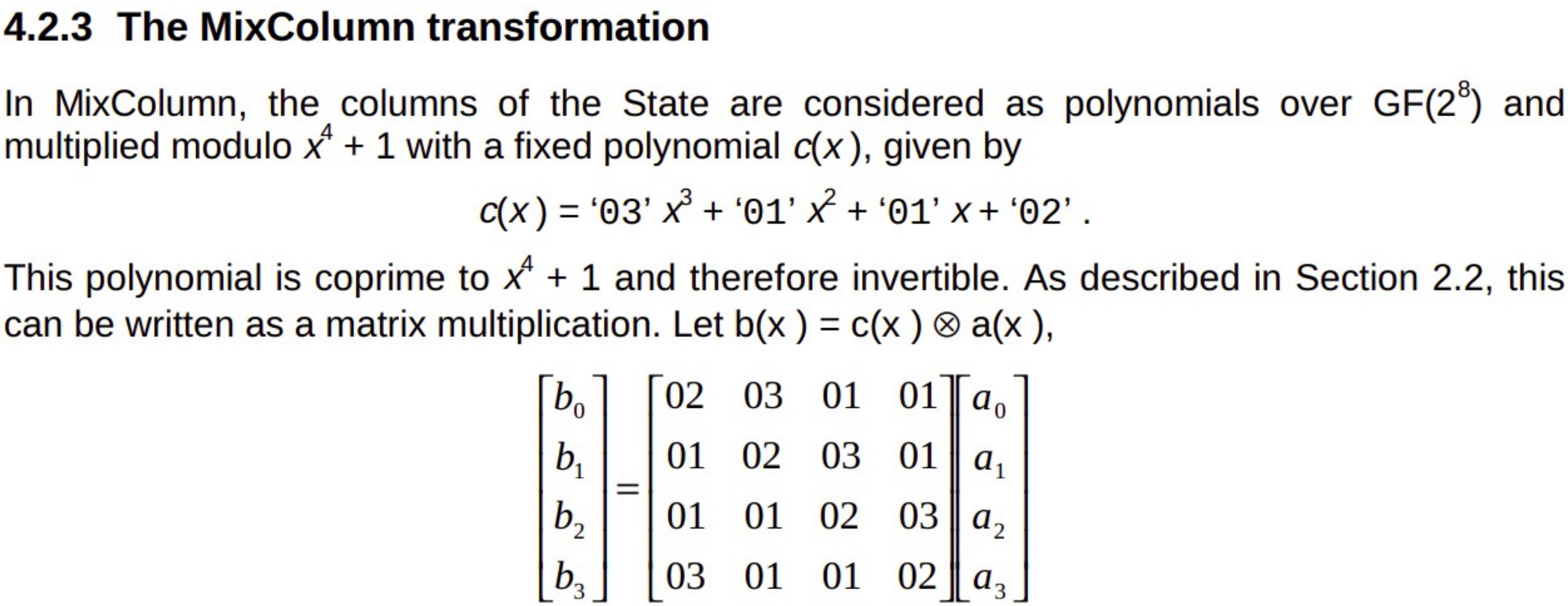
cyclic shift by C1 (1)

cyclic shift by C2 (2)

cyclic shift by C3 (3)

m	*n*	*o*	*p*	…	
					j
				d	*e*
			w	*x*	*y*

MixColumn



4.2.3 The MixColumn transformation

In MixColumn, the columns of the State are considered as polynomials over GF(2^8) and multiplied modulo $x^4 + 1$ with a fixed polynomial $c(x)$, given by

$$c(x) = \text{‘03’}\, x^3 + \text{‘01’}\, x^2 + \text{‘01’}\, x + \text{‘02’}\ .$$

This polynomial is coprime to $x^4 + 1$ and therefore invertible. As described in Section 2.2, this can be written as a matrix multiplication. Let $b(x) = c(x) \otimes a(x)$,

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

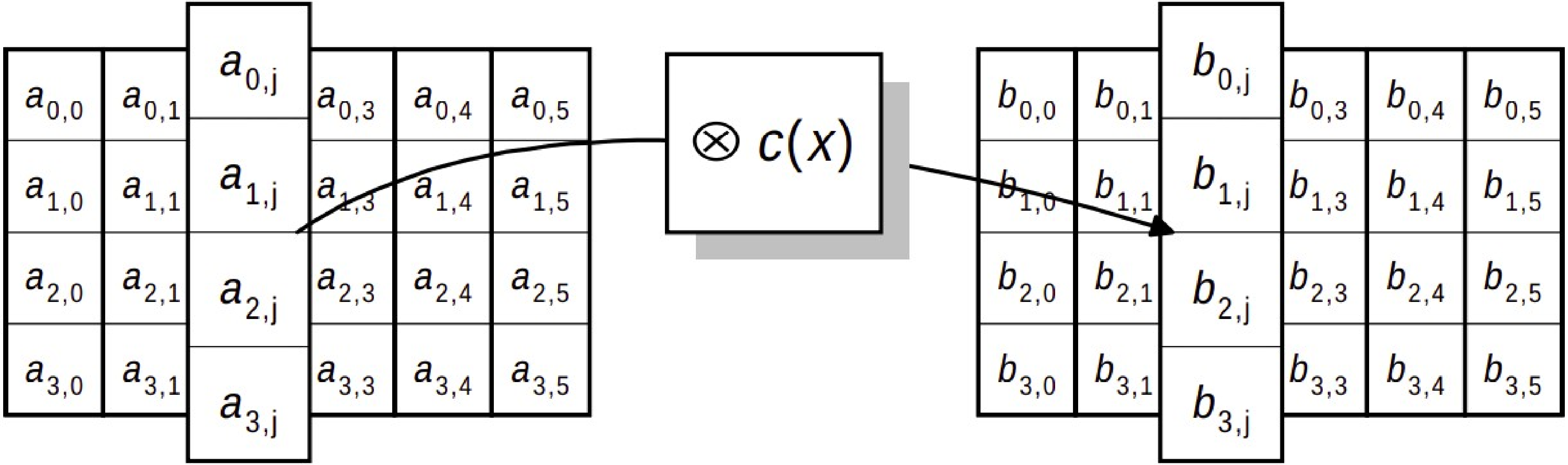

$a_{0,0}$ $a_{0,1}$ $a_{0,j}$ $a_{0,3}$ $a_{0,4}$ $a_{0,5}$
$a_{1,0}$ $a_{1,1}$ $a_{1,j}$ $a_{1,3}$ $a_{1,4}$ $a_{1,5}$
$a_{2,0}$ $a_{2,1}$ $a_{2,j}$ $a_{2,3}$ $a_{2,4}$ $a_{2,5}$
$a_{3,0}$ $a_{3,1}$ $a_{3,j}$ $a_{3,3}$ $a_{3,4}$ $a_{3,5}$
$\otimes\ c(x)$
$b_{0,0}$ $b_{0,1}$ $b_{0,j}$ $b_{0,3}$ $b_{0,4}$ $b_{0,5}$
$b_{1,0}$ $b_{1,1}$ $b_{1,j}$ $b_{1,3}$ $b_{1,4}$ $b_{1,5}$
$b_{2,0}$ $b_{2,1}$ $b_{2,j}$ $b_{2,3}$ $b_{2,4}$ $b_{2,5}$
$b_{3,0}$ $b_{3,1}$ $b_{3,j}$ $b_{3,3}$ $b_{3,4}$ $b_{3,5}$

Figure 4: MixColumn operates on the columns of the State.

The inverse of MixColumn is similar to MixColumn. Every column is transformed by multiplying it with a specific multiplication polynomial $d(x)$, defined by

$$(\text{‘03’}\,x^3 + \text{‘01’}\,x^2 + \text{‘01’}\,x + \text{‘02’}) \otimes d(x) = \text{‘01’}\,.$$

It is given by:

$$d(x) = \text{‘0B’}\,x^3 + \text{‘0D’}\,x^2 + \text{‘09’}\,x + \text{‘0E’}\,.$$

AddRoundKey is a simple XOR on purpose...

8.6 Weak keys as in IDEA

The weak keys discussed in this subsection are keys that result in a block cipher mapping with detectable weaknesses. The best known case of weak keys are those of IDEA [Da95]. Typically, this weakness occurs for ciphers in which the non-linear operations depends on the actual key value. This is not the case for Rijndael, where keys are applied using the EXOR and all non-linearity is in the fixed S-box. In Rijndael, there is no restriction on key selection.