Übungsblatt 7

Abgabe der schriftlichen Lösungen bis 16.06.2022, 24 Uhr

Aufgabe 36 ***mündlich, 10+5 Punkte***

Sei SP' das Substitutions-Permutations-Netzwerk, das sich aus dem in Beispiel 97 betrachteten SPN SP 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
$S'(z)$	8	4	2	1	C	6	3	D	A	5	E	7	F	B	9	0

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

(b) Finden Sie für das SPN SP' lineare Approximationen an drei S-Boxen $S^r_{i_r}$, $r = 1,2,3$, aus denen sich die lineare Approximation $\mathcal{A}' = \mathcal{X}_{16} \oplus U^4_1 \oplus U^4_9$ an die Abbildung $x \mapsto u^4$ zusammensetzen lässt. Verifizieren Sie, dass sich mit dem Piling-up Lemma für $\mathcal{A}'$ eine hypothetische Güte von 1/8 ergibt. ***5 Punkte***

(c) Schreiben Sie ein Programm, das den in Teilaufgabe (b) skizzierten Angriff auf SP' 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. Berechnen Sie zusätzlich einen Schätzwert $\tilde{\beta}$ für den Bias von $\mathcal{A}'$. ***5+5 (Zusatz-)punkte***

Aufgabe 37 ***mündlich***

Überlegen Sie, wie sich ein durch ein SPN verschlüsselter Kryptotext $y = E_{f,S,P}(K,x)$ wieder zu x entschlüsseln lässt. Finden Sie einen Key Schedule Algorithmus f', so dass $x = E_{f',S^{-1},P^{-1}}(K,y)$ gilt, wobei S^{-1} und P^{-1} die Inversen von S bzw. P sind.

Aufgabe 38 ***mündlich***

Die affine Hill-Chiffre H mit Blocklänge ℓ über einem Alphabet der Größe m hat den Schlüsselraum $\{(M,z) \in \mathbb{Z}_m^{(\ell\times\ell)} \times \mathbb{Z}_m^\ell \mid \mathrm{ggT}(\det(M), m) = 1\}$ und es gilt $E((M,z),x) = xM + z$ und $D((M,z),y) = (y-z)M^{-1}$. Zeigen Sie:

(a) Die affine Hill-Chiffre ist idempotent.

(b) Jeder Schlüssel $K \in \{0,1\}^k$ eines SPN SP mit Blocklänge ℓ, dessen S-Boxen $\sigma_S : \{0,1\}^l \to \{0,1\}^l$ affin sind, ist auf einen Schlüssel (M,z) einer binären affinen Hill-Chiffre mit Blocklänge ℓ reduzierbar (vgl. Aufgabe 33), wobei die Matrix M nur von SP, aber nicht von K abhängt.

Aufgabe 39 ***mündlich***

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

Aufgabe 40 ***mündlich***

Seien $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3$ unabhängige Zufallsvariablen mit Wertebereich $W(\mathcal{X}_i) = \{0,1\}$ und Bias $\beta_i = \beta(\mathcal{X}_i)$ für $i = 1,2,3$. Zeigen Sie, dass die Zufallsvariablen $\mathcal{X}_1 \oplus \mathcal{X}_2$ und $\mathcal{X}_2 \oplus \mathcal{X}_3$ genau dann unabhängig sind, wenn $\beta_1 = 0$ oder $\beta_3 = 0$ oder $\beta_2 = \pm 1/2$ ist.

Aufgabe 41 ***mündlich***

Zeigen Sie, dass eine S-Box $\sigma_S : \{0,1\}^l \to \{0,1\}^{l'}$ genau dann affin ist (d.h. $\sigma_S(u) = uA \oplus w$ für eine binäre $(l \times l')$-Matrix A und einen Vektor $w \in \{0,1\}^{l'}$), wenn für alle $a \in \{0,1\}^l$ und $b \in \{0,1\}^{l'}$ der Bias $\beta(\mathcal{U}_a \oplus \mathcal{V}_b)$ einen der drei Werte in $\{-1/2, 0, 1/2\}$ annimmt.

Hinweis: Benutzen Sie für die Rückrichtung Aufgabe 39(c).