

Übungsblatt 7

Aufgabe 37

mündlich

Sei $\alpha_S: \{0, 1\}^l \rightarrow \{0, 1\}^{l'}$ eine S-Box und für $(a, b) \in \{0, 1\}^l \times \{0, 1\}^{l'}$ sei $L(a, b)$ die Anzahl der Paare $(x, y) \in \{(x, \alpha_S(x)) \mid x \in \{0, 1\}^l\}$, 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) $\sum_{\substack{a \in \{0, 1\}^l \\ b \in \{0, 1\}^{l'}}} L(a, b) = \begin{cases} 2^{2l+l'-1} + 2^{l+l'-1} & \alpha_S(0^l) = 0^{l'} \\ 2^{2l+l'-1} & \text{sonst.} \end{cases}$

Aufgabe 38

mündlich

Zeigen Sie, dass eine S-Box genau dann affin ist (d.h. es gibt es für jedes Ausgabebit V_j ein $d_j \in \{0, 1\}^l$ und ein $c_j \in \{0, 1\}$ mit $V_j = U_{d_j} \oplus c_j$), wenn für alle $a \in \{0, 1\}^l$ und $b \in \{0, 1\}^{l'}$ der Bias $\varepsilon(U_a \oplus V_b)$ einen der drei Werte in $\{-\frac{1}{2}, 0, \frac{1}{2}\}$ annimmt.

Aufgabe 39

mündlich

Wir betrachten ein SPN mit der S-Box S' (aus Aufgabe 35)

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

und der Permutation π_P aus der Vorlesung. Überlegen Sie, wie sich durch lineare Approximation von drei S-Boxen $S_{i,r}^r$, $r = 1, 2, 3$, die lineare Approximation $X_{16} \oplus U_1^4 \oplus U_9^4$ 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 40

10 Punkte

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 41

mündlich

(a) Wir betrachten das SPN aus der Vorlesung, wobei die S-Box $\pi_{S''}$ mit

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

benutzt wird. Bestimmen Sie die Werte $D(a, b)$ für $a, b \in \{0, 1\}^4$.

(b) Finden Sie geeignete Differentiale für die vier S-Boxen S_1^1, S_4^1, S_4^2 und S_4^3 , um eine Differentialspur mit einem Weitergabequotienten von $2^{27/2048}$ zu bilden.

Aufgabe 42

10 Punkte

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