Übungen zur Kryptologie 1 Wintersemester 2003-2004

Johannes Köbler/Lorenz Weizsäcker

Übungsblatt 9

Aufgabe 32 (schriftlich, 10 Punkte)

a) Bestimmen Sie für die S-Box $\pi_{S'}$ mit

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

sämtliche Werte $L(a, b)$ für $a, b \in \{0, 1\}^4$.

b) Wir betrachten ein SPN mit der S-Box aus Teil a) und der Permutation π_P aus der Vorlesung. Überlegen Sie, wie sich durch lineare Approximation von drei S-Boxen $S^r_{i_r}$, $r = 1, 2, 3$, die lineare Approximation $X_{16} \oplus U^4_1 \oplus U^4_9$ für die Abbildung $x \mapsto u^4$ gewinnen läßt, so dass diese (bei Verwendung des Piling-up Lemmas) einen hypothetischen bias-Absolutwert von $1/16$ hat.

Aufgabe 33

Schreiben Sie ein Programm, das den in der vorigen Aufgabe skizzierten Angriff auf ein SPN mittels linearer Kryptoanalyse ausführt. Testen Sie Ihr Programm mit zufällig generierten Klartext-Kryptotext-Paaren, um die Anzahl t der zur Bestimmung des korrekten Subkey benötigten Paare herauszufinden.

Aufgabe 34

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)

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

Abgabe am 23.1.2004