Übungsblatt 7

Abgabe der schriftlichen Lösungen am 14. 12. 2017 bis 13.10 Uhr

Aufgabe 35 ***mündlich***

Überlegen Sie, wie sich ein durch ein SPN verschlüsselter Kryptotext $y = E_{f,\pi_s,\pi_P}(K,x)$ wieder zu x entschlüsseln lässt.

Aufgabe 36 ***mündlich***

Sei $\alpha_S\colon \{0,1\}^l \to \{0,1\}^{l'}$ eine S-Box und für $(a,b) \in \{0,1\}^l \times \{0,1\}^{l'}$ sei $L(a,b)$ die Anzahl der Paare $(x,y) \in \left\{(x,\alpha_S(x)) \mid x \in \{0,1\}^l\right\}$, für die $\bigoplus_{i=1}^{l} a_i x_i = \bigoplus_{j=1}^{l'} b_j y_j$ ist. Zeigen Sie:

(a) $L(0^l, 0^{l'}) = 2^l$,

(b) $L(a, 0^{l'}) = 2^{l-1}$ für alle $a \in \{0,1\}^l - \{0^l\}$,

(c) $\displaystyle\sum_{a\in\{0,1\}^l} L(a,b) = 2^{2l-1} \pm 2^{l-1}$ für alle $b \in \{0,1\}^{l'}$,

(d) $\displaystyle\sum_{\substack{a\in\{0,1\}^l\\ b\in\{0,1\}^{l'}}} L(a,b) = \begin{cases} 2^{2l+l'-1} + 2^{l+l'-1} & \alpha_S(0^l) = 0^{l'}, \\ 2^{2l+l'-1} & \text{sonst.} \end{cases}$

Aufgabe 37 Sei $l > 0$ eine feste Zahl. ***10 Punkte***

Für eine Bijektion $\pi\colon \mathbb{Z}_2^l \to \mathbb{Z}_2^l$ sei $N_\pi^1 = (\mathbb{Z}_2^l, \mathbb{Z}_2^l, K^1, E_\pi^1, D_\pi^1)$ das Kryptosystem, das einen Klartext x mit Schlüssel $k \in K^1 = \mathbb{Z}_2^l$ zu

$$E_\pi^1(k,x) = \pi(x \oplus k)$$

verschlüsselt, wobei die Addition modulo 2 komponentenweise erfolgt.
Weiter sei induktiv für $i \geq 2$: $N_\pi^i = (\mathbb{Z}_2^l, \mathbb{Z}_2^l, K^i, E_\pi^i, D_\pi^i) := N_\pi^{i-1} \times N_\pi^1$.

(a) Zeigen Sie: Falls es ein $\phi\colon \{1,\dots,l\} \to \{1,\dots,l\}$ gibt mit $\pi(x) = x_{\phi(1)} \dots x_{\phi(l)}$, dann existiert ein ψ mit $N_\pi^2 = N_\psi^1$ (Äquivalenz, siehe Aufgabe 29).

(b) Sei π beliebig, aber fest. Für wieviele der Bijektionen $\psi\colon \mathbb{Z}_2^l \to \mathbb{Z}_2^l$ existiert ein $k \in K$ mit $\forall x \in \mathbb{Z}_2^l : E_\pi^1(k,x) = \psi(x)$?

(c) Sei π fest, sodass es kein Paar $(k_1, k_1') \in K^2 \setminus \{(0,0)\}$ gibt mit $\forall x \in \mathbb{Z}_2^l : \pi(x \oplus k_1) = \pi(x) \oplus k_1'$. Für wieviele der Bijektionen $\psi\colon \mathbb{Z}_2^l \to \mathbb{Z}_2^l$ existiert ein Paar $k = (k_1,k_2) \in K^2$ mit $\forall x \in \mathbb{Z}_2^l : E_\pi^2(k,x) = \psi(x)$?

(d) Zeigen Sie, dass es eine Bijektion $\pi\colon \mathbb{Z}_2^l \to \mathbb{Z}_2^l$ gibt, sodass für alle Bijektionen $\psi\colon \mathbb{Z}_2^l \to \mathbb{Z}_2^l$ gilt: $N_\pi^2 \neq N_\psi^1$.

(e) Geben Sie eine Bijektion $\pi\colon \mathbb{Z}_2^l \to \mathbb{Z}_2^l$ an, für die $N_\pi^l \neq N_\pi^i$ gilt, falls $i < l$.