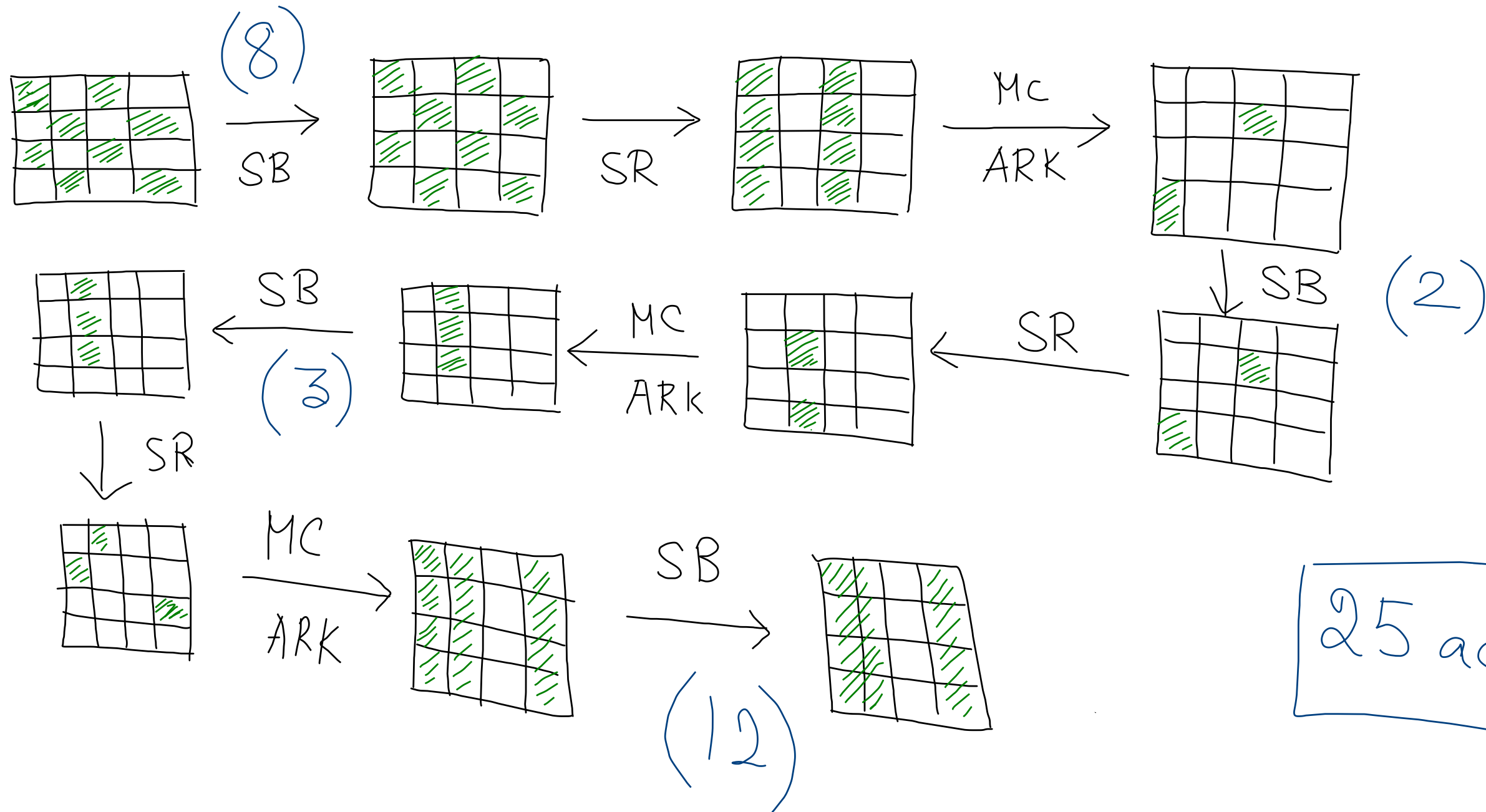


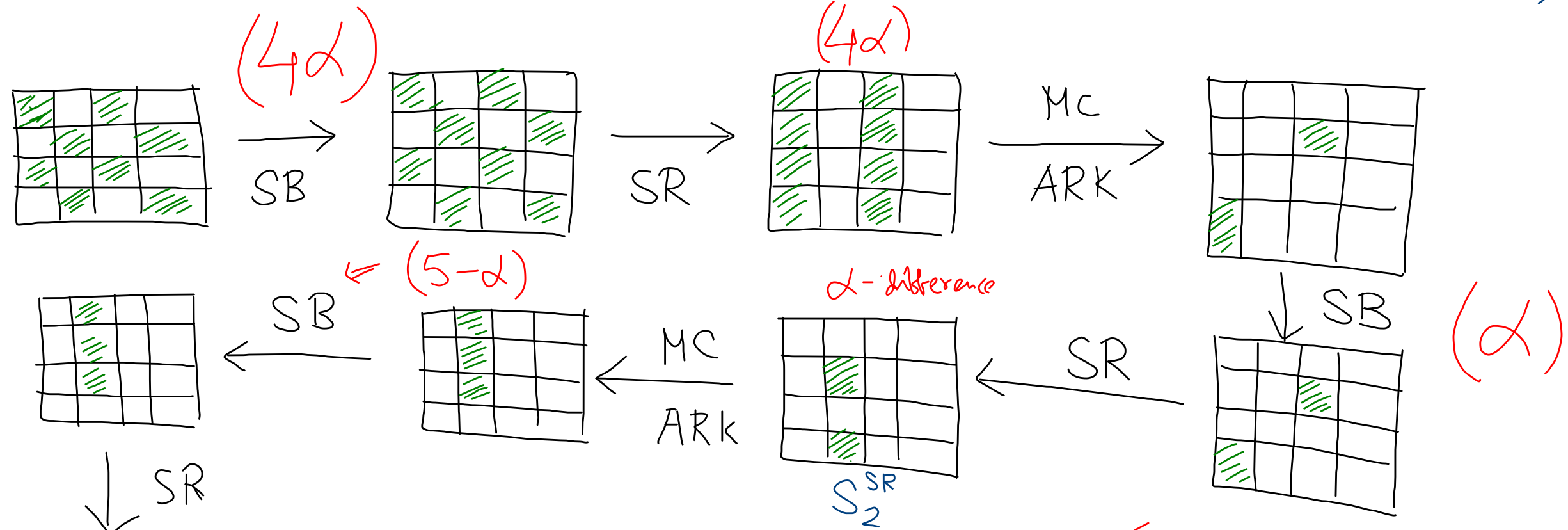
Wide-Trail Strategy

(4round AES has at least 25 active S-Box)



Wide-Trail Strategy

(4round AES has at least 25 active S-Box)

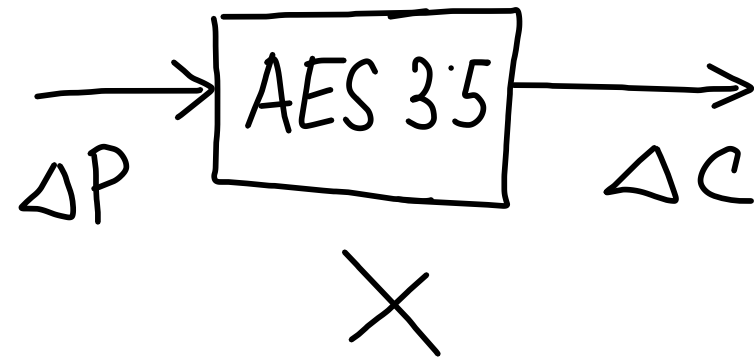


S_2^{SR} → difference in one column only
 #active S-Boxes ≥ 25

$$\begin{aligned} \text{\# active S-boxes} &\geq 4\alpha + \alpha + (5-\alpha) \\ &\geq 25 + 4(5-\alpha) \end{aligned} \quad \boxed{1 \leq \alpha \leq 4}$$

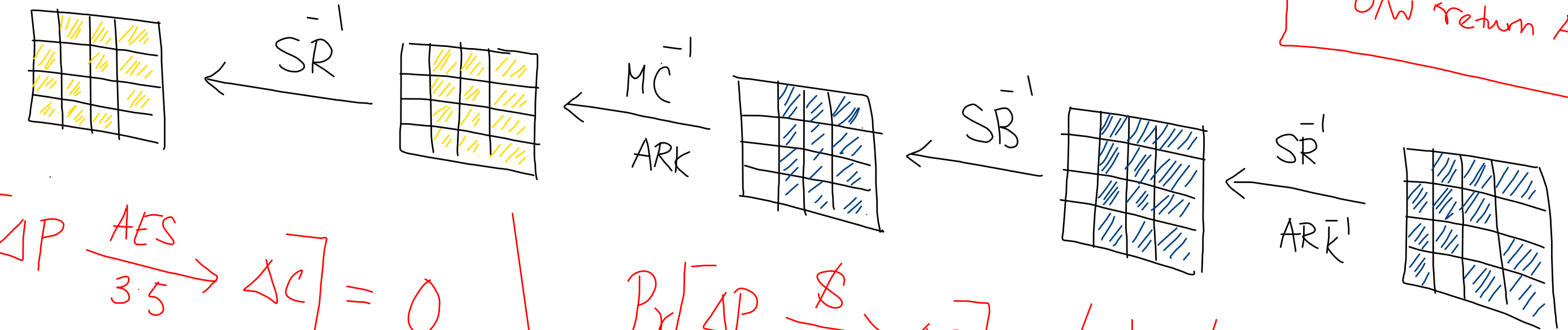
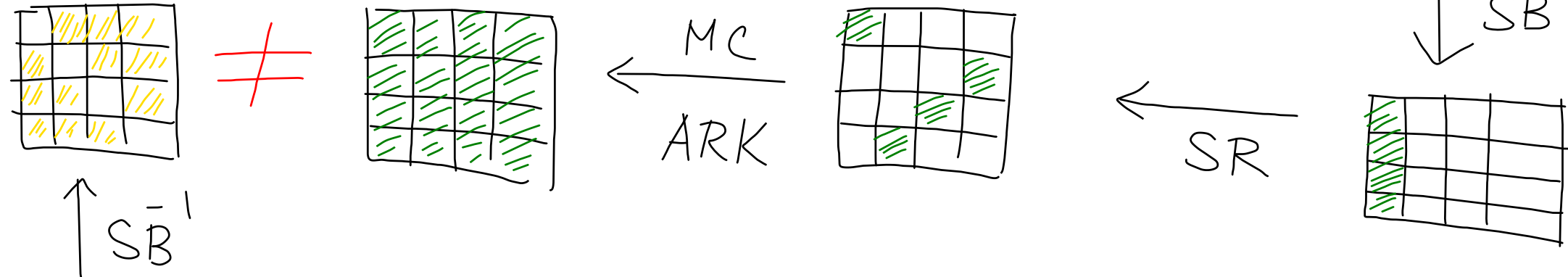
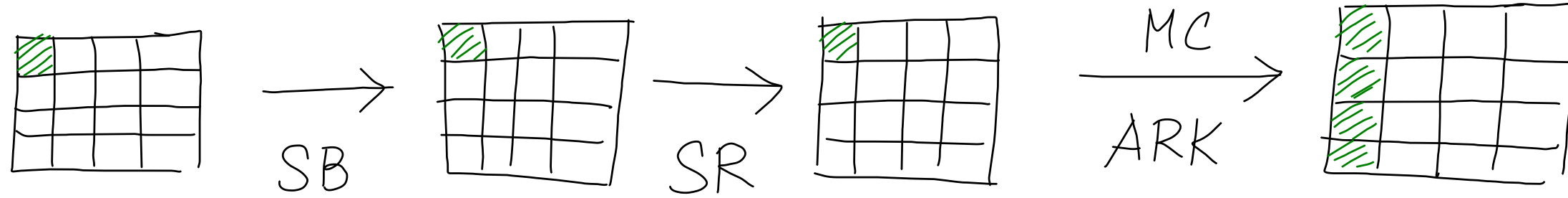
Impossible Differential Attacks

- No differential is possible for a fixed I/P difference & O/P difference.



Impossible Differential for AES-3.5

ΔP



Dist Attack

- Query 2^{32} many ΔP -pairs
- If any of them achieves ΔC -diff return $\$$
- O/w return AES-3.5

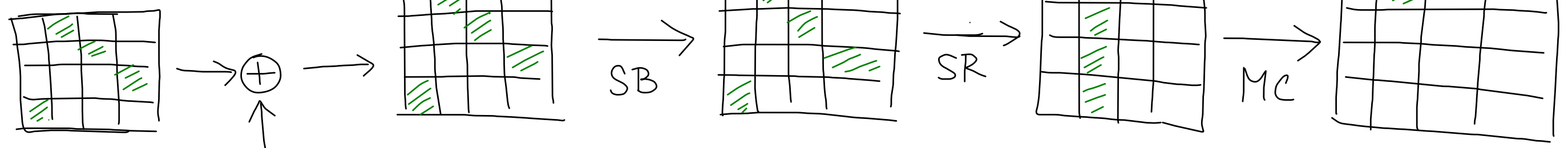
$$\Pr[\Delta P \xrightarrow[3.5]{AES} \Delta C] = 0$$

$$\Pr[\Delta P \xrightarrow{\$} \Delta C] = \left(\frac{1}{2^8}\right)^4 = \frac{1}{2^{32}}$$

ΔC

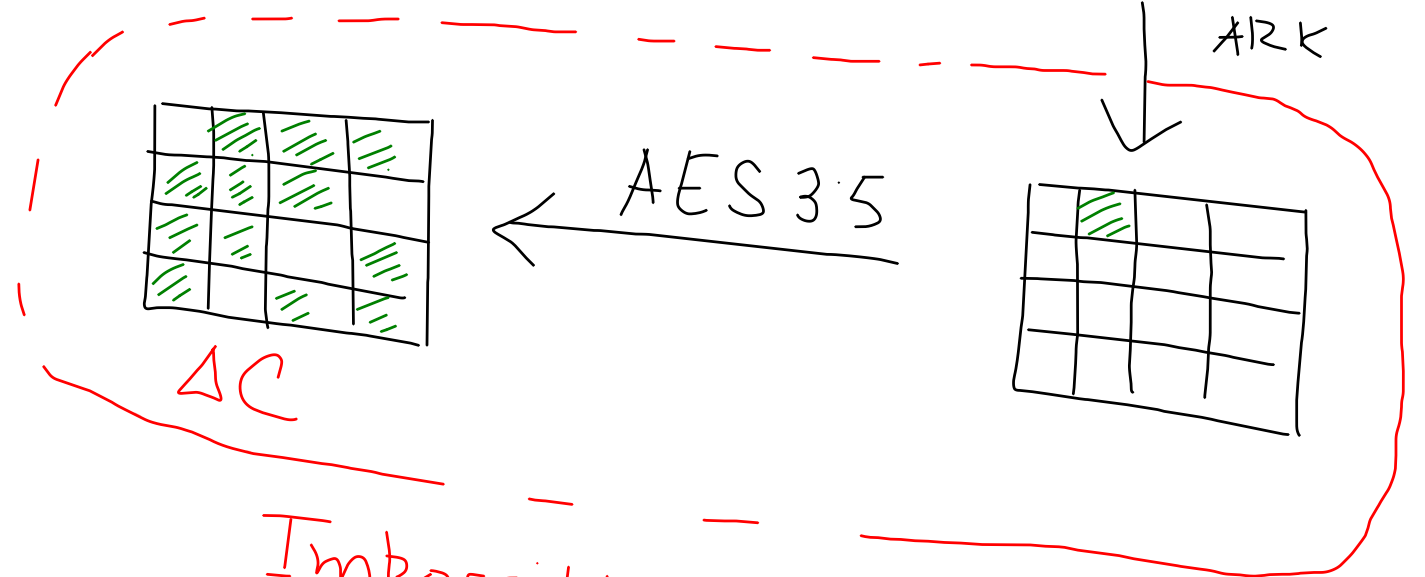
Key-Recovery Attack

ΔP



255 possible values $(T_1, \dots, T_{255})$

ARK



ΔC

Impossible Differential

$$\Rightarrow (2^8)^4 = 2^{32}$$

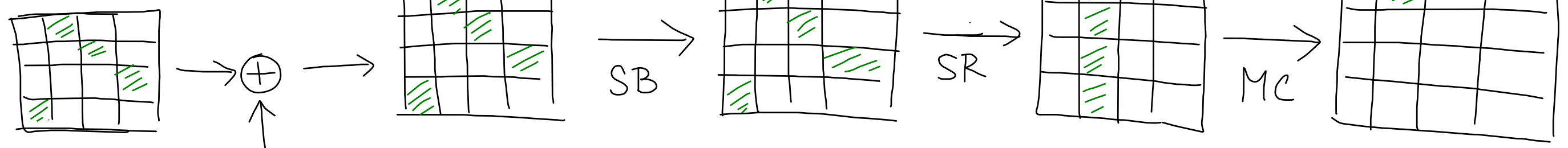
① Store $T_1, \dots, T_{255}$
 $\downarrow$
 $(S_1^{SB})_i$
 $\downarrow$
 $(S_1^{SB})_{255}$
 ΔS_1

② $P_1, P_2 \Rightarrow$ Guess $SK_0[3, 4, 9, 14]$
 $\parallel$
 $P_1 \oplus \Delta P$

③ $\nexists (\Delta S_1^{SB})^* \in \Delta S_1$
 Discard the key.

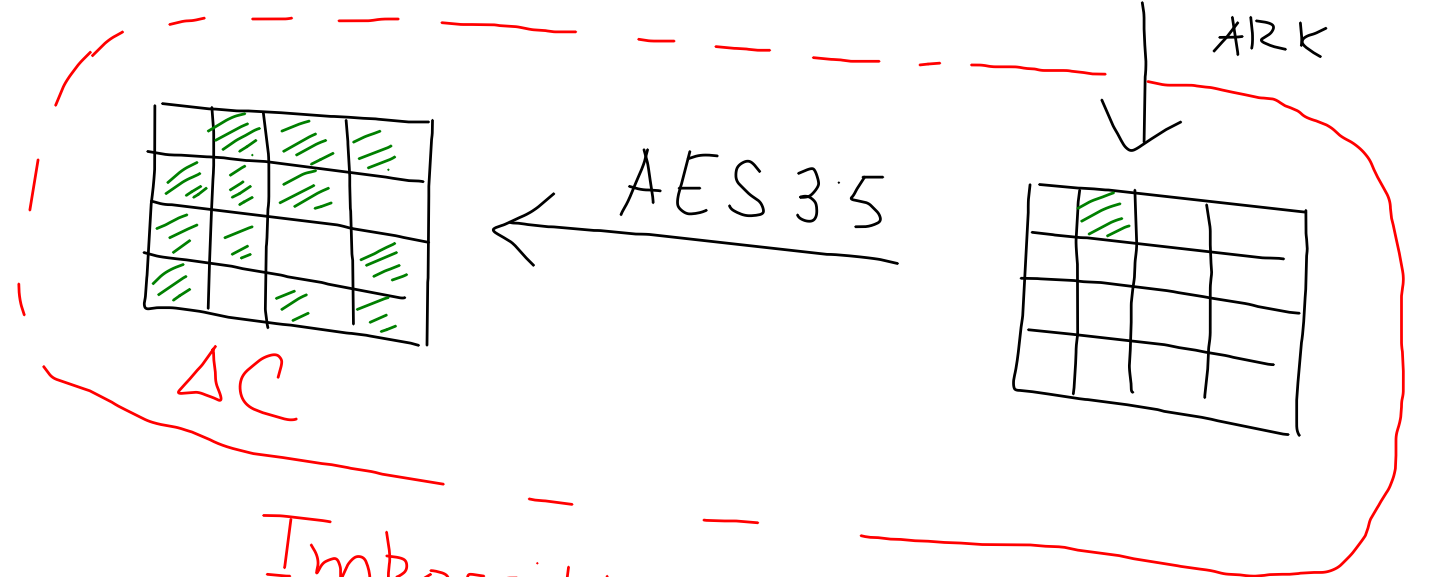
Key-Recovery Attack

ΔP



255 possible values $(T_1, \dots, T_{255})$

ARK



① Store $T_1, \dots, T_{255}$
 $\downarrow$
 (S_1^{SB})
 $\downarrow$
 $(S_1^{SB})_{255}$
 ΔS_1

②

$P_1, P_2 \Rightarrow$ Guess $SK_0[3, 4, 9, 14]$
 $\downarrow$
 $(\Delta S_1^{SB})^*$

③

$\nexists (\Delta S_1^{SB})^* \in \Delta S_1$
 Discard the key.

$$\Rightarrow (2^8)^4 = 2^{32}$$

Impossible Differential

5-Round Key Recovery Attack

- Suppose we make 2^N queries. We have to find N .
- Expected no. of $\overset{\text{valid}}{\Delta C} = 2^{N-32}$
- For every $(\Delta P, \underset{\substack{\Downarrow \\ \text{valid}}}{\Delta C})$ pair, there are 255 wrong key detection.
(expected)

$$2^{N-32} \cdot 255 \approx 2^{32}$$

$N \approx 56$

- However, this does not include Same key discard for multiple times.
- $N \approx 62/63$

- Suppose we make 2^N queries. We have to find N .
- Expected no. of $\overset{\text{valid}}{\Delta C} = 2^{N-32}$
- For every $(\Delta P, \underset{\substack{\Downarrow \\ \text{valid}}}{\Delta C})$ pair, there are 255 wrong key detection.
(expected)

$$2^{N-32} \cdot 255 \approx 2^{32}$$

$N \approx 56$

- However, this does not include Same key discard for multiple times.
- $N \approx 62/63$