CRYPTO2-Übersicht: VL 04: Schlüsselabl. v. Rijndael; „Mini-AES"

↳ & warum diese wichtig ist (vgl. UE03)!

- Was wäre, wenn alle Rundenschlüssel gleich wären? (UE03): → „Slide Attack", vgl. Biryukov & Wagner

$x \to \oplus \to \boxed{\rho} \to \oplus \to \boxed{\rho} \to \oplus \to \dots \to \boxed{\rho} \to \oplus \to c$ (jeweils $\oplus k$) d.h. $k_0 = k_1 = \dots = k_t$

Per CPA kann ich den Schlüssel k nach $\approx\sqrt{2^\lambda}$ Schritten finden, sprich die Bits an Sicherheit von λ auf $\lambda/2$ halbieren:

($\xi = x_1$)

$x \to \oplus \to \boxed{\rho} \xrightarrow{\xi} \oplus \to \boxed{\rho} \cdots \to \oplus \to \boxed{\rho} \to \oplus \to c$ (jeweils $\oplus k$)

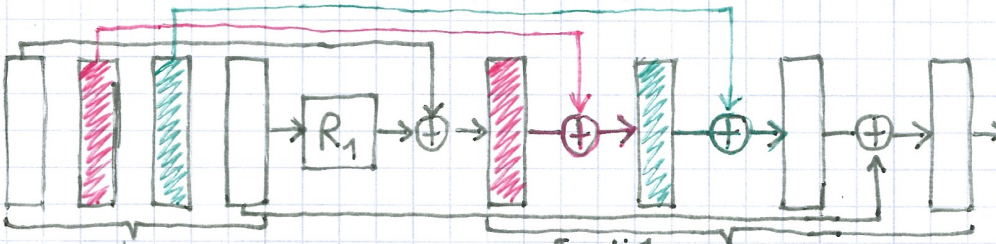
$\xi \to \oplus \to \boxed{\rho} \cdots \to \oplus \to \boxed{\rho} \to \oplus \xrightarrow{c} \boxed{\rho} \to \oplus \to c' = \rho(c) \oplus k$ (Vor.)

Achtung: in GNF falsch! ∇₀ ↯↯

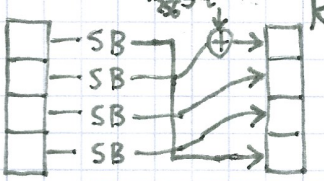
21 ∇₀: Probiere (x, ξ) aus und nehme an, dass $\rho(x \oplus k) = \xi$. Daraus lässt sich k ableiten. Gilt für dieses k außerdem $Enc(k,x) = c \wedge Enc(k,\xi) = c' = \rho(c) \oplus k$, haben wir (x, ξ) richtig geraten und k bestimmt. Die Wk. dafür beträgt $1/2^{\lambda k}$ (die Wk., dass k korrekt ist). Nach dem Geburtstagsparadoxon muss ich $\sqrt{2^{\lambda k}}$ (x,ξ)-Paare durchprobieren, um mit Wk. $\geq \frac{1}{2}$ erfolgreich zu sein.
Wäre der Rundenschlüssel nicht immer der gleiche, müsste x immer mit k_0 und ξ immer mit k_1 verschlüsselt werden; das wird unser Opfer wohl kaum für uns tun.

- Die Schlüsselableitung/-expansion von Rijndael/AES: (engl.: "AES key schedule")

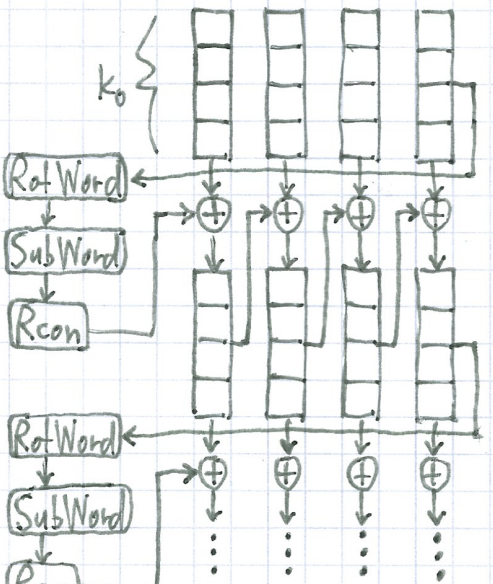
Darstellg. VL:



wobei: i-te Runde R_i:



(Äquivalente) Darstellg. en. wik.:



wobei:
- $RotWord([b_0\ b_1\ b_2\ b_3]) = [b_1\ b_2\ b_3\ b_0]$
- $SubWord([b_0\ b_1\ b_2\ b_3]) = [S(b_0), S(b_1), S(b_2), S(b_3)]$ mit AES S-Box
- $rcon_i = [rc_i\ 00_{16}\ 00_{16}\ 00_{16}]$ mit $rc_i = x^{i-1}$ (im $\mathbb{F}_{256}$/Rijndael)

- Mini-AES: (Phan 2002) (auch in Sage!)

AES: Status $\in (\mathbb{F}_{256})^{4\times4}$ Matrizen
Mini-AES: Status $\in (\mathbb{F}_{16})^{2\times2}$ Matrizen
↳ d.h. Nibbles (Halb-Bytes) statt Bytes

$\mathbb{F}_{16} = \{0,\dots,F\} = \mathbb{F}_2[t]/\langle t^4+t+1\rangle$ (VL → Popov)

```
from sage.crypto.block_cipher.miniaes import MiniAES
```

SB: `MiniAES().sbox()`: (14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7)

Paper:			
0000 ↦ 1110	0100 ↦ 0010	1000 ↦ 0011	1100 ↦ 0101
0001 ↦ 0100	0101 ↦ 1111	1001 ↦ 1010	1101 ↦ 1001
0010 ↦ 1101	0110 ↦ 1011	1010 ↦ 0110	1110 ↦ 0000
0011 ↦ 0001	0111 ↦ 1000	1011 ↦ 1100	1111 ↦ 0111

(eig. Nibble-Sub!)

= 1. Reihe der 1. S-Box von DES; VL: $a \mapsto (t^3+t^2+1)\cdot a + (t^2+t)$ ↯↯

SR: Paper: $\begin{pmatrix} b_0 & b_2 \\ b_1 & b_3 \end{pmatrix} \xrightarrow{SR} \begin{pmatrix} b_0 & b_2 \\ b_3 & b_1 \end{pmatrix} = \begin{pmatrix} c_0 & c_2 \\ c_1 & c_3 \end{pmatrix}$ (in VL x↦x²)

MC: Paper: $\begin{pmatrix} c_0 & c_2 \\ c_1 & c_3 \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} d_0 & d_2 \\ d_1 & d_3 \end{pmatrix}$ mit

Paper: $\begin{pmatrix} d_i \\ d_{i+1} \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} c_i \\ c_{i+1} \end{pmatrix} = \left(\begin{array}{c|c} t+1 & t \\ \hline t & t+1 \end{array}\right) \begin{pmatrix} c_i \\ c_{i+1} \end{pmatrix}$ ← Sage matrix.org

VL: "Schlüsselableitung" / Paper: "The Mini-AES Key-schedule":
VL: "wie beim (großen) AES"; Paper: 2 rounds: K_0, K_1, K_2

$x \to \oplus_{K_0} \to SB \to SR \to MC \to \oplus_{K_1} \to SB \to SR \to \oplus_{K_2} \to c$ ← Paper