# AES

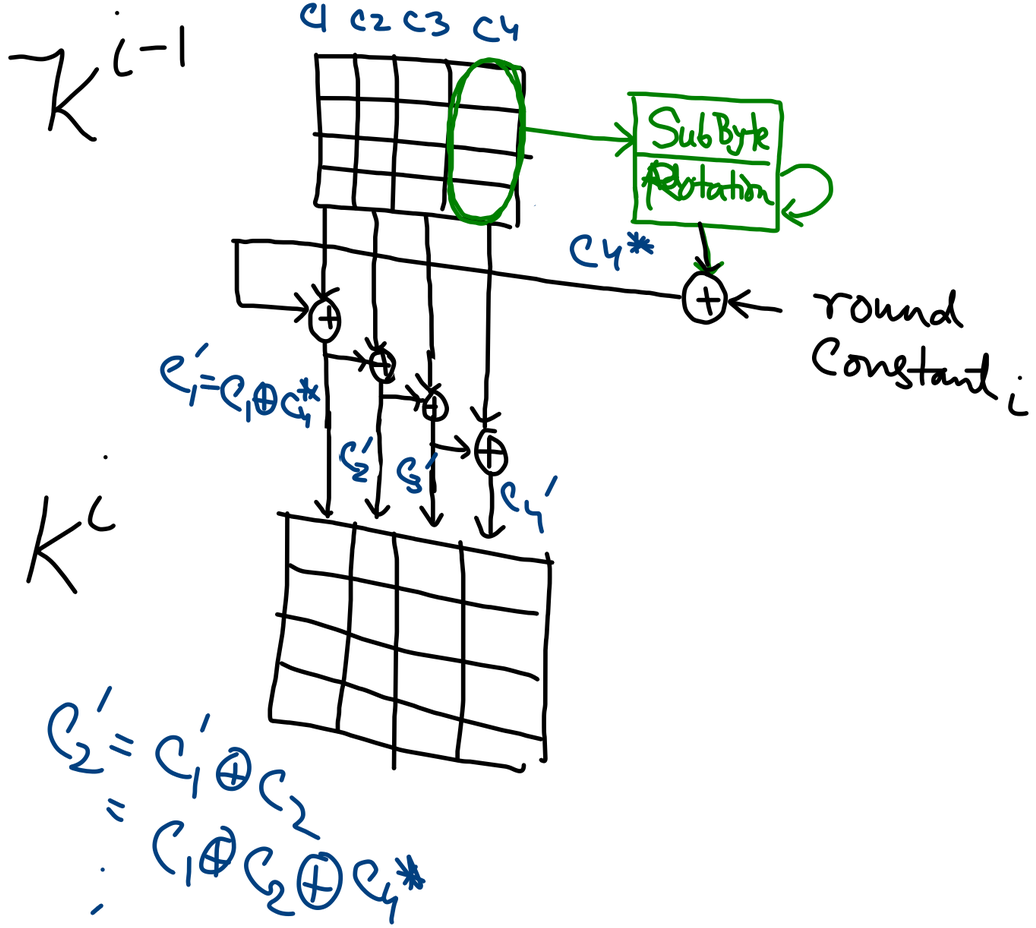
# AES

$K^0, K^1, \ldots, K^{10}$ → SubKey

$K^0 = K$, $K^i = KSF(K^{i-1})$, $i = 1$ to $(10)$

## Key Scheduling Func (KSF)

{ Sub-Key Size → 128-bits




## Observation

- Non-linearity is induced in one-column only.
- round constant$_i$ is different for each round.
- KSF is invertible

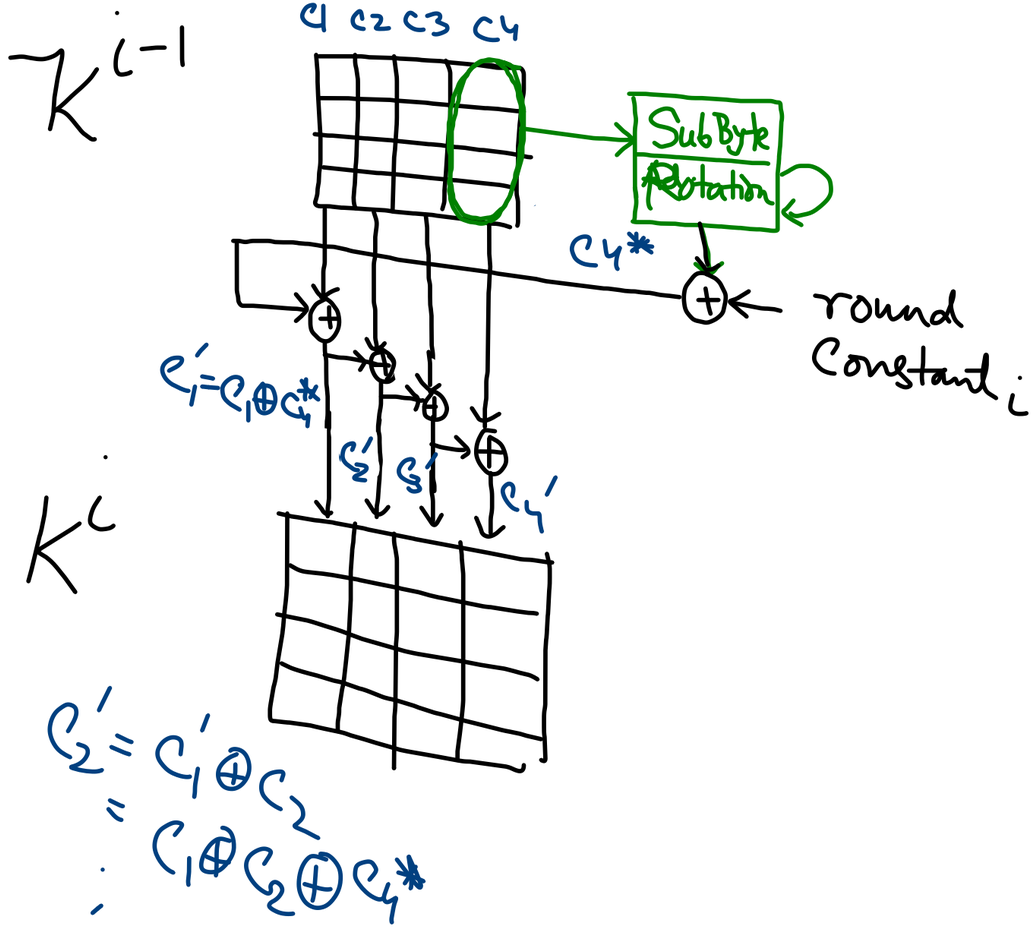
# AES

$K^0, K^1, \ldots, K^{10}$ → SubKey

$K^0 = K$, $K^i = KSF(K^{i-1})$, $i = 1$ to $(10)$

## Key Scheduling Func (KSF)

{ Sub-key Size → 128-bits




## KSF is invertible

$c_2' = c_1 \oplus c_2$
$c_3' = c_2' \oplus c_3$
$c_4' = c_3' \oplus c_4$
$c_1' = c_1 \oplus c_4^*$

$c_2 = c_1' \oplus c_2'$
$c_3 = c_3' \oplus c_2'$
$c_4 = c_3' \oplus c_4'$
$c_1 = c_1' \oplus c_4^*$

# Rationale of Mix-Column Matrix

| | | | |
|---|---|---|---|
| 2 | 3 | 1 | 1 |
| 1 | 2 | 3 | 1 |
| 1 | 1 | 2 | 3 |
| 3 | 1 | 1 | 2 |

- MDS matrix
  (Maximum Distance Separable)
- No entry should be '0'
- Invertible

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_{n-1} \end{pmatrix} = \underbrace{M_0}_{\text{MDS}} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{n-1} \end{pmatrix}$$

At least 5 of the variables are non-zero : $(x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3)$

$(n+1) \rightarrow$ general.

↳ (branch number)

# Rationale of Mix-Column Matrix

| | | | |
|---|---|---|---|
| 2 | 3 | 1 | 1 |
| 1 | 2 | 3 | 1 |
| 1 | 1 | 2 | 3 |
| 3 | 1 | 1 | 2 |

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} = M \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

**Multiplying 2**

↳ 1 shift
1 XOR

**Multiplying 3**

↳ 1 shift
↳ 2 XOR

$$y_0 = \underbrace{2 \cdot x_0}_{\omega_0} \oplus 3 \cdot x_1 \oplus x_2 \oplus x_3$$

$2 \odot x_0$

$x \odot (a_0 x^7 \oplus a_1 x^6 \oplus \dots \oplus a_7)$

$= a_0 x^8 \oplus \underbrace{a_1 x^7 \oplus \dots \oplus a_7 x}$

If $msb(x_0) == 0$,
$\omega_0 = shift(x_0)$
else
$\omega_0 = shift(x_0) \oplus prim\text{-}poly$

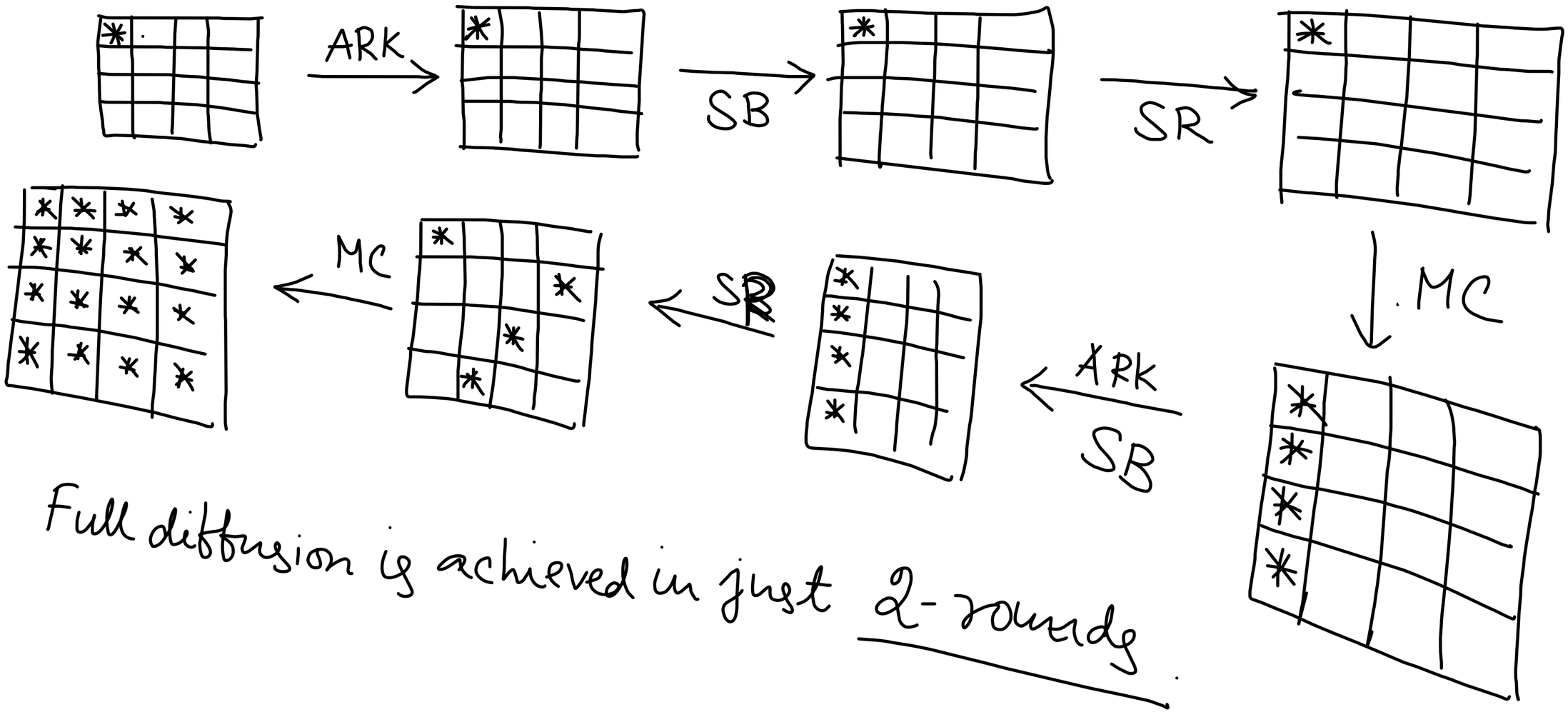
- MDS matrix
  (Maximum Distance Separable)
- No entry should be '0'
- Cost is minimized
  ↙
  (# linear operations)

# Why No Mix-Column in last Round?

| | Enc | Dec | Dec |
|---|---|---|---|
| | ARK | ARK | ARK |
| 1 | SB | SR | SB |
| | SR | SB | SR |
| | MC | ARk | MC |
| | ARk | MC | ARK |
| 2 | SB | SR | SB |
| | SR | SB | SR |
| | Mc | ARk | MC |
| | ARk | MC | ARK |
| 3 | SB | SR | SB |
| | SR | SB | SR |
| | ARK | ARk | ARK |

Underlying operations for encryption & decryption becomes identical

# Difference Propagation




Full diffusion is achieved in just 2-rounds.

# S-Box

S-Box : $\{0,1\}^8 \rightarrow \{0,1\}^8$

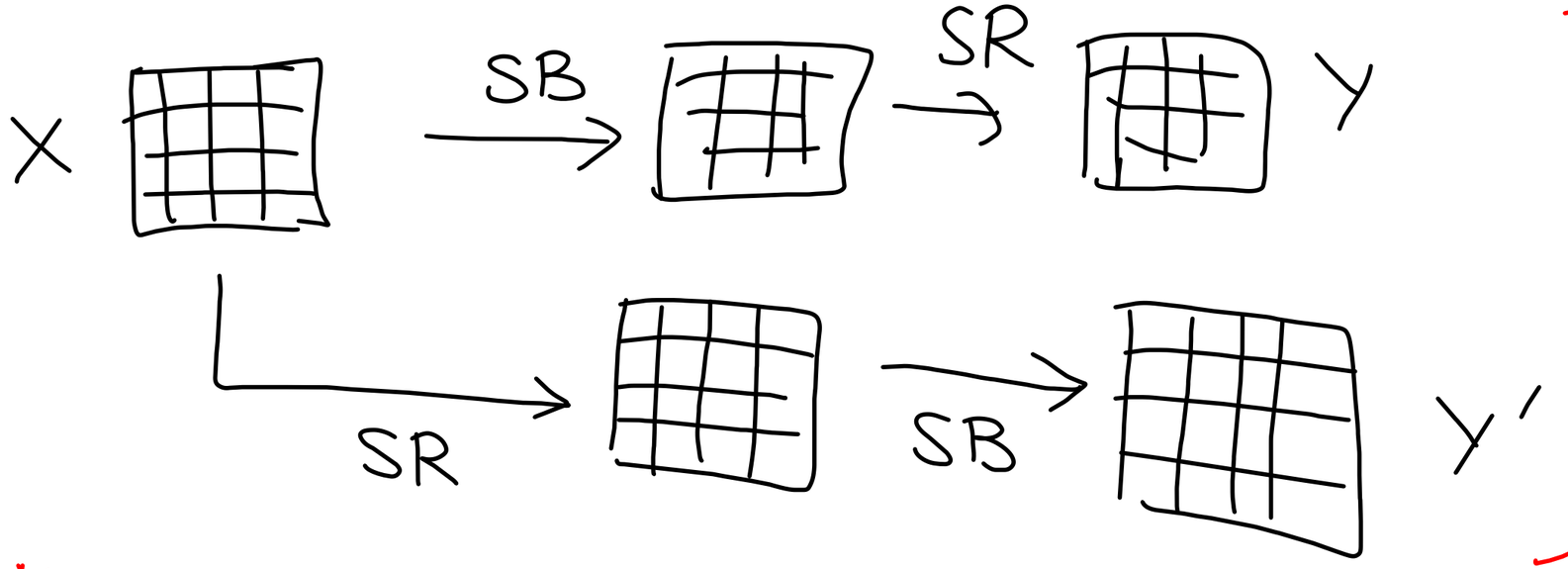
## SB(x)

- $z = x^{-1}$
- $y = A \cdot z \oplus c$ (High Non-linearity)

$$\begin{cases} x \in GF(2^8) \\ \text{Primpoly}: x^8 + x^4 + x^3 + x + 1 \end{cases}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_7 \end{pmatrix} = \begin{pmatrix} 10000111 \\ 11000011 \\ \vdots \\ 00001111 \end{pmatrix} \begin{pmatrix} z_0 \\ \vdots \\ z_7 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$\Rightarrow$ Additional good properties




Sub-Byte & Shift-Row is order independent

Mix Column & Add round key: Are they order independent ?

- $M \circ X \oplus k^i$
- $M \circ (X \oplus k^i)$
- $= M \circ X \oplus M \circ k^i$

MC → ARK: $-k^i$

ARK → MC: $(\overrightarrow{M \circ k^i})$