# Übungsblatt 7

***Abgabe für die mündlichen Aufgaben bis 09. 06. 2020 und für die schriftliche Aufgabe bis 16. 06. 2020***

**Aufgabe 39** ***mündlich***

Sei $E$ die Chiffrierfunktion einer (binären) Blockchiffre $B$ mit Blocklänge $\ell$ und Schlüsselraum $\{0,1\}^k$. Wir betrachten einen Angriff bei *bekanntem Klartext*, d. h. es steht eine ausreichende Zahl von Klartext-Kryptotext-Paaren $(x_i, y_i), i = 1, \ldots, t$, zur Verfügung, die alle mit demselben unbekannten Schlüssel $K_0$ generiert wurden.

(a) Schätzen Sie die erwartete Anzahl von Schlüsseln $K \neq K_0$ nach oben ab, die zu allen Paaren $(x_i, y_i)$ »passen«, d. h. für $i = 1, \ldots, t$ gilt $E_K(x_i) = y_i$. Folgern Sie, dass im Fall $t > k/\ell$ mit hoher Wahrscheinlichkeit nur $K_0$ zu allen Paaren passt.

*Hinweis:* Gehen Sie von der (für den Anwender idealen) Annahme aus, dass $\Pr[E_K(x_i) = y_i] = 2^{-\ell}$ für einen zufällig gewählten Schlüssel $K$ gilt (auch wenn bereits bekannt ist, dass $K$ gewisse Klartexte $x_j \neq x_i$ zu $E_K(x_j) = y_j$ chiffriert).

(b) Wie lässt sich der benutzte Schlüssel $K$ im Fall $t > k/\ell$ (mit hoher Wahrscheinlichkeit) durch einen Brute-Force Angriff mittels $t2^k$ Verschlüsselungen bestimmen?

(c) Um die Sicherheit zu erhöhen, wird nun das Kryptosystem $B \times B$ verwendet, d. h. die Schlüssellänge verdoppelt sich auf $2k$. Zeigen Sie, dass sich dadurch die benötigte Anzahl $t$ an Klartext-Kryptotext-Paaren $(x_i, y_i)$ unter der idealisierten Annahme in Teilaufgabe (a) ebenfalls (auf $> 2k/\ell$) verdoppelt.

(d) Wie lässt sich im Fall $t > 2k/\ell$ der benutzte Schlüssel $(K, K')$ unter Verwendung eines Speichers der Größe $(\ell t + k)2^k$ mittels $t2^{k+1}$ Ver- und Entschlüsselungen bestimmen?

(e) Überlegen Sie, wie sich der Platzbedarf in (d) auf Kosten der Rechenzeit reduzieren lässt. Suchen Sie nach einer möglichst allgemeinen Beziehung für diesen so genannten *Time-Memory-Tradeoff*.

**Aufgabe 40** ***mündlich***

Seien $X_1, X_2, X_3$ unabhängige Zufallsvariablen mit Wertebereich $W(X_i) = \{0,1\}$ und Bias $\varepsilon_i = \varepsilon(X_i)$ für $i = 1, 2, 3$. Zeigen Sie, dass die Zufallsvariablen $X_1 \oplus X_2$ und $X_2 \oplus X_3$ genau dann unabhängig sind, wenn $\varepsilon_1 = 0$ oder $\varepsilon_3 = 0$ oder $\varepsilon_2 = \pm 1/2$ 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 $\varepsilon(U_a \oplus V_b)$ einen der drei Werte in $\{-\frac{1}{2}, 0, \frac{1}{2}\}$ annimmt.

**Aufgabe 42** ***mündlich***

Die affine Hill-Chiffre mit Blocklänge $\ell$ 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 $\ell$, 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 $\ell$ reduzierbar (vgl. Aufgabe 33), wobei die Matrix $M$ nur von *SP*, aber nicht von $K$ abhängt.

**Aufgabe 43** ***mündlich, 10 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\sigma_{S'}(z)$ | 8 | 4 | 2 | 1 | C | 6 | 3 | D | A | 5 | E | 7 | F | B | 9 | 0 |

(a) Bestimmen Sie für die S-Box $S'$ sämtliche Werte $L(a,b)$ für $a, b \in \{0,1\}^4$. ***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 $L = X_{16} \oplus U_1^4 \oplus U_9^4$ an die Abbildung $x \mapsto u^4$ zusammensetzen lässt. Verifizieren Sie, dass sich mit dem Piling-up Lemma für $L$ ein hypothetischer Bias-Absolutwert von $1/16$ 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. ***5 Punkte***