Institut für Informatik
Komplexität und Kryptografie
Prof. Dr. Johannes Köbler

Sommersemester 2006

Übungen zur Kryptologie 2

3. Aufgabenblatt

Aufgabe 1

Sei h eine balancierte (n, m)-Kompressionsfunktion (d.h. $\|h^{-1}\| = n/m$ 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 2

Eine (n, m)-Hashfamilie heißt **stark l-universal**, falls für alle $x_1, \ldots, x_l \in X$ mit $x_i \neq x_j$ für $i \neq j$ und alle $y_1, \ldots, y_l \in Y$ gilt:

$$\|\{k \in K \mid h_k(x_i) = y_i \text{ für } i = 1, \ldots, l\}\| = \frac{\|K\|}{m^l}.$$

a) Zeigen Sie, dass jede stark l-universale Hashfamilie auch stark l'-universal ist, falls $1 \leq l' \leq l$ gilt.

b) Konstruieren Sie für jede Primzahl p und jedes $l \geq 1$ eine stark l-universale (p, p)-Hashfamilie der Größe $\|K\| = p^l$.

Hinweis: Betrachten Sie die Menge aller Polynome vom Grad höchstens $l - 1$ über dem Körper $\mathbb{F}_p$.

Aufgabe 3

Sei H eine stark universale (n, m)-Hashfamilie und sei $\lambda = \|K\|/m^2$.

a) Wieviele Text-Hashwert-Paare $(x_i, h_k(x_i))$ $(i = 1, \ldots, l)$ benötigt der Gegner im Fall $\lambda = 1$ höchstens, um mit Erfolgswahrscheinlichkeit 1 ein gültiges Paar $(x, h_k(x))$ für den unbekannten Schlüssel k mit $x \notin \{x_1, \ldots, x_l\}$ generieren zu können?

b) Mit welcher Erfolgswahrscheinlichkeit kann ein Gegner bei Kenntnis von 2 Text-Hashwert-Paaren $(x_i, h_k(x_i))$ ein gültiges Paar $(x, h_k(x))$ für den unbekannten Schlüssel k mit $x \notin \{x_1, x_2\}$ generieren?

Aufgabe 4 (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 $q \in \{15, \ldots, 30\}$ mit den approximativen Werten $q^2/2m$.

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 $\sqrt{m}$.