Integral Cryptanalysis

Differential → Propagation of difference of values (sum of two values)

Integral → Propagation of sum of many values

Properties :

- ALL property (A) : takes all the values.
- CONSTANT property (C) : takes a fix value.

$$P_i = \begin{bmatrix} i & C_3 & C_7 & C_{11} \\ C_0 & C_4 & C_8 & C_{12} \\ C_1 & C_5 & C_9 & C_{13} \\ C_2 & C_6 & C_{10} & C_{14} \end{bmatrix}$$

$$i = 0, \ldots, 255$$

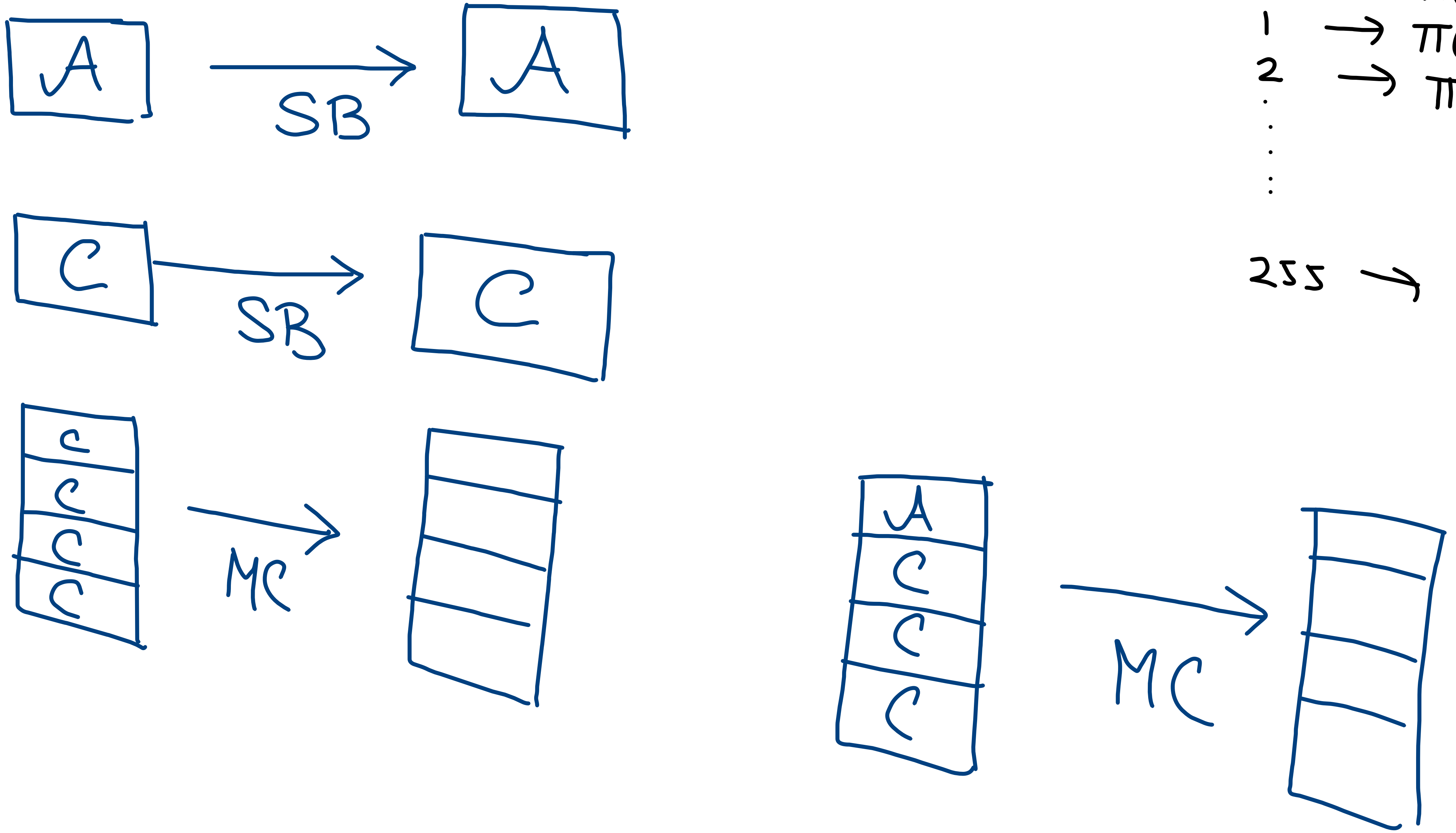
$$\Downarrow$$

$$\begin{bmatrix} A & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{bmatrix}$$

$$\mathcal{P} = \{P_0, \ldots, P_{255}\}$$

$\mathcal{P}$ satisfies this property

Properties after different operations



As SB is a permutation

$$\left.\begin{array}{l} 0 \to \pi(0) \\ 1 \to \pi(1) \\ 2 \to \pi(2) \\ \vdots \\ 255 \to \pi(255) \end{array}\right\} \text{distinct}$$

$$\begin{array}{|c|}\hline C\\ \hline C\\ \hline C\\ \hline C\\ \hline\end{array} \xrightarrow[MC]{} \begin{array}{|c|}\hline C\\ \hline C\\ \hline C\\ \hline C\\ \hline\end{array} \qquad\qquad \begin{array}{|c|}\hline A\\ \hline C\\ \hline C\\ \hline C\\ \hline\end{array} \xrightarrow[MC]{} \begin{array}{|c|}\hline A\\ \hline A\\ \hline A\\ \hline A\\ \hline\end{array}$$

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ & & & \\ & & & \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = 2c_0 + 3c_1 + c_2 + c_3 \longrightarrow$$

Same value for all the plaintexts

1st

$$\begin{pmatrix} 2 & 3 & 1 & 1 \end{pmatrix} \begin{pmatrix} i \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = 2i \oplus 3c_1 \oplus c_2 \oplus c_3 = 2i \oplus c'$$

$\hookrightarrow$ ALL DISTINCT VALUES

$P_0 = c'$

$P_1 = 2 \oplus c'$

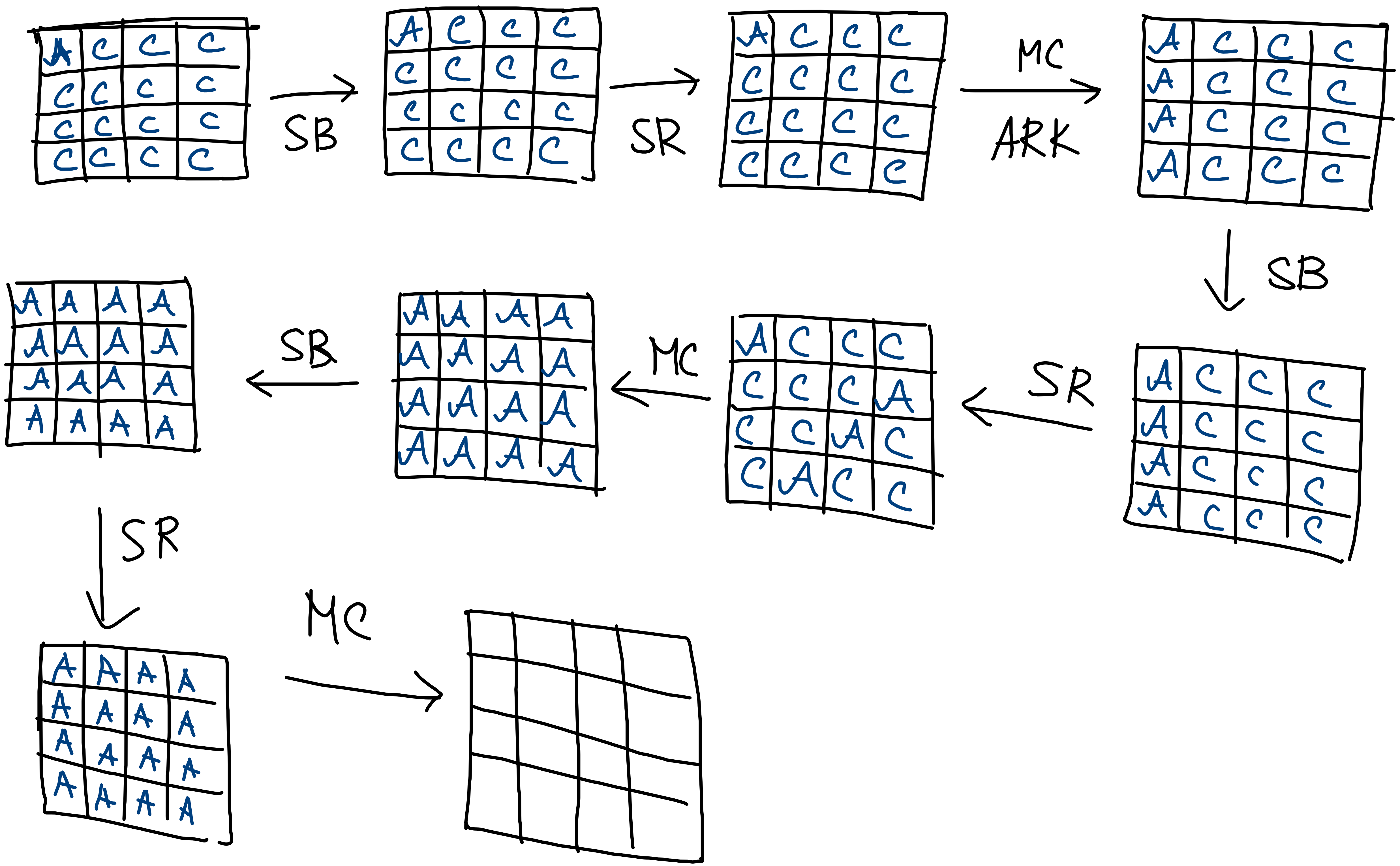
$P_2 =$

$\vdots$

2nd

$$\begin{pmatrix} 1 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} i \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = i \oplus \ldots \longrightarrow$$

All distinct values


SB
SR
MC
ARK
SB
SR
MC
SB
SR
MC

$$\begin{bmatrix} A \\ A \\ A \\ A \end{bmatrix} \xrightarrow{MC} \begin{bmatrix} B \\ B \\ B \\ B \end{bmatrix}$$

$$\begin{pmatrix} 2 & 3 & 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha_i \\ \beta_i \\ \gamma_i \\ \lambda_i \end{pmatrix}$$

$$= 2\alpha_i \oplus 3\beta_i \oplus \gamma_i \oplus \lambda_i$$

$$\{\alpha_0, \alpha_1, \ldots, \alpha_{255}\} = \{0, 1, \ldots, 255\}$$

Balanced Property (B)

$\boxed{\alpha_i}$

$$\bigoplus_{i=0}^{255} \alpha_i = 0$$

$$\Downarrow$$

XOR-SUM = 0

$0 \rightarrow 2\alpha_0 \oplus 3\beta_0 \oplus \gamma_0 \oplus \lambda_0$

$1 \rightarrow 2\alpha_1 \oplus 3\beta_1 \oplus \gamma_1 \oplus \lambda_1$

$\alpha_0 = \alpha_1$

$\beta_0 = \beta_1$

$\gamma_0 = \gamma_1$

$\lambda_0 = \lambda_1$

Doesn't satisfy A or C property

$$\bigoplus_{i=0}^{255}\left(2\alpha_i \oplus 3\beta_i \oplus \gamma_i \oplus \lambda_i\right)$$

$$= \left(2\bigoplus_{i=0}^{255}\alpha_i\right) \oplus \left(3 \cdot \bigoplus_{i=0}^{255}\beta_i\right) \bigoplus_{i=0}^{255}\gamma_i \bigoplus_{i=0}^{255}\lambda_i$$

$$= 0$$

$$\bigoplus_{i=0}^{255}\alpha_i = 0$$

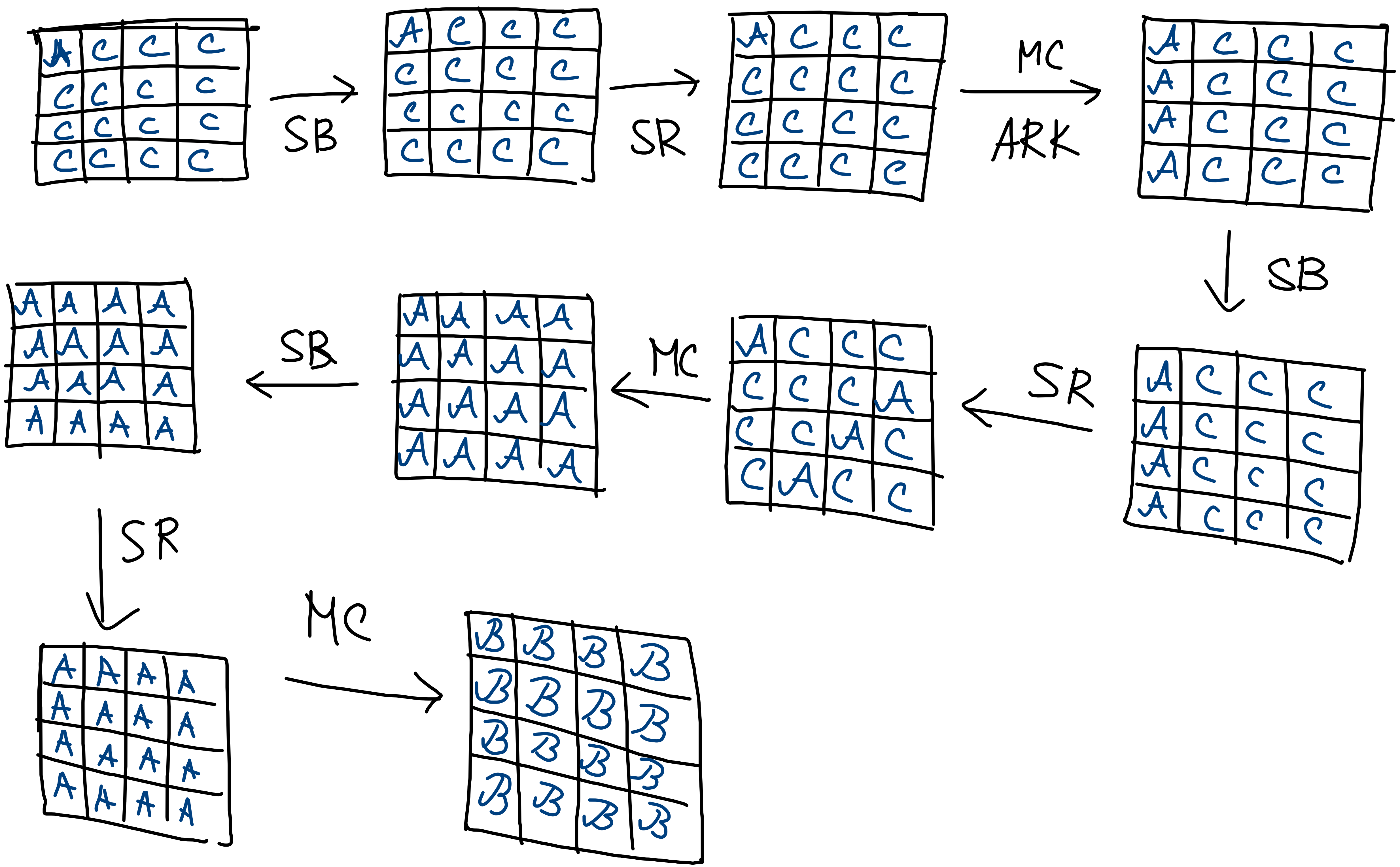
$$\vdots$$

$$\bigoplus_{i=0}^{255}\lambda_i = 0$$

$0, 1, 2, \ldots\ldots, 255$

$$\left.\begin{array}{ll} 0 \rightarrow & 000000000 \\ & 000000001 \\ & \vdots \\ 255 \rightarrow & 111111111 \\ \hline & 000000000 \end{array}\right\}$$

Integral Trail (AES 3 Round)



Distinguishing Attack

- Query $P_0, \ldots, P_{255}$
- Obtain $C_0, \ldots, C_{255}$
- Check if all the bytes are satisfying the balanced property
- If yes AES-3 }
  no random

Complexity

Data : 256

Time : 256

Memory : 1 State (AES)

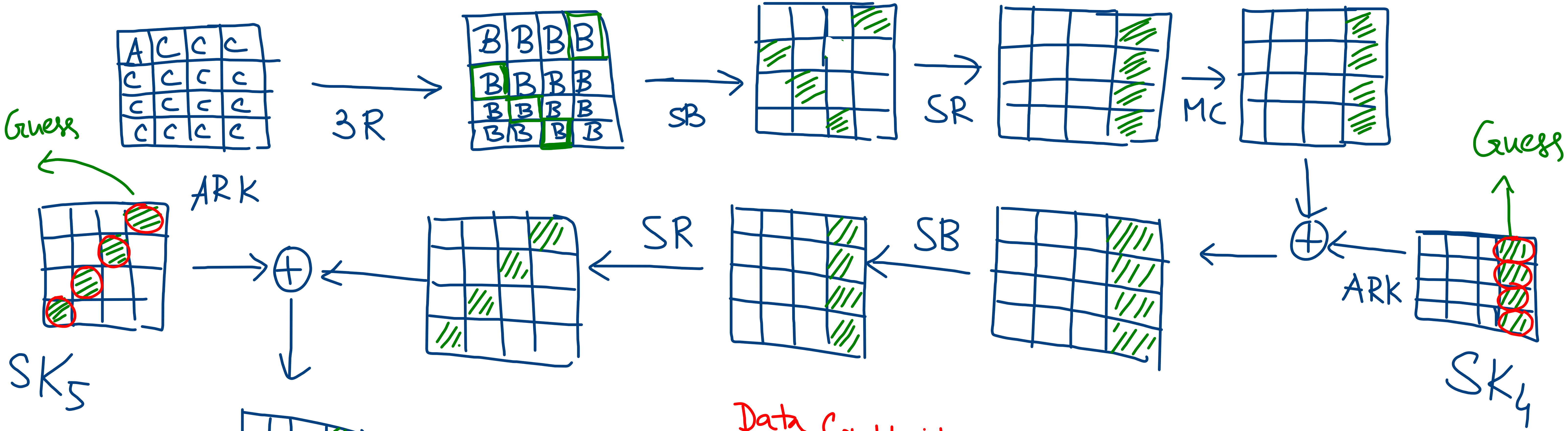
$$Adv = \left(1 - \left(\frac{1}{2^8}\right)^{16}\right)$$

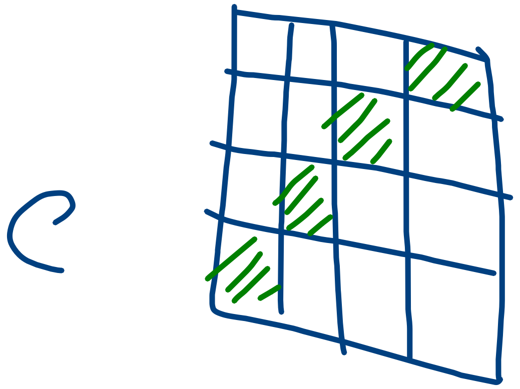
$$= \left(1 - \frac{1}{2^{128}}\right)$$

Key-Recovery Attack

→ Value known

→ Guess the value





Roughly valid keys $= \frac{2^{64}}{2^{32}} = 2^{32}$

Another set of 256 enc

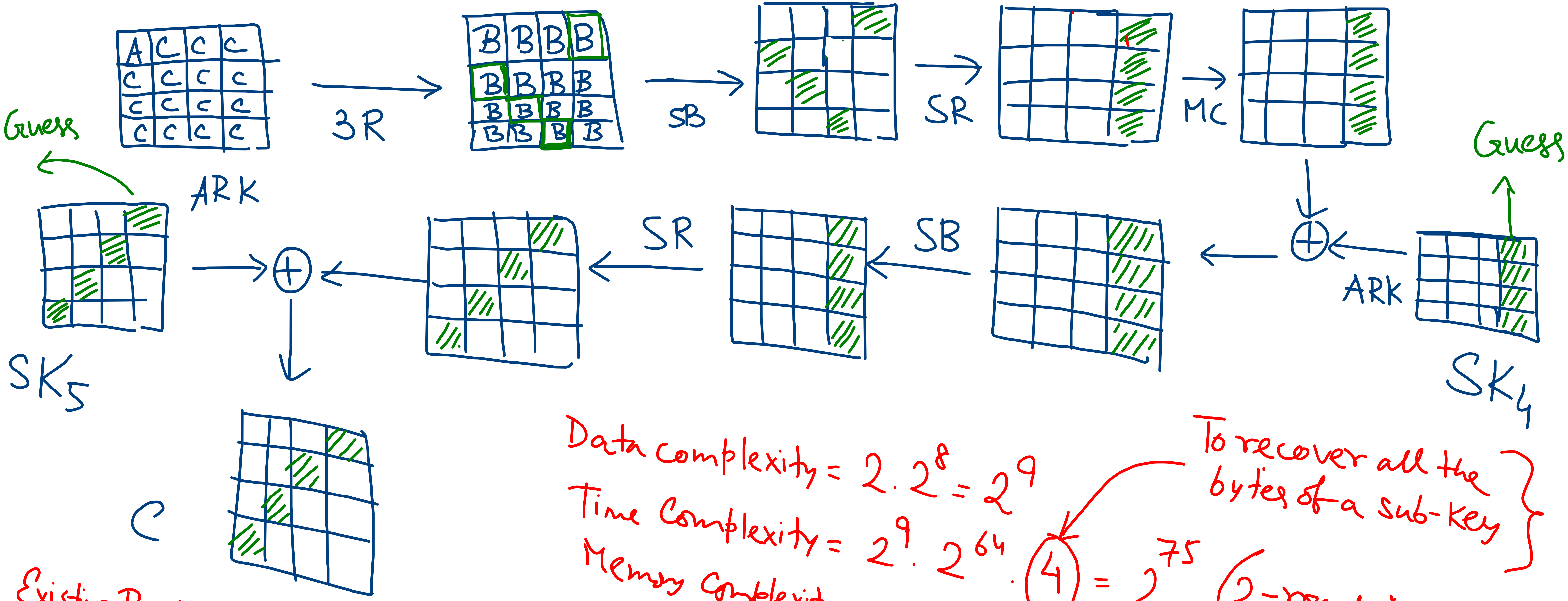
valid key $= \frac{2^{32}}{2^{32}} = 1$

Data Complexity → 256

Time Complexity → $2^{64} \times 256$ − (2 round AES + XOR checking)

(5-round) Key-Recovery Attack

(Repeat twice



Data complexity $= 2 \cdot 2^8 = 2^9$

Time Complexity $= 2^9 \cdot 2^{64} \cdot 4 = 2^{75}$ (2-round AES computation)

To recover all the bytes of a sub-key

Memory Complexity

Existing Best → 6 round (prepend one round at the beginning)

HW

(1) $\boxed{B} \xrightarrow{SB} \boxed{B}$?

(2) $\boxed{\begin{array}{c} A \\ \hline A \\ \hline C \\ \hline C \end{array}} \xrightarrow{MC}$?

(3) Sub-Key Guess diagonal ?

- Proof
- Counter Example

$\{m_1, m_2, m_3, m_4\}$

$\Downarrow$

$m_1 \oplus m_2 \oplus m_3 \oplus m_4 = 0$

$S(m_1) \oplus S(m_2) \oplus S(m_3) \oplus S(m_4) \neq 0$