G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 9

Aufgabe 1 *Ein Beispiel*
Gegeben sei folgende Rekursionsgleichung

$$s_t = s_{t-2} + s_{t-3}$$

über $\mathbb{F}_2$.

1. Berechnen Sie die Folge der s_t für

$$s_0 = 1 \quad s_1 = 1 \quad s_2 = 0$$

2. Bestimmen Sie für jede mögliche Wahl der Initialzustände eine Darstellung der Folge als

$$s_t = \mathrm{Tr}(\theta\alpha^t)$$

Aufgabe 2 *Gleichverteilt*
Sei eine lineare Rekursionsgleichung über $\mathbb{F}_2$ mit irreduziblem charakteristischem Polynom gegeben. Zeigen Sie, dass für jede Wahl der Initialwerte die Rekursionsfolge entweder konstant 0 ist oder die Werte 0 und 1 gleichhäufig auftreten.

Aufgabe 3 *Der zentrale Satz*
Sei eine lineare Rekursionsgleichung mit charakteristischem Polynom f gegeben. Seien $\alpha_1, \ldots, \alpha_r$ verschiedene Nullstellen von f. Dann erfüllt die Folge

$$s_t = \lambda_1\alpha_1^t + \lambda_2\alpha_2^t + \cdots + \lambda_r\alpha_r^t$$

für jede Wahl der Konstanten λ_i die Rekursionsgleichung.