Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Kryptologie - WiSe 2022/23
25. Oktober 2022

Übungsblatt 2

Besprechung der mündlichen Aufgaben am 3. 11. 2022
Abgabe der schriftlichen Lösungen bis 8. 11. 2022, 23:59 Uhr

Aufgabe 9 ***mündlich***

Sei $h\colon X \to Y$ eine *balancierte* (n,m)*-Kompressionsfunktion* (d.h. $\left\|h^{-1}(y)\right\| = n/m$ 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 (und sonst ? ausgibt).

(b) Wieviele Hashwertberechnungen führt B höchstens aus, falls A nicht mehr als q Hashwertberechnungen benötigt?

Aufgabe 10 ***mündlich***

Für eine feste (n,m)-Hashfunktion $h\colon X \to Y$ und für $y \in Y$ sei $h^{-1}(y) = \left\{x \in X \;\middle|\; h(x) = y\right\}$ die Menge aller Texte mit Hashwert y und $c_y = \left\|h^{-1}(y)\right\|$ deren Anzahl. Weiter sei $s(h) = \|\{\{x,x'\} \in \binom{X}{2} \mid h(x) = h(x')\}\|$ die Anzahl aller Kollisionspaare von h. Für eine auf Y gleichverteilte Zufallsvariable $\mathcal{Y}$ bezeichne $\sigma(h)$ die Varianz und $\overline{c}(h)$ den Erwartungswert von $c_{\mathcal{Y}}$.

(a) Bestimmen Sie $\sigma(h)$ und $\overline{c}(h)$.

(b) Zeigen Sie: $s(h) = \frac{1}{2}\left(m\sigma(h) + n^2/m - n\right)$.

(c) Zeigen Sie, dass $s(h) \geq \frac{1}{2}\left(n^2/m - n\right)$ ist, wobei Gleichheit genau dann gilt, wenn h balanciert ist.

Aufgabe 11 ***mündlich***

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

> Sei $IV = 0^m$ und sei $x = x_1 \cdots x_r$ mit $|x_i| = t$ für $i = 1,\ldots,r$. Berechne eine Folge $y_0,\ldots,y_r$ von Strings $y_i \in \{0,1\}^m$ mit
>
> $$y_i = \begin{cases} IV, & i = 0, \\ h(y_{i-1}x_i), & i = 1,\ldots,r, \end{cases}$$
>
> und definiere $\hat{h}(x) = y_r$.

Aufgabe 12 ***mündlich***

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

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

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

(a) $H(\mathcal{X}) \leq \log_2(n)$, wobei $n = \|W\|$ ist und Gleichheit genau im Fall $p(x) = 1/n$ für alle $x \in W$ eintritt.

(b) $H(\mathcal{X}, \mathcal{Y}) = H(\mathcal{Y}) + H(\mathcal{X}|\mathcal{Y}) = H(\mathcal{X}) + H(\mathcal{Y}|\mathcal{X})$.

(c) $H(\mathcal{X}, \mathcal{Y}) \leq H(\mathcal{X}) + H(\mathcal{Y})$, mit Gleichheit genau dann, wenn $\mathcal{X}$ und $\mathcal{Y}$ stochastisch unabhängig sind.

Aufgabe 13 ***10 Punkte***

(a) Schreiben Sie ein Programm, das bei Eingabe von m und q die exakte Erfolgswahrscheinlichkeit ε von $\textsc{Collision}(h, q)$ 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 $\textsc{Collision}(h, q)$ 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. $\sqrt{m}$.