07 - Güte von linearen Approximationen

Luc Spachmann

FSU Jena

14.12.2023

Substitutions-Permutations-Netzwerk

- Designprinzip für Blockchiffren
- Lokale Substitution durch S Boxen
- 'Globale' Permutation
- Schlüsseladdition
- Arbeitet in Runden
- Beispiel: AES

Heutiges SPN

- Das gleiche aus der VL
- 4 Blöcke à 4 Bit
- 4 Runden
- Alle Rundenschlüssel sind gleich
- Alle S-Boxen sind identisch
- S-Box:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
π_S	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

- Permutation:

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
π_P	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Lineare Kryptoanalyse

- Idee: Suche lineare Approximation an S-Boxen
- Sei $a, b \in \{0,1\}^4$, U die gleichverteilte ZV für den Input der S-Box und $V = S(U)$. Dann

$$U_a = \bigoplus_{i=1}^{4} a_i U_i \qquad U_b = \bigoplus_{i=1}^{4} b_i V_i$$

- Suche a, b, c sodass mit hoher Wahrscheinlichkeit gilt:

$$V_b = U_a \oplus c$$

- Bias einer Zufallsvariable X:

$$\varepsilon(X) = Pr[X = 0] - \frac{1}{2}$$

- Wahrscheinlichkeit explizit berechnen durch relative Häufigkeiten

Güte der Approximation

- Güte der Approximation für eine S-Box S:

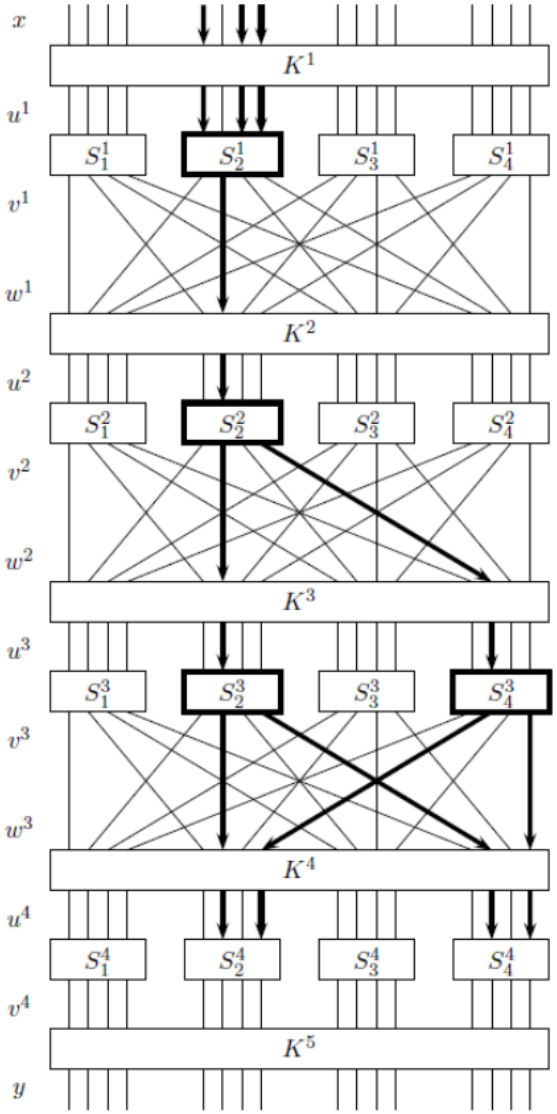
$$T_S = |\varepsilon(U_a \oplus V_b)|$$

- Sei $\mathcal{S}$ die Menge an aktiven S-Boxen
- Für $S \in \mathcal{S}$ ist T_S die Approximation der jeweiligen S-Box
- Güte der Approximation für das gesamte SPN (Piling-up Lemma):

$$\prod_{S \in \mathcal{S}} T_S$$

Aufgaben

- Evaluiert die Güte einer linearen Approximation
- Input: S-Box, Approximation
- Format S-Box: Liste an Hexadezimalziffern (z.B. E4D12FB83A6C5907)
- Format Approximation:
  - Je zwei Hexadezimalziffern pro S-Box (außer letzte Zeile)
  - Erste für Input, zweite für Output
  - 00 für inaktive Box
- Permutation konstant
- Output: Güte der Approximation in standard output
- -1, falls keine gültige Approximation
- Programmname [S-Box] [Approximation]



Kodierung der Approximation:

00	B4	00	00
00	45	00	00
00	45	00	45

Kodierung der S-Box:
E4D12FB83A6C5907