G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 6

Aufgabe 1 *Ein Nachtrag*
Sei $n \in \mathbb{N}$ und $a \in \mathbb{F}_2^n$ gegeben. Zeigen Sie:

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{\langle a,x \rangle} = \begin{cases} 0 & a \neq 0 \\ 2^n & a = 0 \end{cases}$$

Aufgabe 2 *Die Spur Abbildung*
Sei $n \in \mathbb{N}$. Die Spur Abbildung ist definiert als

$$\begin{aligned} \mathrm{Tr} : \mathbb{F}_{2^n} &\rightarrow \mathbb{F}_{2^n} \\ \mathrm{Tr}(x) &= \sum_{i=0}^{n-1} x^{2^i} \end{aligned}$$

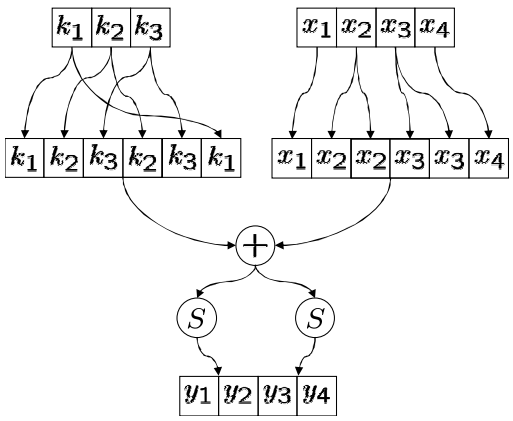
Beweisen Sie, dass für alle $x, y \in \mathbb{F}_{2^n}$ folgende Eigenschaften gelten.

1. $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$
2. $\mathrm{Tr}(x^2) = \mathrm{Tr}(x)$
3. $\mathrm{Tr}(x) \in \mathbb{F}_2$

Aufgabe 3 *Lineare Attacke*
Betrachten Sie das folgende Abbildungsschema, das eine Abbildung

$$E : \begin{cases} GF(2)^3 \times GF(2)^4 & \rightarrow & GF(2)^4 \\ (k_1, k_2, k_3, x_1, x_2, x_3, x_4) & \mapsto & (y_1, y_2, y_3, y_4) \end{cases}$$

beschreibt.



x_1	x_2	x_3	$S(x)$
0	0	0	11
0	0	1	11
0	1	0	10
0	1	1	11
1	0	0	01
1	0	1	01
1	1	0	00
1	1	1	11

1. Berechnen Sie die Linearität der durch die Wertetabelle gegebenen S-Box

$$S : GF(2)^3 \to GF(2)^2$$

und versuchen Sie die Komponentenfunktionen S_1, S_2 und $(S_1 + S_2)$ linear zu approximieren.

2. Bestimmen Sie mit Hilfe von b) 4 Gleichungen der Form

$$\sum_{i=1}^{4} \alpha_i y_i = \sum_{i=1}^{3} \beta_i k_i + \sum_{i=1}^{4} \gamma_i x_i$$

(mit $\alpha_i, \beta_i, \gamma_i \in \{0, 1\}$), die für möglichst viele (k, x, y)-Tripel erfüllt sind.

3. Für festes $k = (k_1, k_2, k_3) \in GF(2)^3$ wurden folgende (x, y)-Paare mit $y = E(k, x)$ erzeugt:

x	0101	0111	1010
y=E(k,x)	0010	0001	1101

Welches k wurde vermutlich verwendet?