

## Übungsblatt 2

### Aufgabe 9

*mündlich*

Sei  $h : X \rightarrow Y$  eine beliebige, aber feste  $(n, m)$ -Hashfunktion.

- Bestimmen Sie die Erfolgswahrscheinlichkeit  $\varepsilon(h, x, q)$  von  $\text{FINDSECONDPREIMAGE}(h, x, q)$ , falls für  $X_0$  eine zufällige Teilmenge von  $X \setminus \{x\}$  der Größe  $q - 1$  gewählt wird.
- Bestimmen Sie die durchschnittliche Erfolgswahrscheinlichkeit  $\varepsilon(h, q)$  von  $\text{FINDSECONDPREIMAGE}(h, x, q)$ , falls  $X_0$  wie in (a) und  $x$  zufällig aus  $X$  gewählt wird.
- Berechnen Sie  $\varepsilon(h, 2)$ .

### 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  $\varepsilon$  für einen zufällig gewählten Hashwert  $y$  ein Urbild  $x$  mit  $h(x) = y$  berechnet.

- Konstruieren Sie einen Las-Vegas Algorithmus  $B$ , der mit Wahrscheinlichkeit mindestens  $\varepsilon/2$  eine Kollision für  $h$  aufspürt.
- 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. 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 12

*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  $i = 1, \dots, r$ . Berechne eine Folge  $y_0, \dots, y_r$  von Strings  $y_i \in \{0, 1\}^m$  mit

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

und definiere  $\hat{h}(x) = y_r$ .

### Aufgabe 13

*mündlich*

Sei  $X$  eine Zufallsvariable mit endlichem Wertebereich  $W$  und für  $x \in W$  sei  $p(x) = \Pr[X = x]$ . Dann ist die **Entropie** von  $X$  definiert als  $\mathcal{H}(X) = \sum_x p(x) \log_2(1/p(x))$ , wobei

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

der **Informationsgehalt** von  $x$  ist. Für zwei Zufallsvariablen  $X$  und  $Y$  sei  $\mathcal{H}(X, Y) = \sum_{x,y} p(x,y) \cdot \log_2(1/p(x,y))$  die (gemeinsame) Entropie von  $X$  und  $Y$ . Zeigen Sie:

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

### Aufgabe 14

**10 Punkte**

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