Übungsblatt 8

Abgabe für die schriftlichen Lösungen bis 23.06.2022, 24 Uhr

Aufgabe 42 ***mündlich, 10+5 Punkte***

Sei SP'' das Substitutions-Permutations-Netzwerk, das sich aus dem in Beispiel 97 betrachteten SPN ergibt, indem wir die S-Box S durch folgende S-Box S'' ersetzen:

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

(a) Bestimmen Sie für alle $a', b' \in \{0,1\}^4$ den Wert $D(a', b')$ für S''. ***mündlich***

(b) Finden Sie geeignete Differentiale für die vier S-Boxen S_1^1, S_4^1, S_4^2 und S_4^3, die sich zu einer Differentialspur mit einem hypothetischen Weitergabequotienten von 27/2048 für die Abbildung $x \mapsto u^4$ zusammensetzen lassen. ***5 Punkte***

(c) Schreiben Sie ein Programm, das den in Teilaufgabe (b) skizzierten Angriff auf SP'' 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. Berechnen Sie zusätzlich einen Schätzwert $\tilde{\rho}$ für den Weitergabequotienten der in (b) gefundenen Differentialspur. Hängen die von Ihrem Programm berechneten Werte für t und $\tilde{\rho}$ vom benutzten Schlüssel K ab? ***5+5 (Zusatz-)punkte***

Aufgabe 43 ***mündlich***

Sei $Sym(M) = \{\pi : M \to M \mid \pi \text{ ist bijektiv}\}$ die Menge aller Permutationen auf einer endlichen Menge M und für $\ell > 0$ und $\varnothing \neq \Pi \subseteq Sym(\mathbb{Z}_2^\ell)$ sei $N_\Pi^1 = (\mathbb{Z}_2^\ell, \mathbb{Z}_2^\ell, K^1, E^1, D^1)$ das Kryptosystem, das einen Klartext x mit Schlüssel $k = (\pi, z) \in K^1 = \Pi \times \mathbb{Z}_2^\ell$ zu

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

verschlüsselt, wobei die Addition komponentenweise modulo 2 erfolgt. Für $i \geq 1$ definieren wir induktiv die Kryptosysteme

$$N_\Pi^i = N_\Pi^{i-1} \times N_\Pi^1 \text{ und } N_\Pi^{-i} = (\mathbb{Z}_2^\ell, \mathbb{Z}_2^\ell, K^i, D^i, E^i),$$

wobei das System N_Π^{-i} aus $N_\Pi^i = (\mathbb{Z}_2^\ell, \mathbb{Z}_2^\ell, K^i, E^i, D^i)$ durch Vertauschen der Ver- und Entschlüsselungsfunktion entsteht. Ist $\Pi = \{\pi\}$, so schreiben wir für N_Π^i auch N_π^i.

(a) Zeigen Sie, dass das SPN aus Beispiel 97 für geeignete Permutationen $\pi, \pi' \in Sym(\mathbb{Z}_2^{16})$ auf $N_\pi^4 \times N_{\pi'}^{-1}$ reduzierbar ist.

(b) Sei $T \subseteq Sym(\mathbb{Z}_2^\ell)$ die Menge aller Transpositionen auf $\mathbb{Z}_2^\ell$. Zeigen Sie, dass das System N_T^1 idempotent ist und $N_T^i = N_T^{-i} = N_T^1$ für alle $i \geq 1$ gilt.

(c) Zeigen Sie, dass für jedes $\pi \in Sym(\mathbb{Z}_2^\ell)$ alle Schlüssel in N_π paarweise inäquivalent sind.

(d) Zeigen Sie, dass in N_π^2 alle Schlüssel paarweise inäquivalent sind, falls für jedes Paar $(z, z') \in (\mathbb{Z}_2^\ell \times \mathbb{Z}_2^\ell) \setminus \{(0,0)\}$ ein $x \in \mathbb{Z}_2^\ell$ mit $\pi(x \oplus z) \neq \pi(x) \oplus z'$ existiert.

(e) Zeigen Sie, dass es im Fall $\ell > 2$ eine Permutation $\pi \in Sym(\mathbb{Z}_2^\ell)$ gibt, so dass N_π^2 für kein $\psi \in Sym(\mathbb{Z}_2^\ell)$ äquivalent zu N_ψ^1 ist.

(f) Finden Sie eine Permutation $\pi \in Sym(\mathbb{Z}_2^\ell)$, so dass die Systeme N_π^r für jede Rundenzahl $r \leq (1 - (\log_2 e)/\ell)2^\ell$ paarweise inäquivalent sind. (*Hinweis:* Benutzen Sie, dass $n! \geq \sqrt{2\pi n}(n/e)^n$ für $n \geq 1$ ist und es für jede Permutation $\phi \in Sym(M) \setminus \{id\}$ eine Permutation $\pi \in Sym(M)$ gibt, so dass $\{\phi, \pi\}$ die Gruppe $Sym(M)$ erzeugen.)