

Übungsblatt 2

Aufgabe 9 Für eine (n, m) -Hashfunktion $h: X \rightarrow Y$ und für $y \in Y$ sei **mündlich** $h^{-1}(y) = \{x \in X \mid h(x) = y\}$ die Menge aller Texte mit Hashwert y .

- (a) Bestimmen Sie die Verteilung und den Erwartungswert \bar{s} der Zufallsvariablen $S_y = \|h^{-1}(y)\|$ im ZOM.
- (b) Zeigen Sie (S ist dabei die Anzahl aller Kollisionspaare von h):

$$\sum_{y \in Y} (S_y - \bar{s})^2 = 2S + n - \frac{n^2}{m}, \text{ mit } S = \|\{\{x, x'\} \in \binom{X}{2} \mid h(x) = h(x')\}\|$$

- (c) Zeigen Sie, dass

$$S \geq \frac{1}{2} \left(\frac{n^2}{m} - n \right)$$

ist, wobei Gleichheit nur im Fall $S_y = \frac{n}{m}$ für alle $y \in Y$ eintritt.

Aufgabe 10 **mündlich**
 Sei $h: X \rightarrow Y$ eine *balancierte* (n, m) -Kompressionsfunktion (d.h. $\|h^{-1}(y)\| = n/m$ für alle Hashwerte y und es gilt $m \leq n/2$). Sei A ein probabilistischer Invertierungsalgorithmus für h , der mit Wahrscheinlichkeit ε für einen zufällig gewählten Hashwert y ein Urbild x mit $h(x) = y$ berechnet.

- (a) Konstruieren Sie einen Las-Vegas Algorithmus B , der mit Wahrscheinlichkeit mindestens $\varepsilon/2$ eine Kollision für h aufspürt.
- (b) Wieviele Hashwertberechnungen führt B höchstens aus, falls A nicht mehr als q Hashwertberechnungen benötigt?

Aufgabe 11 **mündlich**
 Sei $h: \{0, 1\}^{m+t} \rightarrow \{0, 1\}^m$ eine kollisionsresistente Kompressionsfunktion. Welche zusätzliche Eigenschaft sollte h besitzen, damit folgende Konstruktion eine kollisionsresistente Hashfunktion $\hat{h}: \bigcup_{r \geq 1} \{0, 1\}^{rt} \rightarrow \{0, 1\}^m$ liefert?

Sei $IV = 0^m$ und sei $x = x_1 \cdots x_r$ mit $|x_i| = t$ für $i = 1, \dots, r$. Definiere $\hat{h}(x) = y_r$, wobei y_0, \dots, y_r eine Folge von Strings $y_i \in \{0, 1\}^m$ ist mit:

$$y_i = \begin{cases} IV, & i = 0, \\ h(y_{i-1}x_i), & i = 1, \dots, r, \end{cases}$$

Aufgabe 12 **mündlich**
 Seien X, Y Zufallsvariablen mit endlichen Wertebereichen $W(X)$ bzw. $W(Y)$. Dann ist die **Entropie** von X definiert als $H(X) = \sum_{x \in W(X)} p(x) \text{Inf}_X(x)$, wobei

$$\text{Inf}_X(x) = \begin{cases} \log_2(1/p(x)), & p(x) > 0 \\ 0, & \text{sonst} \end{cases}$$

der **Informationsgehalt** von x ist. Weiter sei $H(X, Y) = \sum_{x,y} p(x, y) \log_2 \frac{1}{p(x, y)}$ die Entropie der Zufallsvariablen (X, Y) mit Wertebereich $W(X) \times W(Y)$ und $H(X|Y) = \sum_y p(y)H(X|y)$ mit $H(X|y) = \sum_x p(x|y) \log_2 \frac{1}{p(x|y)}$ die **bedingte Entropie** von X unter Y . Zeigen Sie:

- (a) $H(X) \leq \log_2(n)$, wobei $n = \|W\|$ ist und Gleichheit genau im Fall $p(x) = 1/n$ für alle $x \in W$ eintritt.
- (b) $H(X, Y) = H(Y) + H(X|Y) = H(X) + H(Y|X)$.
- (c) $H(X, Y) \leq H(X) + H(Y)$, mit Gleichheit genau dann, wenn X und Y stochastisch unabhängig sind.

Aufgabe 13 **mündlich**
 Sei $h: \{0, 1\}^{m+t} \rightarrow \{0, 1\}^m$ eine kollisionsresistente Kompressionsfunktion. Wie in der Vorlesung gezeigt, kann h zu einer kollisionsresistenten Hashfunktion $\hat{h}: \{0, 1\}^* \rightarrow \{0, 1\}^m$ erweitert werden, sofern hierzu ein öffentlich bekannter Initialisierungsvektor $IV \in \{0, 1\}^m$ und eine suffixfreie Preprocessing-Funktion y verwendet werden (wobei wir auf die optionale Ausgabetransformation verzichten).

Für die Preprocessing-Funktion wird meist eine Funktion der Bauart $y(x) = x \text{pad}(x)$ verwendet, wobei $\text{pad}: \{0, 1\}^* \rightarrow \{0, 1\}^*$ eine so genannte Paddingfunktion mit $|x| + |\text{pad}(x)| \equiv_t 0$ ist. Um nun einen MAC zu konstruieren, könnte man $K = \{0, 1\}^m$ als Schlüsselraum wählen und bei der Berechnung von $\hat{h}(x)$ anstelle von IV den geheimen Schlüssel k benutzen, um $h_k(x)$ zu erhalten. Zeigen Sie, dass der so konstruierte MAC nicht berechnungsresistent ist.

Aufgabe 14 **10 Punkte**

- (a) Schreiben Sie ein Programm, das bei Eingabe von m und q die exakte Erfolgswahrscheinlichkeit ε von $\text{COLLISION}(h, q)$ im ZOM berechnet.
- (b) Vergleichen Sie die exakten Werte für $m = 365$ und $q = 1, 5, 10, 15, 20, 22, 23, 25, 30$ mit den approximativen Werten $1 - e^{-\frac{q^2}{2m}}$ bzw. $q^2/2m$.
- (c) Schreiben Sie ein Programm, das bei Eingabe von m und ε die Anzahl q von Hashwertberechnungen berechnet, die $\text{COLLISION}(h, q)$ im ZOM benötigt, um eine Erfolgswahrscheinlichkeit von mindestens ε zu erreichen.
- (d) Vergleichen Sie für $\varepsilon = 1/2$ und $m \in \{10, 50, 100, 200, 365, 1000\}$ die exakten Werte von q mit den approximativen Werten $1, 17\sqrt{m}$ bzw. \sqrt{m} .