

AES (Advanced Encryption Standard)

- Rijndael (Vincent Rijmen
Joan Daemen)

- Block size: 128-bit

- Key-size: 128/192/256-bit

- SPN Structure

- $GF(2^8)$ - Primitive poly: $(x^8 + x^4 + x^3 + x + 1)$

AES-128
AES-192
AES-256

$$128 = 16 \times 8$$

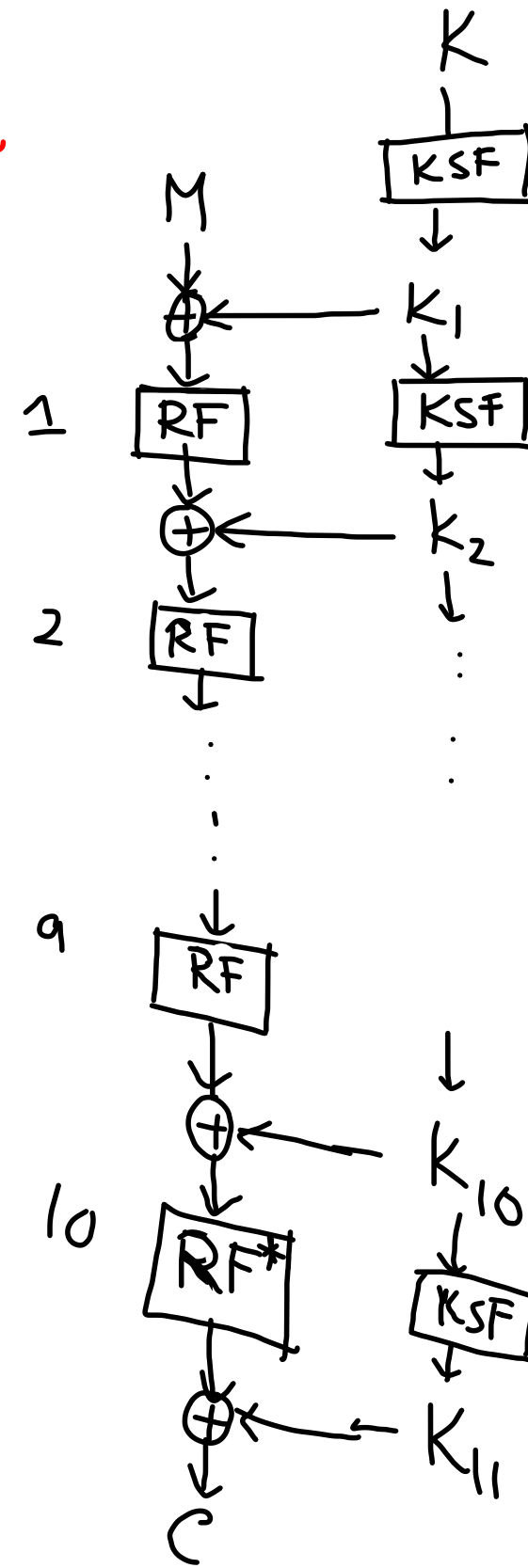
AES Specification

$M =$

$m_{0,0}$	$m_{1,0}$	$m_{2,0}$	$m_{3,0}$
$m_{0,1}$	$m_{1,1}$	$m_{2,1}$	$m_{3,1}$
$m_{0,2}$	$m_{1,2}$	$m_{2,2}$	$m_{3,2}$
$m_{0,3}$	$m_{1,3}$	$m_{2,3}$	$m_{3,3}$

Initial State

Overall Structure



AES-128

RF: Round Function

RF*: Round Function for last round

KSF: Key Scheduling Function

Round Function (RF)

- Sub Byte } Non-linear
- Shift Row } Linear
- Mix Column }

Round Function RF^*

- Sub-Byte
- Shift-Row

Sub-Byte Operation

S_{00}	S_{10}	S_{20}	S_{30}
S_{01}	S_{11}	S_{21}	S_{31}
S_{02}	S_{12}	S_{22}	S_{32}
S_{03}	S_{13}	S_{23}	S_{33}

Sub
Byte

S'_{00}	S'_{10}	S'_{20}	S'_{30}
S'_{01}	.	.	.
S'_{02}	.	.	.
S'_{03}	.	.	.

$SBox(00) = 63$
 $\downarrow$
 00000000
 $\downarrow$
 01100011

	0	1	...	F
0	63	.	...	-
1				
...				
F	1	1		

16X16

$$S'_{ij} = SBox(S_{ij})$$

SB(x)

- Compute x^{-1} in $GF(2^8)$. Let $z = x^{-1}$
- Perform the affine transformation:

→ (Non-linear)

x	00000000	...	11111111
$SBox(x)$			

SBox is a permutation of 8-bits.

{ Circular
Matrix

$$\begin{pmatrix} y_0 \\ \vdots \\ y_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ & & & & & & & \\ & & & & & & & \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} z_0 \\ \vdots \\ z_7 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad \text{--- (affine)}$$

Shift Row

S_{00}	S_{10}	S_{20}	S_{30}
S_{01}	S_{11}	S_{21}	S_{31}
S_{02}	S_{12}	S_{22}	S_{32}
S_{03}	S_{13}	S_{23}	S_{33}

→
SR

S_{00}	S_{10}	S_{20}	S_{30}	- Row 0
S_{11}	S_{21}	S_{31}	S_{01}	.
S_{22}	S_{32}	S_{02}	S_{12}	.
S_{33}	S_{03}	S_{13}	S_{23}	- Row 3

(i^{th} Row $\Rightarrow$ i -many left-shift)

Shift Row

S_{00}	S_{10}	S_{20}	S_{30}
S_{01}	S_{11}	S_{21}	S_{31}
S_{02}	S_{12}	S_{22}	S_{32}
S_{03}	S_{13}	S_{23}	S_{33}

→
SR

S_{00}	S_{10}	S_{20}	S_{30}	- Row 0
S_{11}	S_{21}	S_{31}	S_{01}	.
S_{22}	S_{32}	S_{02}	S_{12}	.
S_{33}	S_{03}	S_{13}	S_{23}	- Row 3

(i^{th} Row $\Rightarrow$ i -many left-shift)

Mix Column

S_{00}	S_{10}	S_{20}	S_{30}
S_{01}	S_{11}	S_{21}	S_{31}
S_{02}	S_{12}	S_{22}	S_{32}
S_{03}	S_{13}	S_{23}	S_{33}

MC →

elements from $GF(2^8)$

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

×

S_{00}	-	-	.
1	-	-	-
.			S_{33}

=

$2 \odot S_{00} \oplus 3 \odot S_{01} \oplus S_{02} \oplus S_{03}$			
$S_{00} \oplus 2 \odot S_{01} \oplus 3 \odot S_{02} \oplus S_{03}$			

Rationale of Mix-Column Matrix for AES

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

$\Rightarrow$ MDS matrix
 $\hookrightarrow$ (Maximum distance separable)

(Branch no: 5)

MSB=1

$$\begin{aligned} & x \odot (x^7 \oplus x^2) \\ &= x^8 \oplus x^3 \\ &= (x^4 \oplus x^3 \oplus x \oplus 1) \oplus x^3 \\ & \text{1 Shift + 1 XOR} \end{aligned}$$

MSB=0

$$\begin{aligned} & x \odot (x^5 \oplus x) \\ &= x^6 \oplus x^2 \\ & \text{Shift} \end{aligned}$$

Multiplication
by 2

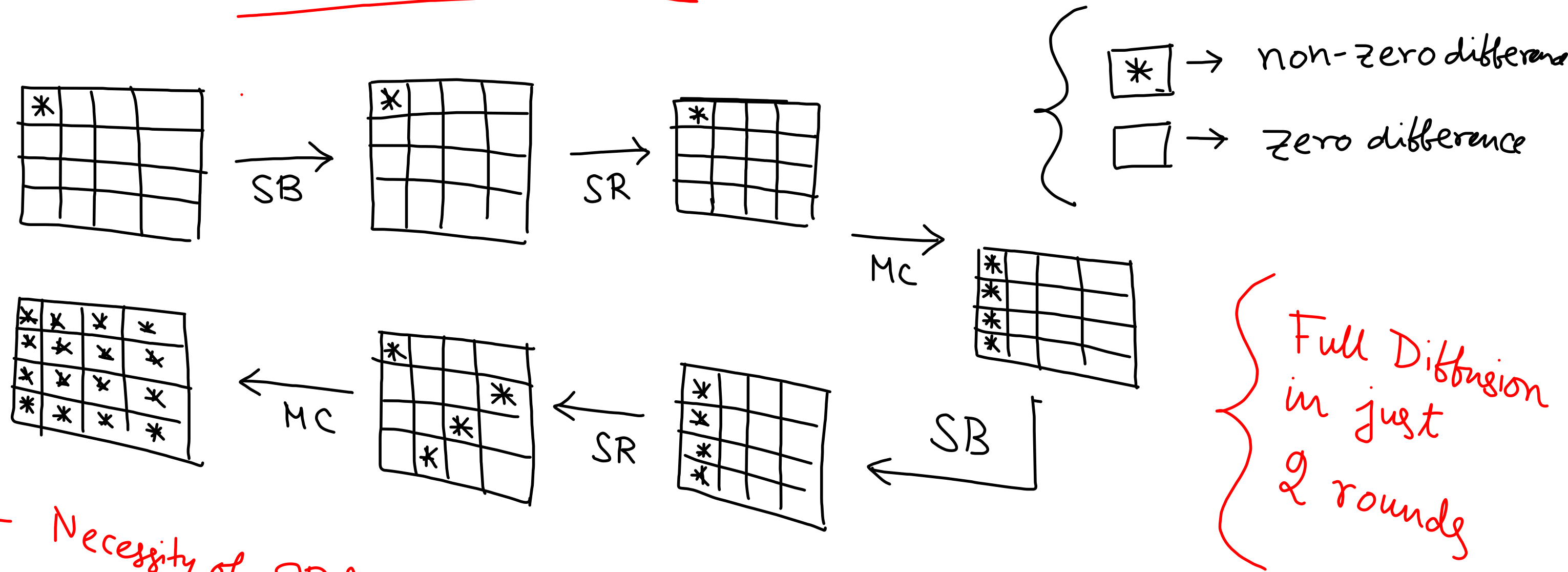
Mult by 3
 - 1S + 1XOR
 - 1S + 2XOR

$$y_{n \times 1} = M_{n \times n} \cdot x_{n \times 1}$$

of non-zero values
 $x_1 + \dots + x_n + y_1 + \dots + y_n \geq n+1$,
 if $x \neq 0^n$

int addition.
 Branch no. = (n+1)

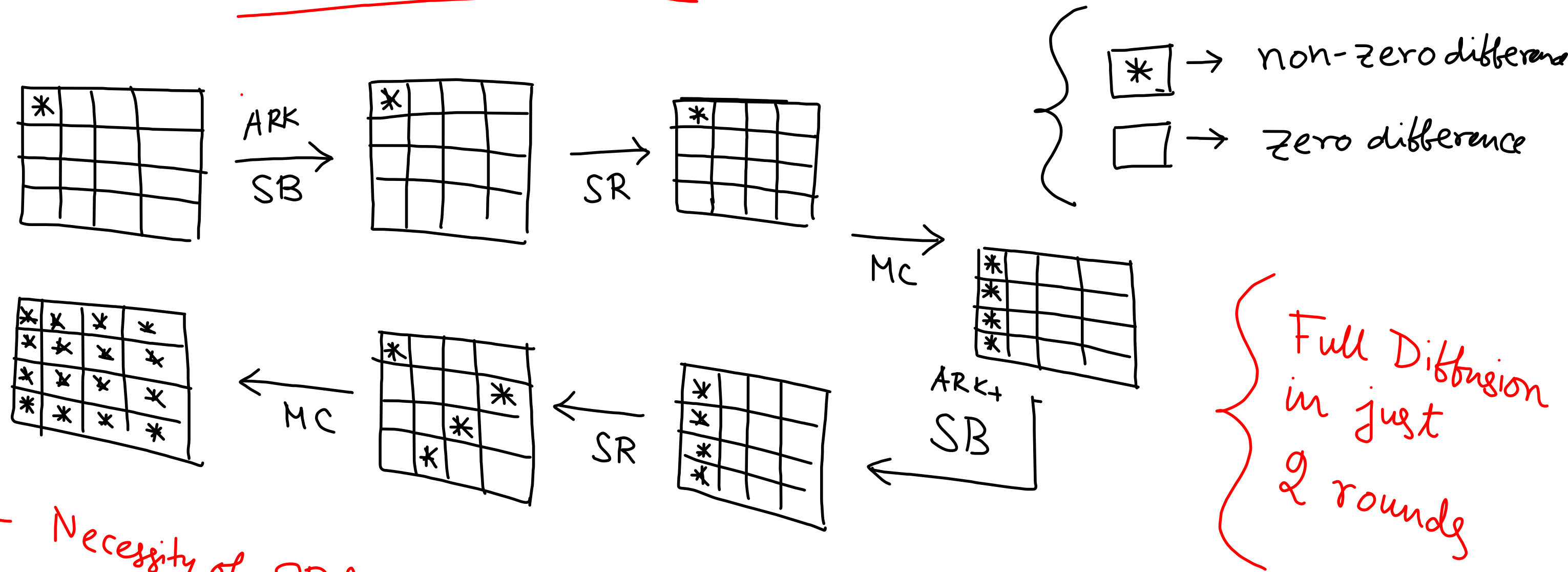
Diffusion in AES



- Necessity of SR & MC in diffusion

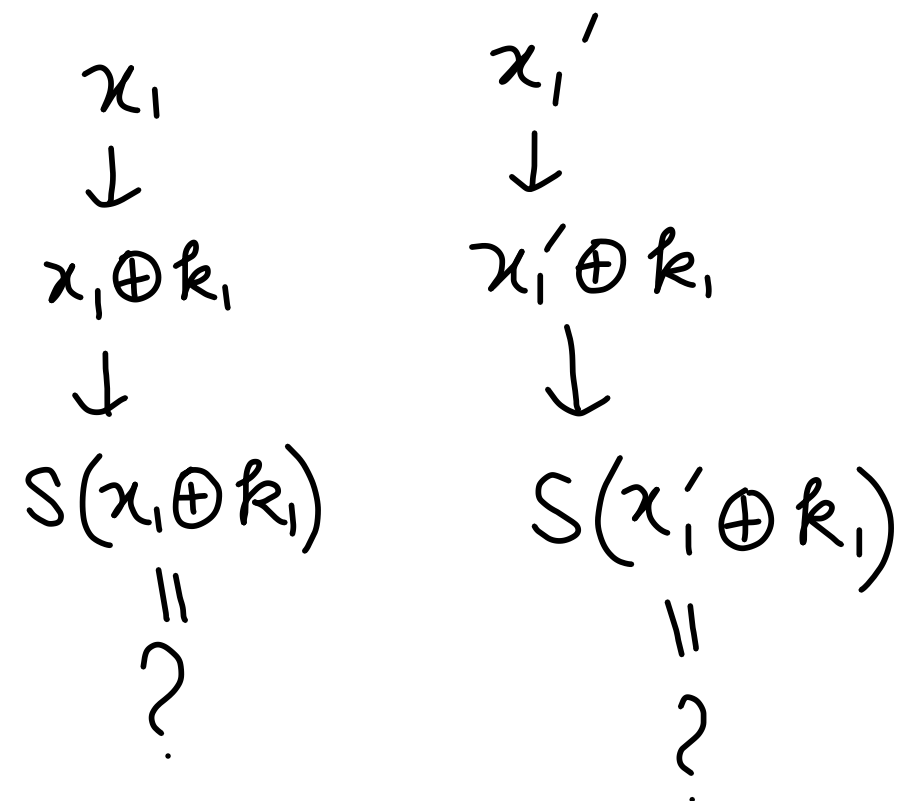
Full Diffusion
in just
2 rounds

Diffusion in AES

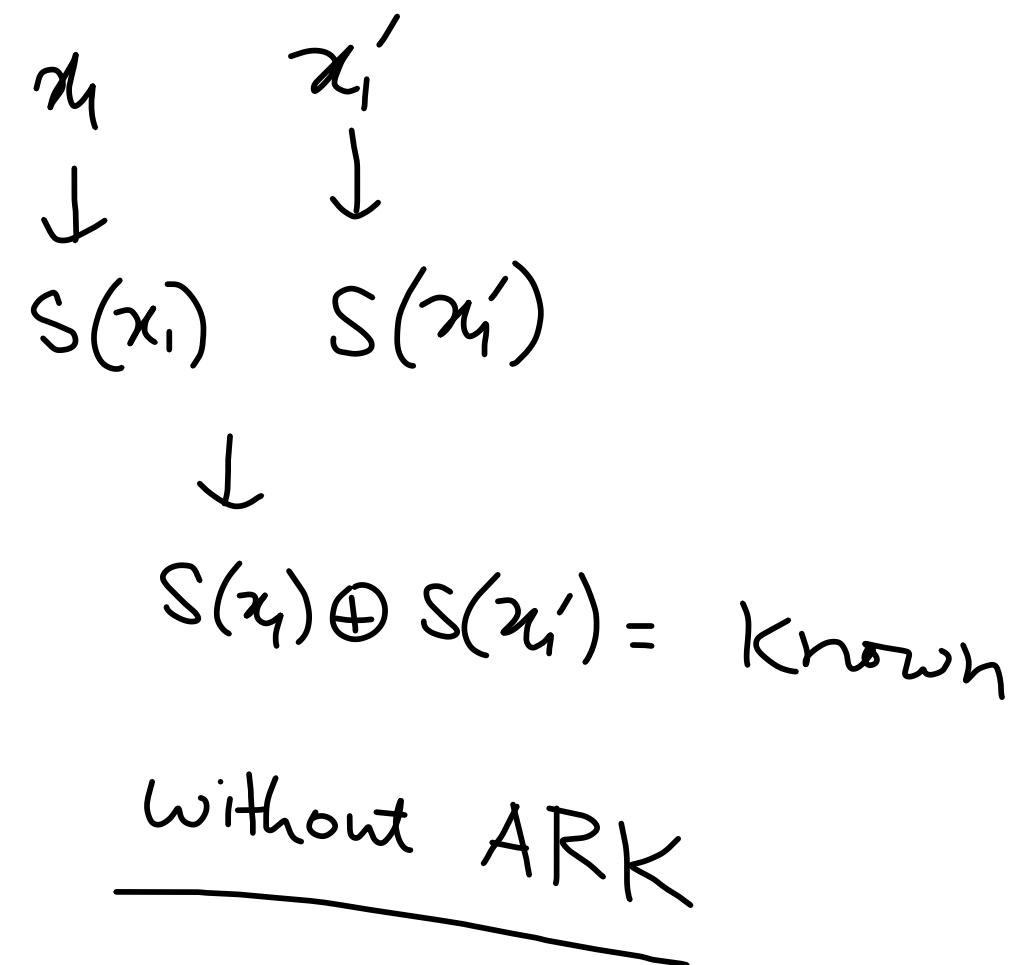


- Necessity of SR & MC in diffusion

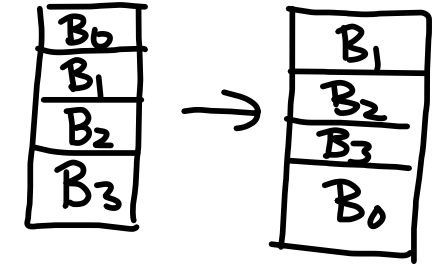
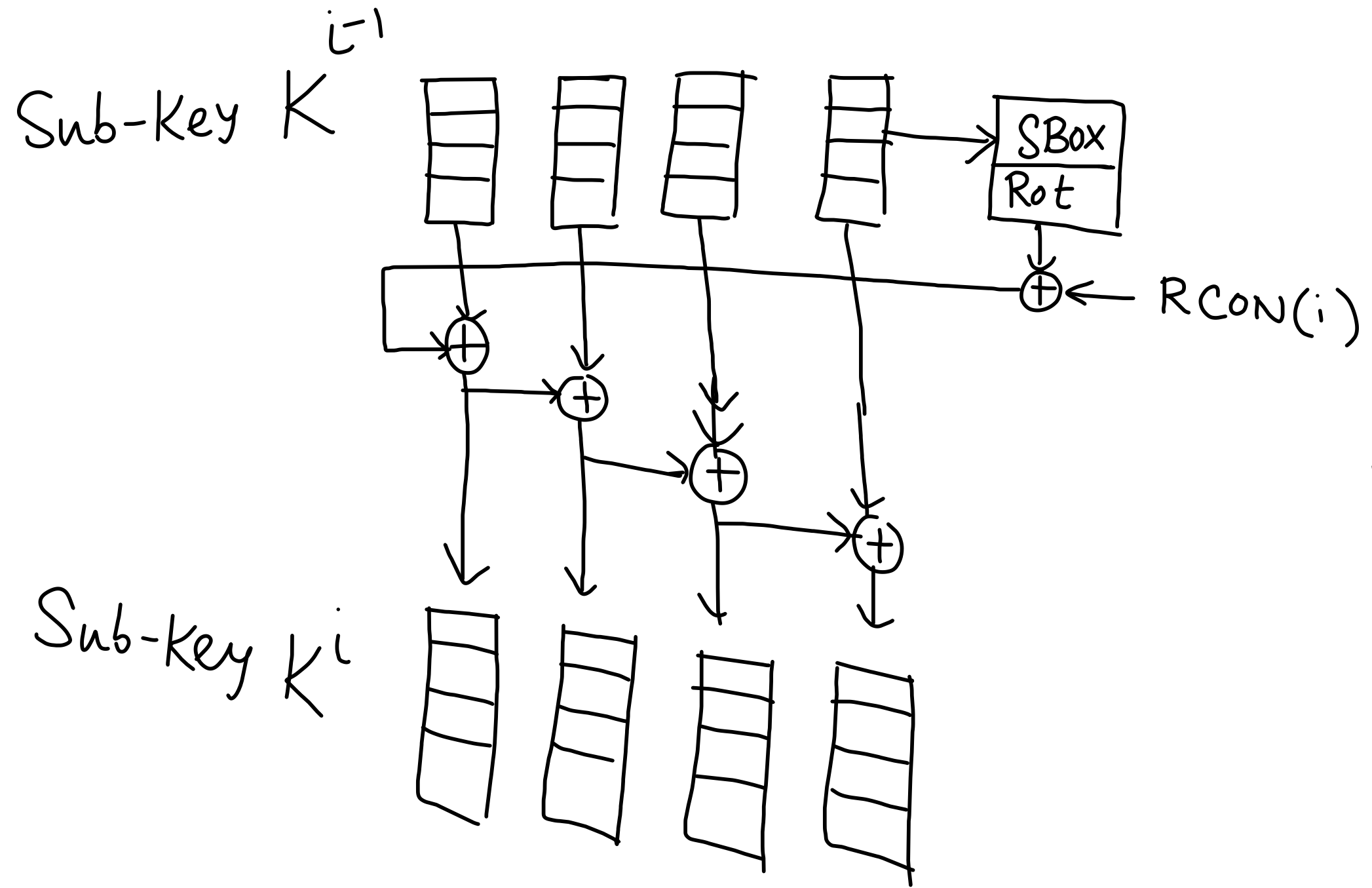
Full Diffusion
in just
2 rounds



With ARK



Key Scheduling Function



$K^0 = K$ $\xrightarrow{\text{master-key of AES}}$

Why Discard the last Mix Column?

AES-ENC (3 round)		<u>AES-DEC</u>	
ARK	 Structurally Same	ARK	ARK
SB		SB	SR
SR		SR	SB
MC		MC	ARK
ARK		ARK	MC
SB		SB	SR
SR		SR	SB
MC		MC	ARK
ARK		ARK	MC
SB		SB	SR
SR		SR	SB
ARK		ARK	ARK

$$\begin{cases}
 S \xrightarrow{SB} S' \xrightarrow{SR} S'' \\
 S \xrightarrow{SR} S''' \xrightarrow{SB} S^{IV}
 \end{cases}$$

$$S'' = S^{IV}$$

$\{ SB \ \& \ SR \rightarrow$
 order remains
 invariant

ARK $\rightarrow$ MC: $M \cdot (S \oplus K)$
 MC $\rightarrow$ ARK: $K \oplus M \cdot S$
 Subkey $\rightarrow M \cdot K_1, M \cdot K_2, \dots$
 then MC & ARK remains invariant