G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 10

Aufgabe 1 *Verschiedene Perioden???*
Sei eine lineare Rekursionsgleichung mit irreduziblem charakteristischem Polynom f vom Grad m gegeben. In der Vorlesung haben wir gesehen, das die Periode einer Folge, welche die Rekursionsgleichung erfüllt, der Ordnung *einer* Nullstelle des Polynoms f in $\mathbb{F}_{2^m}^*$ entspricht. Das Polynom f hat über $\mathbb{F}_{2^m}$ aber m verschiedene Nullstellen. Daraus folgt insbesondere, das die Ordnung aller Nullstellen gleich sein muss. Zeigen Sie dies direkt.

Aufgabe 2 *Zyklische Verschiebungen*
Zwei Folgen s_t und s'_t heißen *zyklisch äquivalent*, wenn es ein $r \in \mathbb{N}$ gibt, so dass

$$s_t = s'_{t+r} \text{ für alle } t \in \mathbb{N}$$

gilt. Sei eine lineare Rekursionsgleichung über $\mathbb{F}_2$ mit irreduziblem charakteristischem Polynom f vom Grad m gegeben. Die Periode der Rekursionsgleichung sei N.

1. Zeigen Sie, dass es $\frac{2^m-1}{N}$ bis auf zyklische Äquivalenz verschiedene Folgen gibt, die die Rekursionsgleichung erfüllen.

2. Folgern Sie nun, dass für eine lineare Rekursionsgleichung mit maximaler Periode *alle* Folgen zyklisch äquivalent sind. Geben Sie hierfür eine alternative Begründung.

Aufgabe 3 *Correlations Angriffe*
Betrachten Sie einen Combination Cipher, der die Ausgaben von drei LFSRs mit folgende Funktion f verknüpft.

$$f : \mathbb{F}_2^3 \to \mathbb{F}_2$$

mit

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

1. Berechnen Sie die Walshkoeffizienten von f

2. Bestimmen Sie die Wahrscheinlichkeit, das $f(x_1, x_2, x_3) = x_i$ für $i = 1, 2, 3$.

3. Was fällt auf? Formulieren Sie ihre Vermutung.