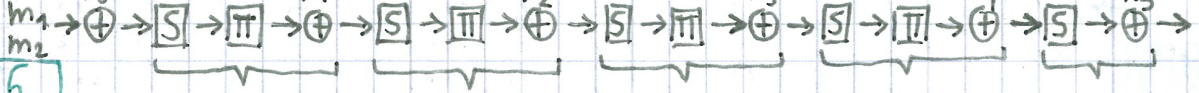
# CRYPTO2-Übersicht: VL07: Diff. Cryptoanalyse auf Chiffre 4 (=S-Box und Permutation)

(Bsp. von Knudsen)

- Chiffre 4 (key-iterated wie AES): ↳ & DDT der AES-Substitution (b.w.!)
  Blöcke $\in \mathbb{B}^{16} \simeq (\mathbb{B}^4)^4$ (=4 Nibbles) ($\pi \hat{=} MC \circ SR$ bei AES)




in VL nur textuell

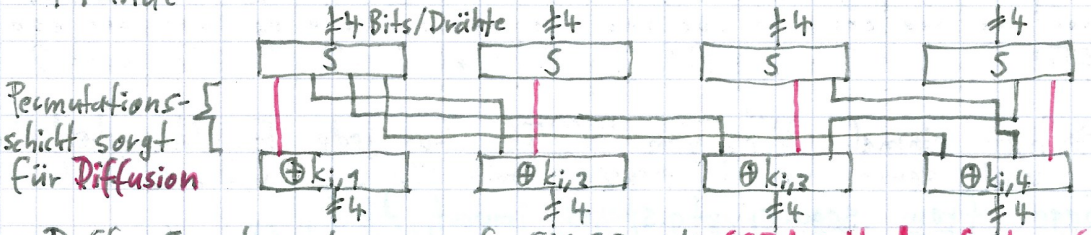
$5 \cdot 16 = 96$ Schlüsselbits

wobei: Substitution: $S^{(4)}: (x_1, x_2, x_3, x_4) \mapsto (S(x_1), S(x_2), S(x_3), S(x_4))$ ; $x_i \in \mathbb{B}^4$ ($\in \mathbb{B}^{16}$)

Permutation: Sei Block $e_i := (0, \dots, 1, 0, \dots, 0)$ mit 1 an $i$-ter Stelle
Dann wird $e_i$ durch die Permutation auf $e_{\pi(i)}$ abgebildet; mit:

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\pi(i)$ | 1 | 5 | 9 | 13 | 2 | 6 | 10 | 14 | 3 | 7 | 11 | 15 | 4 | 8 | 12 | 16 |

1 Runde:




- Diff. Cryptoanalyse auf Chiffre 4 (CPA → d.h. Angreifer kann (m,c)-Paare generieren):
  Selbe Strategie wie bei Chiffre 3: Anstatt einmal $6 \cdot 16 = 96$ Schlüsselbits zu raten (das wäre stupides Brute-Force mit Aufwand $2^{96}$), rate sechsmal 16 Schlüsselbits (Aufwand: $6 \cdot 2^{16} < 2^{19}$)! Rate also zunächst $k_5$ als $k_5^*$.
  Was macht einen guten Kandidaten $k^*$?
  Und woher weiß ich nun, ob ich gut geraten habe?! Mit $c_1, c_2, k_5^*$ und $S^{-1}$ kann ich die Eingabedifferenz $\Delta_{in}$ an der letzten S-Box bestimmen. Gut geraten habe ich, wenn diese gleich der tatsächlichen Eingabedifferenz ist. Doch leider kenne ich diese nicht (obwohl ich $m_1 \& m_2$ kenne, doch schon ab Chiffre 2 sind mir ja weitere S-Boxen und unbekannte Rundenschlüssel im Weg). Deshalb muss ich auch diese Eingabedifferenz an der letzten S-Box schlau(!) raten; dazu bediene ich mich (wie bei Chiffre 3 mit einem 2-Runden-Differential) eines 4-Runden-Differentials; das sind all die Möglichkeiten (sog. 4-Runden-Charakteristiken), um von $\Delta_{in} = m_1 + m_2$ auf $\Delta_{out}$ zu kommen: $\Delta_{in} \xrightarrow{S} ? \xrightarrow{S} ? \xrightarrow{S} ? \xrightarrow{S} \Delta_{out}$. Habe ich Glück und die verwendete S-Box ist schlecht, gibt es ein solches Differential mit recht hoher Wahrscheinlichkeit, dann wähle ich $m_1, m_2$ mit $m_1 + m_2 = \Delta_{in}$ und nehme $\Delta_{out}$ als Eingabedifferenz $\Delta_{in}$ an der letzten S-Box an.
  Wähle gute $(m_1, m_2)$-Paare!
  Ich tue also folgendes, um $k_5$ zu bestimmen:
  - Wähle Paare $(m_1, m_2), (m_1', m_2'), \dots$ - stets mit $c_1 + c_2 \in S(\Delta_{out})$, d.h. "gute" Paare.
  - Generiere für jedes dieser Paare eine Kandidatenliste
    $K(m_1, m_2) = \{k^* \mid S^{-1}(c_1 + k^*) + S^{-1}(c_2 + k^*) = \Delta_{out} \hat{=} \Delta_{in, \text{letzte S-Box}}\}$
  - Der wirkliche Schlüssel $k_5$ liegt in allen diesen Listen: $k_5 \in K(m_1, m_2) \cap K(m_1', m_2') \cap \dots$

Chiffre 4: Chiffre 4 addiert mit den Permutationen $\pi$ nun jedoch eine Schwierigkeit: Die DDT für die 4 S-Boxen mit Perm. $\pi$ wäre $2^{16} \times 2^{16}$ Einträge groß ↯
Neue Strategie: Mache (möglichst viele) S-Boxen "inaktiv", d.h. sorge dafür, dass gar keine Eingabedifferenz anliegt ($\Delta_{in} = 0$). Nutze außerdem die Tatsache aus, dass die Permutation $\pi$ Fixpunkte besitzt (=Schwäche▽):
4-Runden-Charakteristik: $(0x0, 0x0, 0x2, 0x0) \xrightarrow{S} (0x0, 0x0, 0x2, 0x0)$
$\xrightarrow{S} \dots \xrightarrow{S} \dots \xrightarrow{S} (0x0, 0x0, 0x2, 0x0)$
Denn: (a) Nach der DDT von $S$ ist häufig $\Delta_{in} = 0x2 \xrightarrow{S} 0x2 = \Delta_{out}$ (Wk. $\frac{6}{16}$)
(b) Das 11. Bit ist das einzig gesetzte und $\pi(11) = 11$ (Fixpunkt v. $\pi$)▽
Die Wk. dieser Charakteristik ist zwar mit $(6/16)^4 \approx 0{,}02$ nicht gut, doch es gibt noch weitere Charakteristiken im Differential $(0,0,2,0) \xrightarrow{(4)} (0,0,2,0)$; insg. gibt es 4 4-Runden-Charakteristiken im Differential, jede mit Wk. 0,02, d.h. insg. mit Wk. 0,08 und $0{,}08 > 1/16 = 0{,}06$, was gut ist!
▽ Damit haben wir einen "feinen Riss" im Kryptosystem, mit dem wir "prokeln" können! ↯

(crypto.stackexchange.com/questions/37659)

(cntrdvc.com/bcd10869)

• DDT der AES-Substitution:

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | ... | 1E (30) | 1F (31) | 20 (32) | 21 (33) | ... | FF | ← $\Delta_{out}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 256 | 0 | 0 | 0 | 0 | 0 | 0 | ... | 0 | 0 | 0 | 0 | ... | 0 | |
| 01 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | ... | 2 | 4 | 0 | 2 | ... | 2 | |
| 02 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | ... | 0 | 0 | 0 | 0 | ... | 2 | |
| 03 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | ... | 2 | 2 | 0 | 2 | ... | 2 | |
| 04 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... | 2 | 0 | 2 | 2 | ... | 2 | |
| 05 ← $\Delta_{in}$ | 0 | 0 | 0 | 0 | 2 | 0 | 0 | ... | 2 | 2 | 2 | 0 | ... | 2 | |
| 06 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | ... | 0 | 0 | 2 | 0 | ... | 2 | |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | |
| (30) 1E | 0 | 2 | 2 | 2 | 2 | 2 | 0 | ... | 2 | 2 | 0 | 2 | ... | 0 | |
| (31) 1F | 0 | 0 | 2 | 0 | 0 | 0 | 0 | ... | 2 | 2 | 0 | 0 | ... | 0 | |
| (32) 20 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | ... | 0 | 0 | 2 | 2 | ... | 2 | |
| (33) 21 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | ... | 2 | 0 | 2 | 0 | ... | 2 | |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | |
| FF | 0 | 2 | 2 | 2 | 0 | 0 | 0 | ... | 2 | 2 | 0 | 2 | ... | 2 | |

⇒ hat einmal Wk. von 4/256 für jede Ein-/Ausgabedifferenz und sonst nur Differenziale mit Wk. von max. 2/256

Sage: `from sage.crypto.sboxes import AES`
`AES.difference_distribution_table().str()` ✓
`[0][0]`

→ Wie kommt das? (VL):
↳ hat mit Lösungen von quadratischen Gleichungen zu tun

SubBytes: $\mathbb{F}_{256} \to \mathbb{F}_{256}: b \mapsto 1F_{16} \cdot b^{254} \oplus 63_{16}$
(Mult. im TR; Inv. im $\mathbb{F}_{256}$; Plus im TPR = XOR Bits)

Seien die Eingaben $x$ und $x+\Delta$, d.h. die Eingabedifferenz $\Delta_{in} = \Delta$.
In AES gilt für die S-Box: $S(x) = 1F_{16} \cdot x^{-1} \oplus 63_{16}$
D.h. die Ausgabedifferenz ist hier: $\Delta_{out} =$
$S(x) + S(x+\Delta)$
$= [1F_{16} \cdot x^{-1} \oplus 63_{16}] + [1F_{16} \cdot (x+\Delta)^{-1} \oplus 63_{16}]$
$= 1F_{16} \cdot \left(\frac{1}{x} + \frac{1}{x+\Delta}\right) = 1F_{16} \cdot \left(\frac{x+\Delta+x}{x(x+\Delta)}\right) = 1F_{16} \cdot \frac{\Delta}{x(x+\Delta)}$

Die Frage ist nun:
Zu gegebenem $\Delta_{in}$ und $\Delta_{out}$, wie viele Werte $x$ erfüllen die Gleichung $\Delta_{out} = 1F_{16} \cdot \frac{\Delta_{in}}{x \cdot (x+\Delta_{in})}$ ?

Durch Umstellen sieht man, dass es sich um eine quadratische Gleichung handelt und quadratische Gleichungen haben max. 2 Lösungen:

$$\Leftrightarrow \Delta_{out} \cdot x \cdot (x+\Delta_{in}) = 1F_{16} \cdot \Delta_{in}$$
$$\Leftrightarrow x \cdot (x+\Delta_{in}) = \frac{1F_{16} \cdot \Delta_{in}}{\Delta_{out}}$$
$$\Leftrightarrow \underset{=}{x^2} + \Delta_{in} \cdot \underset{=}{x} - \frac{1F_{16} \cdot \Delta_{in}}{\Delta_{out}} = 0 \quad \blacksquare$$