Übungsblatt 8

Abgabe für die mündlichen Aufgaben bis 16. 06. 2020 und für die schriftlichen Aufgaben bis 23. 06. 2020

Aufgabe 44 ***mündlich***

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

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

verschlüsselt, wobei die Addition modulo 2 komponentenweise erfolgt.

Zudem definieren wir für $i \geq 1$ induktiv das Kryptosystem $N_P^{i+1} = N_P^i \times N_P^1$. Im Fall $P = \{\pi\}$ schreiben wir für N_P^i auch einfach N_π^i.

(a) Zeigen Sie, dass das SPN aus Beispiel 97 für eine geeignete Permutation $\pi \in Sym(\mathbb{Z}_2^{16})$ auf N_π^5 reduzierbar ist.

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

(c) Sei $\pi \in P$ beliebig. Zeigen Sie, dass in N_π^1 alle Schlüssel $(\pi, z) \neq (\pi, z')$ inäquivalent sind.

(d) Sei $\pi \in P$ eine Permutation, für die kein Paar $(z, z') \in \mathbb{Z}_2^\ell \times \mathbb{Z}_2^\ell \setminus \{(0,0)\}$ mit $\pi(x \oplus z) = \pi(x) \oplus z'$ für alle $x \in \mathbb{Z}_2^\ell$ existiert. Zeigen Sie, dass dann in N_π^2 alle Schlüssel $k \neq k'$ inäquivalent sind.

(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 $\psi \in Sym(\mathbb{Z}_2^\ell)$ äquvalent zu N_ψ^1 ist.

(f) Finden Sie eine Permutation $\pi \in Sym(\mathbb{Z}_2^\ell)$, so dass für eine möglichst große Zahl t alle Systeme N_π^i und N_π^j mit $1 \leq i < j \leq t$ inäquivalent sind.

Aufgabe 45 ***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
$\sigma_{S''}(z)$	E	2	1	3	D	9	0	6	F	4	5	A	8	C	7	B

(a) Bestimmen Sie die Werte $D(a, b)$ für alle $a, b \in \{0,1\}^4$. ***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 Weitergabequotienten von $^{27}/_{2048}$ 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. ***5 Punkte***

(d) Modifizeren Sie Ihre Programme aus Teilaufgabe (c) und Aufgabe 43(c), um den exakten Betrag des Bias der linearen Approximation $X_5 \oplus X_7 \oplus X_8 \oplus U_6^4 \oplus U_8^4 \oplus U_{14}^4 \oplus U_{16}^4$ an das SPN SP im Skript und den exakten Weitergabequotienten der Differentialspur aus Beispiel 105 zu berechnen. Benutzen Sie bei der Berechnung des Weitergabequotienten den Schlüssel von Beispiel 97. ***5 Zusatzpunkte***