G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 11

Aufgabe 1 *Algebraische Attacke I*
Gegeben Sei ein nichtlineares Gleichungssystem über $\mathbb{F}_2$ der Form

$$\begin{aligned} P_1(x_1, \ldots, x_n) &= 0 \\ P_2(x_1, \ldots, x_n) &= 0 \\ \vdots &\quad \vdots \\ P_t(x_1, \ldots, x_n) &= 0 \end{aligned}$$

mit Polynomen $P_i \in \mathbb{F}_2[x_1, \ldots, x_n]$ vom Grad d. Eine Möglichkeit, solche Gleichungen zu lösen bietet eine Linearisierung. Hierbei wird für jedes vorkommende Monom eine neue Variable eingeführt. Das so konstruierte *lineare* Gleichungssystem kann man zum Beispiel mit Gauss lösen. Die Effizienz dieses Verfahrens ist stark davon abhängig, wie groß der Lösungsraum des linearisierten Systems ist.

1. Wie groß muss t in Abhängigkeit von n und d mindestens sein, damit das lineare Gleichungssystem eindeutig lösbar ist?

2. Wie groß ist in diesem Fall der Aufwand um das Gleichungssystem zu lösen?

Aufgabe 2 *Algebraische Attacke II*
Betrachten Sie einen Stream Cipher, der aus n LFSRs und einer Kombinations-Funktion $f : \mathbb{F}_2^n \to \mathbb{F}_2$ mit $\text{grad}(f) = d$ besteht. Angenommen Sie kennen einen Teil des Schlüsselstroms.

1. Stellen Sie ein Gleichungssystem für die (geheimen) initialen Zustände der LFSRs auf. Welchen Grad hat dieses System?

2. Was würde es helfen, wenn es eine Funktion $g : \mathbb{F}_2^n \to \mathbb{F}_2$ geben würde mit $\text{grad}(g) < d$ und $g(x)f(x) = 0$ für alle $x \in \mathbb{F}_2^n$?

Aufgabe 3 *Algebraische Attacke III*
In der vorherigen Aufgabe wurde deutlich, das es nicht ausreicht, wenn $f : \mathbb{F}_2^n \to \mathbb{F}_2$ hohen Grad hat. Vielmehr darf es auch keine Funktion $g : \mathbb{F}_2^n \to \mathbb{F}_2$ mit kleinem Grad geben, so dass $f(x)g(x) = 0$ für alle x gilt. Zeigen Sie das die Menge

$$\{g : \mathbb{F}_2^n \to \mathbb{F}_2 \mid g(x)f(x) = 0 \ \forall x \in \mathbb{F}_2^n\}$$

ein Vektorraum bildet.