

05 - Lineare Kryptoanalyse

Luc Spachmann

Friedrich-Schiller-Universität Jena

26.11.2021

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

Heutiges SPN

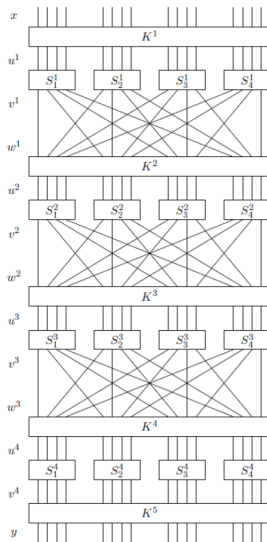
- Das gleiche aus der VL
- 4 Blöcke à 4 Bit
- 4 Runden
- Alle Rundenschlüssel sind gleich
- Alle S-Boxen sind identisch
- S-Box:

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

Heutiges SPN



- 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

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

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

$$V_b = U_a \oplus c$$

- Bias einer Zufallsvariable X :

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

- Güte der Approximation:

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

- Gute Approximationen für unsere S-Boxen z.B.:

$$T = U_1 \oplus U_3 \oplus U_4 \oplus V_2$$

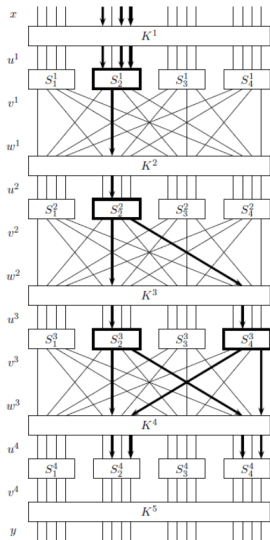
$$T' = U_2 \oplus V_2 \oplus V_4$$

- Bias der Approximationen:

$$\varepsilon(T) = \frac{1}{4}$$

$$\varepsilon(T') = -\frac{1}{4}$$

Lineare Kryptoanalyse



- 'Verfolgen' Bits durch die Approximation
- Zusammengefasst erhalten wir

$$X_5 \oplus X_7 \oplus X_8 \oplus U_6^4 \oplus U_8^4 \oplus U_{14}^4 \oplus U_{16}^4$$

- Gesamtgüte ungefähr Produkt der Güten der Approximationen

$$\varepsilon \approx \left(\frac{1}{4}\right)^4 = \frac{1}{32}$$

(Teil-) Schlüsselbestimmung

- Zufälliger Klartext X erfüllt mit hoher oder niedriger (nicht mittlerer) Wahrscheinlichkeit die Approximation

$$X_5 \oplus X_7 \oplus X_8 \oplus U_6^4 \oplus U_8^4 \oplus U_{14}^4 \oplus U_{16}^4 = 0$$

- Benötigen Menge M an Klartext-Kryptotextpaaren (x, y)
- Berechnen für jeden Teilschlüssel-Kandidat (L_1, L_2) für $(K_{(2)}^5, K_{(2)}^5)$ Rückwärts benötigte Bits von u_4 (für jedes Paar)
- Für jeden Teilschlüssel-Kandidat berechne Wahrscheinlichkeit der Approximation
- Höchste oder niedrigste W'keit vermutlich richtiger Teilschlüssel (größte Differenz zu $\frac{1}{2}$)
- Teilschlüssel verringert Suchraum für Brute-Force

- Implementiert das beschriebene SPN
- Implementiert Teilschlüsselsuche für gegebene lineare Approximation
- Erzeugt dazu die Klartext-Kryptotextpaare einfach selber
- Wie viele Paare werden benötigt?
- In der Theorie sind es ca $t\epsilon^{-2} \approx t \cdot 1000$ für kleines t (in VL $t = 8$)