

## Übungsblatt 1

### Aufgabe 1 *mündlich*

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

$$f(x) = x^2 + ax + b \pmod{2^k}$$

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

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

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

### Aufgabe 3 *mündlich*

Sei  $f: \{0, 1\}^m \rightarrow \{0, 1\}^m$  eine Einwegpermutation. 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 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

$$h(x) = h_1(x)h_2(x)$$

kollisionsresistent ist.

### Aufgabe 5 *mündlich*

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

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

induktiv definierten Hashfunktionen  $h_i$  ( $i \geq 2$ ) kollisionsresistent sind.

### Aufgabe 6 *mündlich*

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

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

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

### Aufgabe 7 *mündlich*

Für eine  $(n, m)$ -Hashfunktion  $h: X \rightarrow Y$  und für  $y \in Y$  sei

$$h^{-1}(y) = \{x \in X \mid h(x) = y\}$$

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:

$$\sum_{y \in Y} (S_y - \bar{s})^2 = 2S + n - \frac{n^2}{m},$$

wobei  $S$  die Anzahl  $\left\| \left\{ \{x, x'\} \in \binom{X}{2} \mid h(x) = h(x') \right\} \right\|$  aller Kollisionspaare von  $h$  bestimmt.

(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 8 *10 Punkte*

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

(a) 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  $S_y = \|h^{-1}(y)\| = \frac{n}{m}$  für alle  $y \in Y$  eintritt.

(b) Bestimmen Sie für einen gegebenen Hashwert  $y$  die Erfolgswahrscheinlichkeit  $\epsilon(h, y, q)$  von  $\text{FINDPREIMAGE}(h, y, q)$ , falls für  $X_0$  eine zufällige Teilmenge von  $X$  der Größe  $q$  gewählt wird.

(c) Berechnen Sie die durchschnittliche Erfolgswahrscheinlichkeit  $\epsilon(h, q)$  von  $\text{FINDPREIMAGE}(h, y, q)$ , falls  $X_0$  wie in (b) und  $y$  zufällig aus  $Y$  gewählt werden.

(d) Bestimmen Sie  $\epsilon(h, 1)$ .