Übungsblatt 4

Besprechung der mündlichen Aufgaben am 4. 12. 2020
Abgabe der schriftlichen Lösungen bis 8. 12. 2020, 23:59 Uhr

Aufgabe 22 ***mündlich***

Zeigen Sie, dass die in der Vorlesung hergeleitete Entropieschranke für die Impersonationswahrscheinlichkeit α »scharf« ist.

Hinweis: Betrachten Sie einen beliebigen 2-universalen MAC.

Aufgabe 23 ***mündlich***

(a) Konstruieren Sie für jede Primzahl p und jede natürliche Zahl $d \geq 2$ einen 2-universalen (n, m, l)-MAC mit $n = (p^d - 1)/(p - 1)$, $m = p$ und $l = p^d$.

(b) Sei H ein 2-universaler (n, m, l)-MAC. Konstruieren Sie auf der Basis von H einen 2-universalen (n, m^d, l^d)-MAC H'.

Aufgabe 24 ***mündlich***

Ein (n, m, l)-MAC heißt **(stark) j-universal**, falls für alle $x_1, \ldots, x_j \in X$ mit $x_i \neq x_{i'}$ für $i \neq i'$ und alle $y_1, \ldots, y_j \in Y$ gilt:

$$\left\| \left\{ k \in K \;\middle|\; h_k(x_i) = y_i \text{ für } i = 1, \ldots, j \right\} \right\| = \frac{\|K\|}{m^j} \quad .$$

(a) Zeigen Sie, dass jeder j-universale MAC auch j'-universal ist, falls $1 \leq j' \leq j$ gilt.

(b) Konstruieren Sie für jede Primzahl p und jedes $j \geq 1$ einen j-universalen (p, p, p^j)-MAC.

Hinweis: Betrachten Sie die Menge aller Polynome vom Grad höchstens $j - 1$ über dem Körper $\mathbb{F}_p$.

Aufgabe 25 ***mündlich***

Konstruieren Sie einen 2-universalen $(6, 5, l)$-MAC und einen 2-universalen $(13, 3, l')$-MAC für geeignete l, l'.

Aufgabe 26 ***mündlich***

Sei (X, Y, K, H) ein (n, m, l)-MAC mit $\alpha, \beta \leq j^{-1}$. Wie groß muss dann der Schlüsselraum K mindestens sein, wenn der Schlüssel unter Gleichverteilung gewählt wird?

Aufgabe 27 ***mündlich***

Für eine Primzahl $p > 2$ und ein Paar $(a, b) \in K = \mathbb{Z}_p \times \mathbb{Z}_p$ sei die Funktion $h_{(a,b)} : \mathbb{Z}_p \to \mathbb{Z}_p$ definiert durch $h_{(a,b)}(x) = (x + a)^2 + b \bmod p$. Zeigen Sie, dass (X, Y, K, H) mit $X = Y = \mathbb{Z}_p$ und $H = \{h_k \mid k \in K\}$ ein $(p, p, p^2, 1)$-MAC ist.

Aufgabe 28 ***mündlich***

Sei $E_k \colon \{0,1\}^l \to \{0,1\}^l$, $k \in K$, eine Familie von Verschlüsselungsfunktionen. Betrachten Sie für eine Konstante $d \geq 2$ den MAC (X, Y, K, H) mit $X = \{0,1\}^{dl}$, $Y = \{0,1\}^l$ und $H = \left\{h_k \,\middle|\, k \in K\right\}$, wobei $h_k \colon X \to Y$ durch

$$h_k(x_1 \cdots x_d) = E_k(x_1) \oplus \cdots \oplus E_k(x_d), |x_1| = \cdots = |x_d| = l$$

definiert ist.

(a) Geben Sie im Fall d gerade einen existentiellen $(1, 0)$-Fälscher für diesen MAC an.

(b) Geben Sie einen selektiven $(1, 1)$-Fälscher für diesen MAC an.

Aufgabe 29 ***10 Punkte***

Sei $E_k \colon \{0,1\}^l \to \{0,1\}^l$, $k \in K$, eine Familie von Verschlüsselungsfunktionen. Betrachten Sie für eine Konstante $d \geq 2$ den MAC (X, Y, K, H) mit $X = \{0,1\}^{dl}$, $Y = \{0,1\}^l$ und $H = \left\{h_k \,\middle|\, k \in K\right\}$, wobei $h_k \colon X \to Y$ durch

$$h_k(x_1 \cdots x_d) = E_k(x_1) + 3E_k(x_2) + \cdots + (2d-1)E_k(x_d) \bmod 2^l, |x_1| = \cdots = |x_d| = l$$

definiert ist. Hierbei identifizieren wir einen Binärstring $x_{l-1} \ldots x_0 \in \{0,1\}^l$ mit der Zahl $\sum_{i=0}^{l-1} x_i 2^i \in \mathbb{Z}_{2^l}$.

(a) Geben Sie einen existentiellen $(1, 2)$-Fälscher für diesen MAC an.

(b) Geben Sie einen selektiven $(1, 3)$-Fälscher für diesen MAC an.