Übungen zur Kryptologie 1 Wintersemester 05/06

Johannes Köbler/Olaf Beyersdorff

Übungsblatt 9

Aufgabe 34 (mündlich)

a) Wir betrachten ein SPN mit der S-Box S' (aus Aufgabe 33)

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 $S^r_{i_r}$, $r = 1, 2, 3$, 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.

b) Schreiben Sie ein Programm, das den in der vorigen Teilaufgabe 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 35 (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^1_4, S^2_4 und S^3_4, um eine Differentialspur mit einem Weitergabequotienten von $27/2048$ zu bilden.

Aufgabe 36 (schriftlich, 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.