G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 1

Definition Für eine Abbildung $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ bezeichne

$$\Delta_{F,c}(x) := F(x) + F(x+c).$$

Der Wert

$$\delta_F := \max_{c \in \mathbb{F}_2^n, c \neq 0, a \in F_2^m} |\Delta_{F,c}(a)^{-1}|$$

heist *Uniformität* von F.

Aufgabe 1 *Differentielle Attacke*
Bei der differentiellen Attacke auf DES spielt für jede S-Box S die Abbildung

$$\begin{aligned} \Delta_{S,c} : \mathbb{F}_2^6 &\to F_2^4 \\ \Delta_{S,c}(x) &= S(x) + S(x+c) \end{aligned}$$

eine wichtige Rolle. Warum? Was zeichnet die Elemente

$$\Delta_{S,c}(a)^{-1}$$

aus?

Aufgabe 2 *APN*

1. Sei $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ eine Funktion. Wir definieren

   $$\Delta_{f,c}(x) := f(x) + f(x+c).$$

   Zeigen Sie, das jedes Element $a \in \mathbb{F}_{2^n}$ eine gerade Anzahl von Urbildern hat, d.h das die Größe der Menge

   $$\Delta_{f,c}^{-1}(a) = \{x \in \mathbb{F}_{2^n} \quad | \quad \Delta_{f,c}(x) = a\}$$

   für jedes a und jedes c immer gerade ist.

2. Wie groß sind diese Mengen, wenn f eine lineare Funktion ist? Bestimmen Sie die Uniformität von lineare Funktionen.

3. Zeigen Sie das für die Abbildung $f(x) = x^3$ und für jedes $c \neq 0$ die Anzahl der Urbilder von $\Delta_{f,c}$ für jedes c höchstens 2 ist.

Aufgabe 3 *AES S-Box*

1. Zeigen Sie, das für die Abbildung

$$\begin{aligned} I : \mathbb{F}_{2^n} &\rightarrow F_{2^n} \\ I(x) &= x^{2^n-2} \end{aligned}$$

die Uniformität 2 ist wenn n ungerade ist und 4 wenn n gerade ist.

2. Seien $L, L' : \mathbb{F}_{2^n} \rightarrow F_{2^n}$ bijektive Lineare Abbildungen und $c, c' \in \mathbb{F}_{2^n}$ Konstanten. Zeigen Sie, das die Uniformität einer Abbildung $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ und der Abbildung $F' : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ mit

$$F'(x) = L(F(L'(x) + c')) + c'$$

gleich sind.

3. Folgern Sie, dass die Uniformität der AES S-Box 4 ist.