G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 12

Definition Für eine Boolesche Funktion $f : \mathbb{F}_2^n \to \mathbb{F}_2$ gibt es eindeutig bestimmte Elemente $\lambda_u \in \mathbb{F}_2$ für $u \in \mathbb{F}_2^n$ so dass

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} \lambda_u \prod_{i=1}^{n} x_i^{u_i}$$

für alle $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$ gilt. Diese Darstellung heißt *Algebraische Normalform (ANF).*

Aufgabe 1 *Ein Beispiel*
Sei $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ mit

x	000	001	010	011	100	101	110	111
$f(x)$	0	1	1	0	0	0	1	0

Bestimmen Sie die ANF von f und überprüfen Sie ihr Ergebnis.

Aufgabe 2 *Eine Basis*
Betrachten Sie die Funktionen

$$\begin{aligned} \delta_a : \mathbb{F}_2^n &\to \mathbb{F}_2 \\ \delta_a(x) &= \begin{cases} 0 & x \neq a \\ 1 & x = a \end{cases} \end{aligned}$$

für $a \in \mathbb{F}_2^n$.

1. Bestimmen Sie die ANF für die Funktionen δ_a.
2. Wie lässt sich damit die ANF für eine beliebige Funktion $f : \mathbb{F}_2^n \to \mathbb{F}_2$ bestimmen.

Aufgabe 3 *Algebraische Immunität*

1. Zeigen Sie, dass die Algebraische Immunität von jeder Funktion δ_a gleich 1 ist.
2. Zeigen Sie, dass die Algebraische Immunität jeder Funktion $f : \mathbb{F}_2^n \to \mathbb{F}_2$ mit $|\{x \in \mathbb{F}_2^n \mid f(x) \neq 0\}| \leq n$ gleich 1 ist.

Aufgabe 4 *Der Grad*
Zeigen Sie, das für zwei Funktionen $f, g : \mathbb{F}_2^n \to F_2$

$$\text{grad}(f + g) \leq \max\{\text{grad}(f), \text{grad}(g)\}$$

gilt.Zeigen Sie, das im Allgemeinen

$$\text{grad}(f + g) = \max\{\text{grad}(f), \text{grad}(g)\}$$

falsch ist.