

Übungsblatt 3

Aufgabe 15

Angenommen, Sie wollen Nachrichten über dem 26-stelligen Alphabet $\{A, \dots, Z\}$ 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

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

Aufgabe 17

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

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 Gleichungssystem für alle $y \in K^m$ lösbar ist.

Aufgabe 19

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

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

Aufgabe 21

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

Eine (n, m) -Hashfamilie heißt **stark l -universal**, falls für alle $x_1, \dots, x_l \in X$ mit $x_i \neq x_j$ für $i \neq j$ und alle $y_1, \dots, y_l \in Y$ gilt:

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

- Zeigen Sie, dass jede stark l -universale Hashfamilie auch stark l' -universal ist, falls $1 \leq l' \leq l$ gilt.
- Konstruieren Sie für jede Primzahl p und jedes $l \geq 1$ eine stark l -universale (p, p) -Hashfamilie der Größe $\|K\| = p^l$.

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

Aufgabe 23

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

- Wieviele Text-Hashwert-Paare $(x_i, h_k(x_i))$ ($i = 1, \dots, l$) benötigt der Gegner im Fall $\lambda = 1$ höchstens, um mit Erfolgswahrscheinlichkeit 1 ein gültiges Paar $(x, h_k(x))$ für den unbekanntes Schlüssel k mit $x \notin \{x_1, \dots, x_l\}$ generieren zu können?
- 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 unbekanntes Schlüssel k mit $x \notin \{x_1, x_2\}$ generieren?

Aufgabe 24

Zeigen Sie, dass für beliebige reelle Zahlen a_1, \dots, 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

Sei H eine (n, m) -Hashfamilie mit $\alpha, \beta \leq M^{-1}$. 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 $(6, 5)$ -Hashfamilie und eine stark universale $(13, 3)$ -Hashfamilie.

Aufgabe 27 (4 Punkte)

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