Übungen zur Kryptologie 1 Wintersemester 05/06
Johannes Köbler/Olaf Beyersdorff

Übungsblatt 8

Aufgabe 30 (mündlich)

Sei $S = (M, C, E, D, K)$ ein Kryptosystem und bezeichne α_{max} den maximalen Vorteil, den ein Gegner (mit unbeschränkten Rechenressourcen) erzielen kann. Zeigen Sie:

a) Wenn $\|K\| < \|M\|$ ist, dann ist $\alpha_{max} > 0$.

b) Wenn $\|K\|(\|K\| - 1) < \|M\|$ ist, dann ist $\alpha_{max} = 1/2$.

c) Über welche Rechenressourcen muss ein optimaler Gegner in Teilaufgabe b) höchstens verfügen, wenn die Verschlüsselungsfunktion E effizient berechenbar ist?

Aufgabe 31 (mündlich)

Seien X_1, X_2, X_3 unabhängige Zufallsvariablen mit Wertebereich $W(X_i) = \{0, 1\}$ und bias $\varepsilon(X_i)$ für $i = 1, 2, 3$. Zeigen Sie, dass die Zufallsvariablen $X_1 \oplus X_2$ und $X_2 \oplus X_3$ genau dann unabhängig sind, wenn $\varepsilon(X_1) = 0$ oder $\varepsilon(X_3) = 0$ oder $\varepsilon(X_2) = \pm 1/2$ ist.

Aufgabe 32 (mündlich)

Sei $\pi_S : \{0,1\}^l \to \{0,1\}^{l'}$ eine S-Box und für $(a, b) \in \{0,1\}^l \times \{0,1\}^{l'}$ sei $L(a, b)$ die Anzahl der Paare $(x, y) \in \{(x, \pi_S(x)) \mid x \in \{0,1\}^l\}$, 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) $\sum_{a \in \{0,1\}^l} L(a, b) = 2^{2l-1} \pm 2^{l-1}$ für alle $b \in \{0,1\}^{l'}$,

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

Aufgabe 33 (schriftlich, 10 Punkte)

Bestimmen Sie für die durch folgende Permutation $\pi_{S'}$ definierte S-Box S' sämtliche Werte $L(a, b)$ für $a, b \in \{0,1\}^4$.

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_{S'}(z)$	8	4	2	1	C	6	3	D	A	5	E	7	F	B	9	0