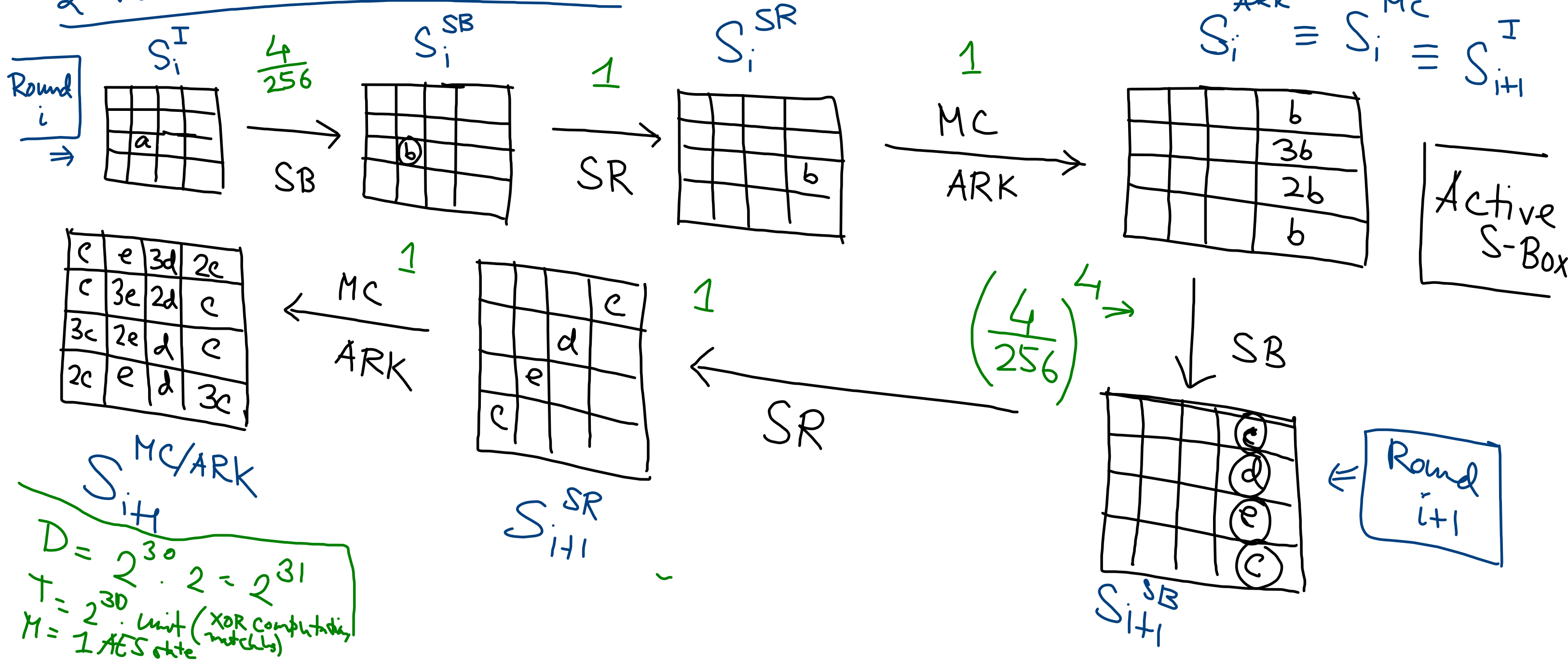


Differential Cryptanalysis on AES (reduced round)

$$\text{Diff Prob} = \left(\frac{4}{256}\right)^5 = \frac{1}{2^{30}}$$

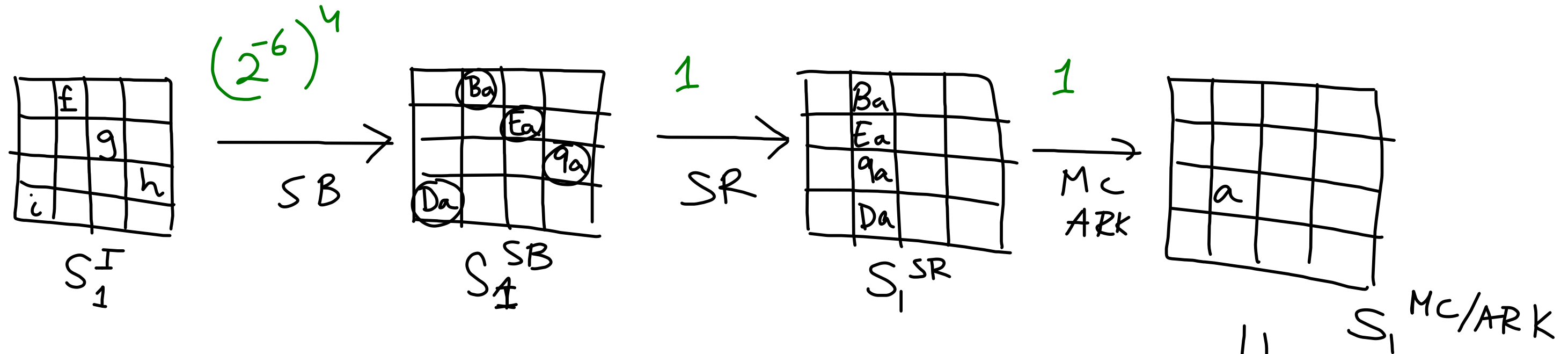
2-round differential Trail



$D = 2^{30}$
 $T = 2^{30} \cdot 2 = 2^{31}$
 $M = 2^{30} \cdot \text{Unit (XOR computation matches)}$
 1 AES state

3-Round Differential Trail

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} _ \\ _ \\ _ \\ _ \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ a \\ 0 \end{pmatrix}$$



$$(2^{-6})^9 = 2^{-54}$$

$D = 2^{54} \cdot 2 = 2^{55}$
 $T = 2^{54}$
 $M = 1$ AES state
 XOR + Matching

Distinguishing

c	e	3d	2c
c	3e	2d	c
3c	2e	d	e
2c	e	d	3e

S_3^{Mc}

Operation: $2R$ (2 Rounds) with differential $(2^{-6})^5$

	a		

S_2^I

Active S-Box = 9

Diff Trail = $(2^{-6})^9$

Key Recovery Attack

(4 Round AES)

2^{55} pairs
↓

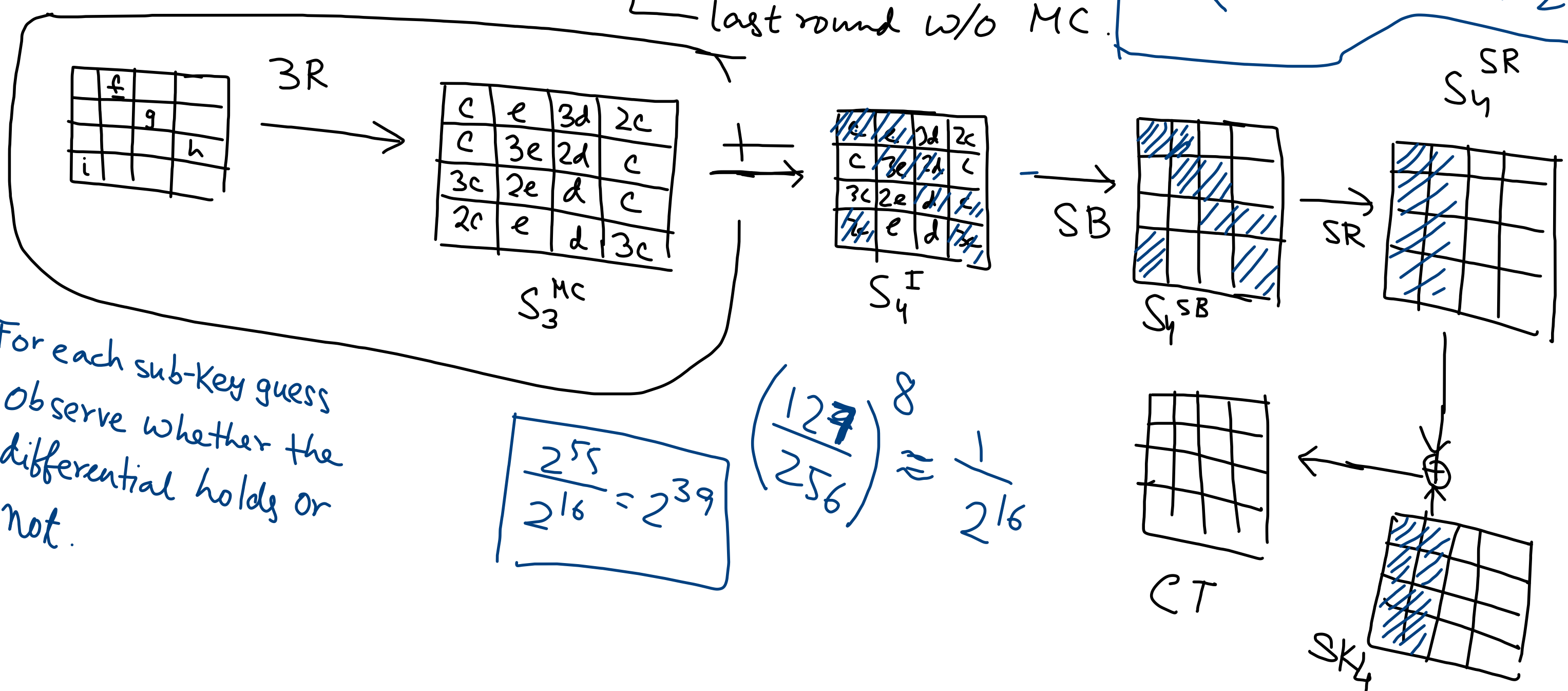
last round w/o MC.

Complexity

$$D = 2^{55}$$

$$T = 2^{55} \cdot 2^{64} \Rightarrow 2^{39} \cdot 2^{64}$$

$$M = \frac{2^{55}}{2^{64}} \Rightarrow 2^{39} \cdot 2^{64} = 2^{103}$$



For each sub-key guess
observe whether the
differential holds or
not.

$$\frac{2^{55}}{2^{16}} = 2^{39}$$

$$\left(\frac{127}{256} \right)^8 \approx \frac{1}{2^{16}}$$

When can you say AES is secure

- r -Round AES $\Rightarrow$ # active S-box: N_S

- Best differential attack = $\left(\frac{1}{2^6}\right)^{N_S}$

$\Downarrow$

- How many P/T queries = $(2^6)^{N_S} \cdot 2$

- P/T queries possible = 2^{128}

$$\left\{ \begin{array}{l} (2^6)^{N_S} \cdot 2 \leq 2^{128} \\ N_S \geq 22 \end{array} \right. \Rightarrow \text{I cannot mount differential attack}$$

MILP

$\hookrightarrow$ Mixed integer
linear programming

Wide Trail Strategy

$\hookrightarrow$ AES 4-R

$$N_S \geq 25$$

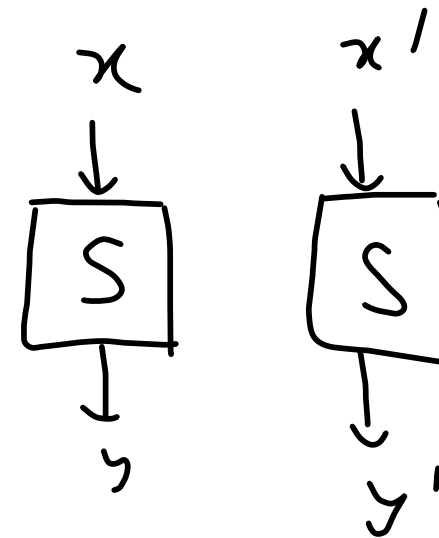
$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{bmatrix} 0 \\ 0 \\ b \\ 0 \end{bmatrix} = \begin{bmatrix} b \\ 3b \\ 2b \\ b \end{bmatrix}$$

MC $\Rightarrow$

MC $\swarrow$

$$256 \left\{ \begin{array}{c|c} 0 & 0 \rightarrow 0 \\ \hline 1 & 1 \rightarrow 0 \\ \vdots & \vdots \\ \hline 2^{24} & 2^{24}-1 \rightarrow 0 \end{array} \right.$$

$$\frac{0}{1} \bigg| \frac{i}{10i} \rightarrow \frac{j}{j'}$$



Δx may be same
 $\downarrow$
 Δy may not be same

(*) AES DDT-table

For all $\Delta_{in} \neq 0$

- there is exactly one Δ_{out} with "4"
- there is exactly 126 Δ_{out} with "2"
- ... 129 Δ_{out} with "0"

$\Delta_{in} \backslash \Delta_{out}$	0	1	...	2^8-1
0	256	0	...	0
1	1	1	...	1
...	...	...	...	...
$2^{24}-1$	...	...	...	...

$$(256 \times 256) \Downarrow (2^8 \times 2^8)$$

Properties of DDT

- All values in DDT is even.
- All row sum = Column sum = 2^n

S-Box
↳ Size n
(even)