

Übungsblatt 1

*Besprechung der mündlichen Aufgaben am 27. 10. 2022
Abgabe der schriftlichen Lösungen bis 1. 11. 2022, 23:59 Uhr*

Aufgabe 1

mündlich

Sei $f: \{0, 1\}^k \rightarrow \{0, 1\}^k$ wie folgt definiert (dabei identifizieren wir $\{0, 1\}^k$ mit \mathbb{Z}_{2^k})

$$f(x) = (x^2 + ax + b) \bmod 2^k$$

Zeigen Sie, dass f nicht schwach kollisionsresistent ist.

Aufgabe 2

mündlich

Sei $k > l$ und seien $a_i \in \mathbb{Z}_{2^l}$ für $i = 0, \dots, d$ mit $a_d \neq 0$. Zeigen Sie, dass die durch

$$f(x) = \left(\sum_{i=0}^d a_i x^i \right) \bmod 2^l$$

definierte Funktion $f: \{0, 1\}^k \rightarrow \{0, 1\}^l$ nicht schwach kollisionsresistent ist.

Aufgabe 3

mündlich

Sei $f: \{0, 1\}^m \rightarrow \{0, 1\}^m$ eine Einwegpermutation (also eine bijektive Einweg-Hashfunktion). Zeigen Sie, dass die durch

$$h(x_1 x_2) = f(x_1 \oplus x_2), \quad x_1, x_2 \in \{0, 1\}^m$$

definierte Funktion $h: \{0, 1\}^{2m} \rightarrow \{0, 1\}^m$ nicht schwach kollisionsresistent, aber immer noch eine Einweg-Hashfunktion ist.

Aufgabe 4

mündlich

Seien $h_i: X \rightarrow Y_i$ (n, m_i)-Hashfunktionen (für $i = 1, 2$), von denen mindestens eine kollisionsresistent ist. Zeigen Sie, dass dann die Funktion

$$h(x) = h_1(x)h_2(x) \quad (\text{Konkatenation})$$

kollisionsresistent ist.

Aufgabe 5

mündlich

Sei $h_1: \{0, 1\}^{2m} \rightarrow \{0, 1\}^m$ kollisionsresistent. Zeigen Sie, dass dann auch die durch

$$h_i(x_1 x_2) = h_1(h_{i-1}(x_1)h_{i-1}(x_2)), \quad x_1, x_2 \in \{0, 1\}^{2^{i-1}m}, i \geq 2$$

induktiv definierten Hashfunktionen $h_i: \{0, 1\}^{2^i m} \rightarrow \{0, 1\}^m$ kollisionsresistent sind.

Aufgabe 6*mündlich*

Sei $n = pq$ für zwei Primzahlen $p > q$. Betrachten Sie die Funktion

$$h(x) = x^2 \bmod n, \quad x \in \mathbb{Z}_n^* .$$

Welche Eigenschaften (Einweg-Hashfunktion, (schwache) Kollisionsresistenz) hat h , falls n nur mit sehr hohem Aufwand faktorisiert werden kann?

Aufgabe 7*mündlich*

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

Hinweis: Nutzen Sie für diese und die nächste Aufgabe, dass die Anzahl der (weiteren) Urbilder hypergeometrisch verteilt ist bzw. argumentieren Sie mit Hilfe des Urnenmodells ohne Zurücklegen.

- Bestimmen Sie die Erfolgswahrscheinlichkeit $\varepsilon(h, x, q)$ von `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 `FINDSECONDPREIMAGE`(h, x, q), falls X_0 wie in (a) und x zufällig aus X gewählt werden.
- Berechnen Sie $\varepsilon(h, 2)$.

Aufgabe 8**10 Punkte**

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

- Zeigen Sie, dass für zufällig unter Gleichverteilung aus X gewählte Texte x_1, x_2

$$\Pr [h(x_1) = h(x_2)] \geq \frac{1}{m}$$

ist, wobei Gleichheit nur im Fall $c_y = \|h^{-1}(y)\| = \frac{n}{m}$ für alle $y \in Y$ eintritt.

- Bestimmen Sie für einen gegebenen Hashwert y die Erfolgswahrscheinlichkeit $\varepsilon(h, y, q)$ von `FINDPREIMAGE`(h, y, q), falls für X_0 eine zufällige Teilmenge von X der Größe q gewählt wird.
- Berechnen Sie die durchschnittliche Erfolgswahrscheinlichkeit $\varepsilon(h, q)$ von `FINDPREIMAGE`(h, y, q), falls X_0 wie in (b) und y zufällig aus Y gewählt werden.
- Bestimmen Sie $\varepsilon(h, 1)$.