Kryptologie 2 Sommersemester 2010
Johannes Köbler, Sebastian Kuhnert 28. April 2010

Übungsblatt 3

Aufgabe 15 ***mündlich***

Angenommen, Sie wollen Nachrichten über dem 26-stelligen Alphabet $\{A, \ldots, Z\}$ der Länge 1000 authentisieren. Wie könnte ein entsprechender MAC aussehen, falls die Erfolgswahrscheinlichkeit eines Gegners bei Durchführung eines Impersonations- oder Substitutionsangriffs nicht größer als 10^{-4} sein soll?

Aufgabe 16 ***mündlich***

(a) Geben Sie einen MAC an, bei dem $\alpha > \beta$ gilt.
(b) Zeigen Sie, dass für jede (n, m, l)-Hashfamilie gilt: $\beta = 1/m \Rightarrow \alpha = 1/m$.

Aufgabe 17 ***mündlich***

Sei eine Textmenge X und eine Menge Y von Hashwerten mit $\|Y\| = m$ vorgegeben. Charakterisieren Sie die MACs mit dem optimalen Wert $\alpha = 1/m$ und minimaler Schlüsselmenge K (bei geeigneter Wahl der Wahrscheinlichkeitsverteilung auf K).

Aufgabe 18 ***mündlich***

Sei A eine $m \times l$-Matrix über einem endlichen Körper K und sei $y \in K^m$. Zeigen Sie, dass das Gleichungssystem $Ax = y$ im Falle der Lösbarkeit genau $\|K\|^{l-r}$ Lösungen besitzt, falls r der Rang von A ist. Geben Sie eine notwendige und hinreichende Bedingung dafür an, dass das Gleichungssystems für alle $y \in K^m$ lösbar ist.

Aufgabe 19 ***mündlich***

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

Hinweis: Betrachten Sie eine beliebige stark universale Hashfamilie.

Aufgabe 20 ***mündlich***

(a) Konstruieren Sie für jede Primzahl p und jede natürliche Zahl $d \geq 2$ eine stark universale (n, m, l)-Hashfamilie mit $n = (p^d - 1)/(p - 1)$, $m = p$ und $l = p^d$.
(b) Sei H eine stark universale (n, m, l)-Hashfamilie. Konstruieren Sie auf der Basis von H eine stark universale (n, m^d, l^d)-Hashfamilie H'.

Aufgabe 21 ***mündlich***

Zeigen Sie, dass für eine Zufallsvariable X mit endlichem Wertebereich $W(X) \subseteq \mathbb{R}^+$ immer $E(\log X) \leq \log E(X)$ gilt.

Hinweis: Benützen Sie die Ungleichung von Jensen.

Aufgabe 22 ***mündlich***

Eine (n, m, l)-Hashfamilie 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:

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

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

(b) Konstruieren Sie für jede Primzahl p und jedes $j \geq 1$ eine stark j-universale (p, p, p^j)-Hashfamilie.

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

Aufgabe 23 ***mündlich***

Sei H eine stark universale (n, m, l)-Hashfamilie und sei $\lambda = l/m^2$.

(a) Wieviele Text-Hashwert-Paare $(x_i, h_k(x_i))$ $(i = 1, \ldots, j)$ benötigt der Gegner im Fall $\lambda = 1$ höchstens, um mit Erfolgswahrscheinlichkeit 1 ein gültiges Paar $(x, h_k(x))$ für den unbekannten Schlüssel k mit $x \notin \{x_1, \ldots, x_j\}$ generieren zu können?

(b) Mit welcher Erfolgswahrscheinlichkeit kann ein Gegner bei Kenntnis von 2 Text-Hashwert-Paaren $(x_i, h_k(x_i))$ ein gültiges Paar $(x, h_k(x))$ für den unbekannten Schlüssel k mit $x \notin \{x_1, x_2\}$ generieren?

Aufgabe 24 ***mündlich***

Zeigen Sie, dass für beliebige reelle Zahlen $a_1, \ldots, a_m$ folgende Ungleichung gilt:

$$\left(\sum_{i=1}^{m} a_i\right)^2 \leq m \sum_{i=1}^{m} a_i^2.$$

Aufgabe 25 ***mündlich***

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

Aufgabe 26 ***6 Punkte***

Konstruieren Sie eine stark universale $(6, 5, l)$-Hashfamilie und eine stark universale $(13, 3, l')$-Hashfamilie für geeignete l, l'.

Aufgabe 27 ***4 Punkte***

Schreiben Sie ein Programm, das für den MAC aus Aufgabe 12 die Entropiewerte $\mathcal{H}(K)$ und $\mathcal{H}(K \mid X, Y)$ und daraus die in der Vorlesung hergeleitete Entropieschranke für α berechnet. Vergleichen Sie diese Schranke mit dem tatsächlichen Wert von α.