G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 4

Definition Für eine Boolsche Funktion $f : \mathbb{F}_2^n \to \mathbb{F}_2$ bezeichnet für $a \in \mathbb{F}_2^n$

$$f^W(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle a,x \rangle}$$

den *Walsh-Koeffizient* von f an der Stelle a.

Aufgabe 1 *Differentielle Attacke auf AES I*
Aus dem letzten Übungsblatt wurde gezeigt, das die Uniformität der AES S-Box 4 beträgt. Was bedeutet das für die Resistenz von AES gegen differentielle Attacken?

Aufgabe 2 *Differentielle Attacke auf AES II*
Sei $L : (\mathbb{F}_{2^m})^n \to (\mathbb{F}_{2^m})^n$ eine lineare Abbildung. Die Menge

$$\mathcal{C} = \{(x, L(x)) \mid x \in (\mathbb{F}_{2^m})^n\}$$

beschreibt einen *linearen Code* in $(\mathbb{F}_{2^m})^{2n}$ der Länge $2n$ und mit der Dimension n über $\mathbb{F}_{2^m}$. Die Differenz zweier Codewörter $a, b \in (\mathbb{F}_{2^m})^{2n}$ beschreibt man mit

$$\mathrm{wt}(a + b) = |\{0 \leq i \leq 2n - 1 \mid (a + b)_i \neq 0\}|.$$

Sei nun L die MixColumns Abbildung des AES, d.h. $L : (\mathbb{F}_{2^8})^{16} \to (\mathbb{F}_{2^8})^{16}$ und $\mathcal{C}_{AES}$ der entsprechende Lineare Code. Man kann zeigen, das der minimal Abstand zweier Codewörter in diesem Code 5 ist. Was bedeutet das für die Resistenz von AES gegen differentielle Attacken?

Aufgabe 3 *Walsh-Transformation*
Sei $f : \mathbb{F}_2 \to \mathbb{F}_2^n$ geben. Zeigen Sie folgende Eigenschaften der Walsh-Transformierten.

1. $$\sum_{a \in \mathbb{F}_2^n} f^W(a) = 2^n(-1)^{f(0)}$$

2. $$f^W(a) = 0 \bmod 2$$

3. $$\sum_{a \in \mathbb{F}_2^n} f^W(a)^2 = 2^{2n}$$

Überlegen Sie, in welchem Sinne

$$L(f) = \max_{a \in \mathbb{F}_2^n} |f^W(a)|$$

ein Maß für die Linearität von f ist.
Hinweis: $x \mapsto \langle a, x \rangle$ beschreibt für alle $a \in \mathbb{F}_2^n$ eine lineare Funktion. Weiterhin können alle linearen Boolschen Funktionen auf $\mathbb{F}_2^n$ durch ein passendes $a \in \mathbb{F}_2^n$ so beschrieben werden.