$$\left(\det M = 2k \cdot m^{n-1} \right)$$

Mini-AES

1° Math background

Finite fields (of characteristic 2)

$$GF(2) = \mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$$

↓ Galois Field

XOR ↙

+	0	1
0	0	1
1	1	0

AND ↙

·	0	1
0	0	0
1	0	1

In a field

$$a + b = b + a$$
$$a - b = a + (-b)$$
$$a - a = 0$$

$$ab = ba$$
$$\frac{a}{b} = a \cdot b^{-1} \text{ if } b \neq 0$$

$$GF(2^k) = \{ f = f_0 + f_1 x + f_2 x^2 + \cdots f_{k-1} x^{k-1} \mid f_i \in \mathbb{F}_2 \}$$

$$GF(2^4) = \{ f_0 + f_1 x + f_2 x^2 + f_3 x^3 \}$$

1001 | 1110 | 1001 | 1100

$[0, 2^4)$ 5

$[0, 2^4)$ $[0, 15]$ (binary numbers)

$1 + x^3$ $\downarrow x=2$ 9

$1 + x + x^2$ $\downarrow x=2$ 7

$1 + 0 \cdot x + 0 \cdot x^2 + 1$ 9

16 bits $\rightarrow$ 4 elements of $\mathbb{F}_{16}$

$P_0, P_1, P_2, P_3 \in GF(16)$

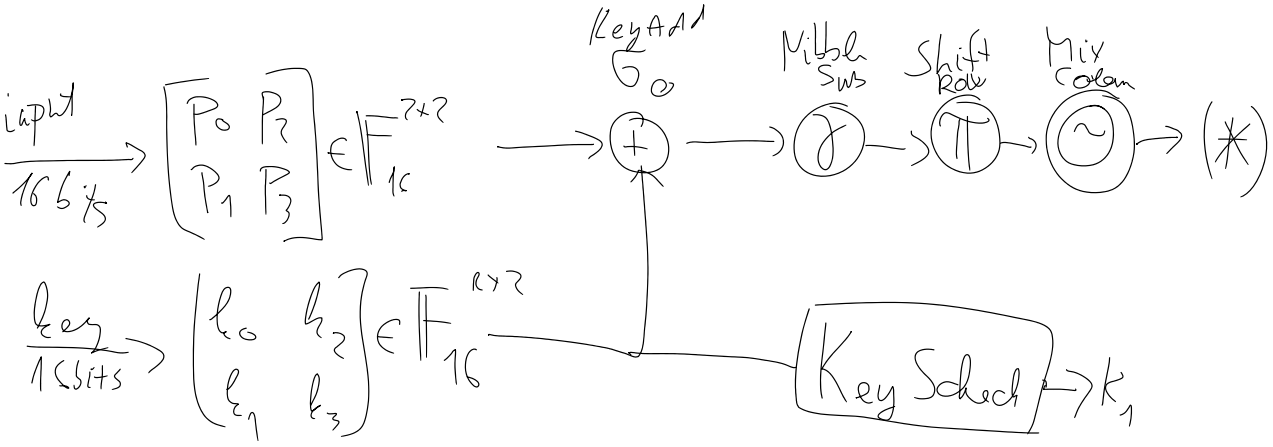
$\begin{bmatrix} P_0 \\ P_1 \end{bmatrix} \begin{bmatrix} P_2 \\ P_3 \end{bmatrix} \in GF(2^4)^2$

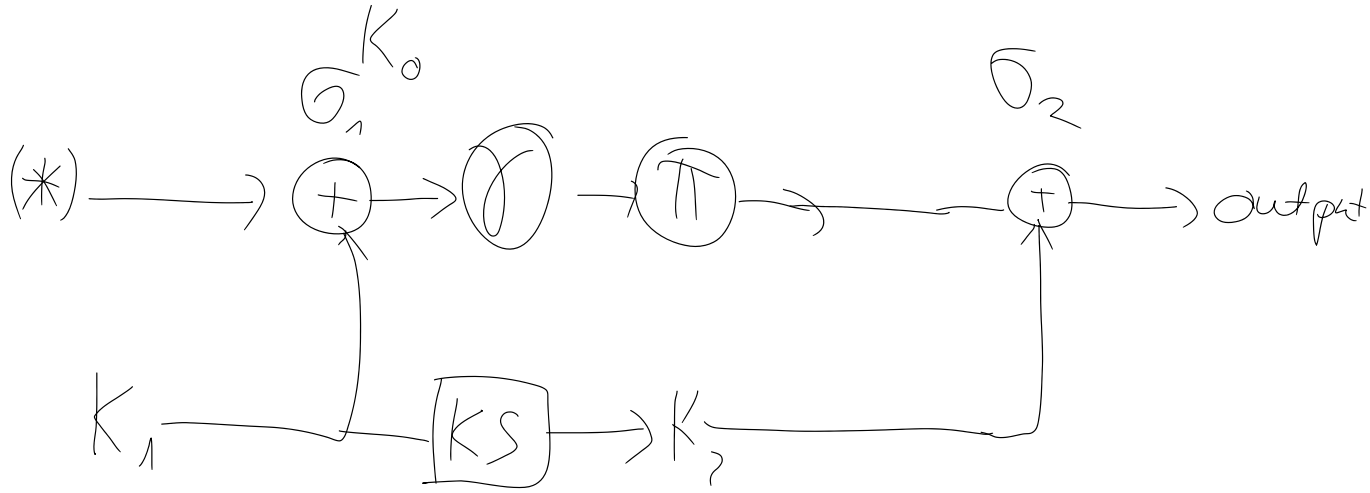
$\begin{bmatrix} P_0 & P_2 \\ P_1 & P_3 \end{bmatrix} \in \mathbb{F}_{16}^{2\times 2}$

$b_0 b_1 b_2 b_3$ to nibble = to take a small ~~byte~~ byte

NibbleSub : $x \mapsto \underline{a \cdot x^{-1} + b}$ for a fixed a, b

3°





$$(\alpha \circ \beta)(x) = \alpha(\beta(x))$$

$$(\alpha \circ \beta)^{-1} = \beta^{-1} \circ \alpha^{-1}$$

$$(\sigma_2 \circ \pi \circ \gamma \circ \sigma_0 \circ \theta \circ \pi \circ \gamma \circ \sigma_0)^{-1} =$$
$$\sigma_0^{-1} \circ \gamma^{-1} \circ \pi^{-1} \circ \theta^{-1} \circ \sigma_1^{-1} \circ \gamma^{-1} \circ \pi^{-1} \circ \sigma_2^{-1} =$$
$$\sigma_0 \circ \gamma^{-1} \circ \pi \circ \theta \circ \sigma_1 \circ \gamma^{-1} \circ \pi \circ \sigma_2$$