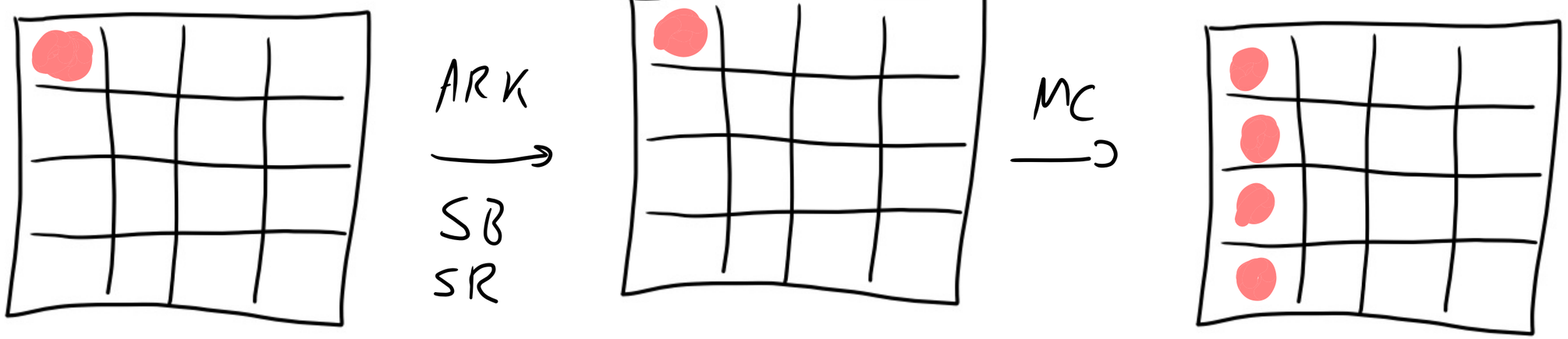
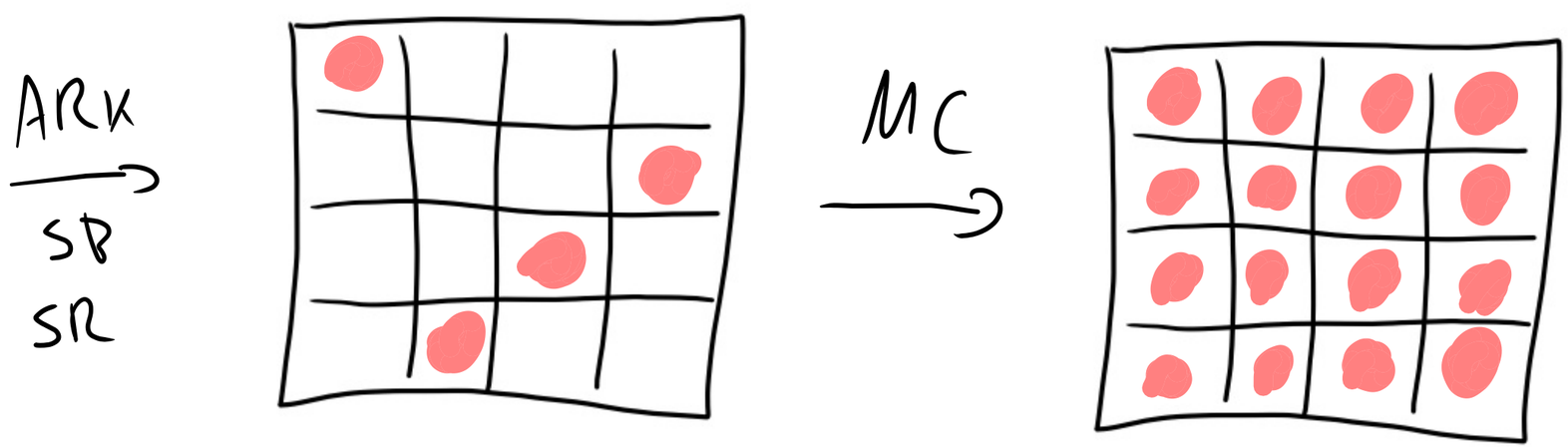

ARK
SB
SR
MC


ARK
SB
SR
MC

Rijndael data path

Input $x \in \mathbb{Z}_2^{128}$ and $K \in \mathbb{Z}_2^{128\text{ (or 192 or 256)}}$

- Key schedule: $(K_i) \leftarrow \texttt{KeyExpansion}(K)$
- state $\leftarrow x$ (but represented as $\mathrm{GF}(2^8)^{4\times 4}$)
- $\texttt{AddRoundKey}(\text{state}, K_0)$
- For each round $i = 1$ to 9 (or 11 or 13):
  - $\texttt{SubBytes}(\text{state})$
  - $\texttt{ShiftRows}(\text{state})$
  - $\texttt{MixColumns}(\text{state})$
  - $\texttt{AddRoundKey}(\text{state}, K_i)$
- And for the last round:
  - $\texttt{SubBytes}(\text{state})$
  - $\texttt{ShiftRows}(\text{state})$
  - $\texttt{AddRoundKey}(\text{state}, K_{10\text{ (or 12 or 14)}})$

Output $y \leftarrow$ state back in $\mathbb{Z}_2^{128}$

y
Add Round Key (K_{last})
Inv ShiftRows
Inv SubBytes ← z
Add Round Key (K_{last-1})
Inv MixColumns ← z+k
Inv ShiftRows
Inv SubBytes
$MC^{-1}(z+k) = MC^{-1}(z) + MC^{-1}(k)$
Add Round Key ← z
Inv MixColumns $MC^{-1}(z)$
Add Round Key ($MC^{-1}(k)$)
$MC^{-1}(z) + MC^{-1}(k) = MC^{-1}(z+k)$

$$M\begin{pmatrix} SB(a) \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$+ M\begin{pmatrix} 0 \\ SB(b) \\ 0 \\ 0 \end{pmatrix} = M\begin{pmatrix} SB(a) \\ SB(b) \\ SB(c) \\ SB(d) \end{pmatrix}$$

$$+ M\begin{pmatrix} 0 \\ 0 \\ SB(c) \\ 0 \end{pmatrix}$$

$$+ M\begin{pmatrix} 0 \\ 0 \\ 0 \\ SB(d) \end{pmatrix}$$