# Kryptografie und -analyse, Zusammenfassung Vorlesung 6

Henry Haustein

## Was ist eine iterative Charakteristik?

Ein Sonderfall sind sogenannte iterative Charakteristiken, mit $\Omega_1 = \Omega_2$, welche immer wieder an sich selbst angehängt werden können. Die vertauschten Hälften der Klartextdifferenz sind also gleich der Geheimtextdifferenz derselben Charakteristik. Diese lassen sich also leicht zu beliebig großen $n$-Runden-Charakteristiken zusammenhängen. Während bei nicht-iterativen Charakteristiken die Wahrscheinlichkeit mit größerem $n$, bedingt durch den Avalanche-Effekt, immer schneller abnimmt, bleiben die Wahrscheinlichkeiten der Teilcharakteristiken aus denen iterative Charakteristiken zusammengesetzt sind gleich. Iterative Charakteristiken werden deshalb bei einem Angriff bevorzugt eingesetzt.

## Wie wirkt sich die Anzahl aktiver S-Boxen auf die differentielle Kryptoanalyse aus?

Es wird aufwendiger, je mehr S-Boxen aktiv sind.

## Was ist das Ziel der linearen Kryptoanalyse?

Klartext-Schlüsseltext-Angriff

- Ziel: Approximation der Chiffrierfunktion durch eine lineare Abbildung
- Suche nach Approximationsgleichungen mit möglichst hoher Güte
- Untersuchung genügend vieler Klartext-Schlüsseltext-Paare liefert Schlüsselbits

Lineare Abhängigkeit einzelner Ausgabebits einer S-Box $Si_O[i]$? gesucht: Funktionen $\phi : \mathbb{F}_2^6 \to \mathbb{F}_2$ mit

$$Si_O[i] = \phi(Si) = \bigoplus_{k=1}^{6} l_k \cdot Si_I[k]$$

## Wie werden lineare Approximationen für die Substitutionsboxen ermittelt?

Systematische Suche

## Wie kann mit Hilfe einer solchen Approximationsgleichung eine Runde analysiert werden?

Mit Auswahlvektor $u = (010000)$ und $v = (1111)$ (Güte $\frac{12}{64} \Rightarrow$ affine Approximation, Güte $\frac{52}{64}$) ergibt sich für S5:

$$\begin{aligned} u^T \cdot S5_I &= v^T \cdot S5_O \oplus 1 \\ u^T \cdot (m \oplus k) &= v^T \cdot c \oplus 1 \\ (010000)^T \cdot m \oplus (010000)^T \cdot k &= (1111)^T \cdot c \oplus 1 \\ m^{[2]} \oplus k^{[2]} &= c^{[1,2,3,4]} \oplus 1 \end{aligned}$$

Umstellen nach $k^{[2]}$:

$$k^{[2]} = m^{[2]} \oplus c^{[1,2,3,4]} \oplus 1$$

Analyse von genügend Klartext-Schlüsseltext-Paaren liefert $k^{[2]}$.

## Wie ist das allgemeine Vorgehen bei der linearen Kryptoanalyse (einfacher Algorithmus)?

Vorbereitung:

- Auswahlvektoren $u$, $v$, $w$ bestimmen mit:

$$\begin{aligned} w^k &= u^T \cdot m \oplus v^T \cdot c \quad \text{oder} \\ w^k &= u^T \cdot m \oplus v^T \cdot c \oplus 1 \end{aligned}$$

- Güte der Approximation $p_A > 0.5$

1. Schritt

- Untersuchung von $N$ Klartext-Schlüsseltext-Paaren
- $Z$: Anzahl von Paaren, für die die rechte Seite der entsprechenden Gleichung 0 ist

2. Schritt: $Z > \frac{N}{2} : w^T \cdot k = 0$ oder $Z < \frac{N}{2} : w^T \cdot k = 1$

## Wie erfolgt die Analyse des DES mit 3 Runden?

Zwei verschiedene Approximationsgleichungen für erste und dritte Runde

- 1. Runde: $k_1^{[26]} = x_1^{[17]} \oplus y_1^{[3,8,14,25]} \oplus 1$
- 3. Runde: $k_3^{[26]} = x_3^{[17]} \oplus y_3^{[3,8,14,25]} \oplus 1$

Ersetzen von $y_1 = L_m \oplus x_2$ und $y_3 = L_c \oplus x_2 \Rightarrow$ Addieren der Gleichungen entfernt $x_2$ (für Näheres siehe Übung)