

Der Körper \mathbb{F}_{28}

$\mathbb{F}_{28} \ni a = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7$,
wobei $a_i \in \mathbb{F}_2 = \{0, 1\}$.

Darstellung: 8 Bits für ein Element = 1 Byte.

Addition: XOR, $(a + b)_i = a_i + b_i$.

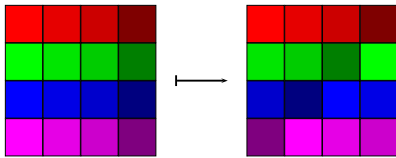
Multiplikation: wie für Polynome modulo $x^8 + x^4 + x^3 + x + 1$.

Beispiel $57 \cdot 83 = C1$:

$$\begin{aligned} (x^4 + x^3 + x^2 + 1) \cdot (x^7 + x + 1) &= x^{11} + x^{10} + x^9 + x^8 + x^7 + \\ &\quad x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + \\ &\quad x^4 + x^3 + x^2 + 1 \\ &= x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + \\ &= x^7 + x^6 + 1 \pmod{x^8 + x^4 + x^3 + x + 1}. \end{aligned}$$

Körper: Durch jedes Element ungleich Null darf geteilt werden.

Die ShiftRow Operation



Die Zeilen werden zyklisch um null, ein, zwei oder drei Byte verschoben.

Polynome über dem Körper \mathbb{F}_{28}

$R = \mathbb{F}_{28}[z]/(z^4 + 1) \ni a_0 + a_1z + a_2z^2 + a_3z^3$,
wobei $a_i \in \mathbb{F}_{28}$.

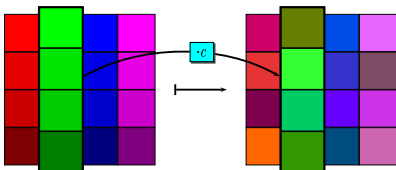
Addition: koeffizientenweise $(a + b)_i = a_i + b_i$, XOR.

Multiplikation: wie für Polynome modulo $z^4 + 1$. Eine Gleichung $d = a \cdot b$ ist gleichbedeutend mit

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Kein Körper: $(z + 1)^4 = 0$.

Die MixColumn Operation



Jede Spalte wird als Polynom mit $c = 02 + 01z + 01z^2 + 03z^3$ multipliziert.

Umkehrung: Multiplikation mit $d = 0E + 09z + 0Dz^2 + 0Bz^3$.

Die S-Box

$$\mathbb{F}_{28} \xrightarrow{S} \mathbb{F}_{28} \xrightarrow{S} \mathbb{F}_{28}$$

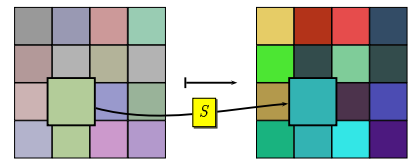
$$y \mapsto y^{-1} \stackrel{S}{\mapsto} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Hochgradig nichtlinear:

$$y \mapsto 05 \cdot y^{254} + 09 \cdot y^{253} + F9 \cdot y^{251} + 25 \cdot y^{247} + F4 \cdot y^{239} + 01y^{223} + B5 \cdot y^{191} + 8F \cdot y^{127} + 63.$$

Implementierung einfach durch 256 Byte Lookup-Tabelle.

Die ByteSub Operation



Auf jedes Byte wird die S-Box angewendet.

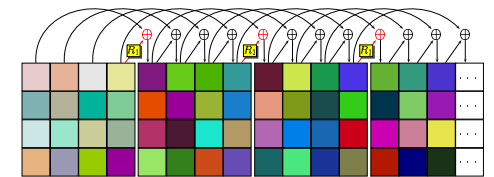
Nichtlinearer Teil der Rundschlüsselzeugung

$$(\mathbb{F}_{28})^4 \rightarrow (\mathbb{F}_{28})^4$$

$$R_i: \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} \mapsto \begin{bmatrix} S(b) + x^{i-1} \\ S(c) \\ S(d) \\ S(a) \end{bmatrix}$$

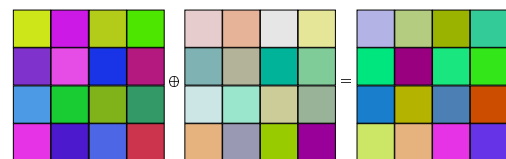
Durch die Verwendung der S-Box ist diese Abbildung nichtlinear.

Die Rundschlüsselzeugung (Key Schedule)



Aus dem 128 bis 256 Bit Schlüssel werden die Rundschlüssel erzeugt.

Die AddRoundKey Operation



Einfaches XOR mit dem Rundschlüssel.