Kryptographische Algorithmen

Blatt 3 05.05.2004, Abgabe 12.05.2004

Aufgabe 1. Sei $F_n \in_R [n]^{[n]}, x_{i+1} := F_n(x_i)$. Zeige:

1. $\mathbf{Ws}[\mu + \lambda = k] = \frac{k}{n} e^{-(k^2+\varepsilon_k)/2n}$ mit $-3k \le 2\varepsilon_k \le k$ für $k \le 2\sqrt{n} - 2$.

Somit $\mathbf{Ws}[\mu + \lambda = \lfloor\sqrt{2n}\rceil + i\rceil = (\sqrt{2/n} + \frac{i}{n})\, e^{-1+O(k/n)}$ für $k = \lfloor\sqrt{2n}\rceil + i$.

Hinweise: $(1-\frac{1}{n})^{j+2} \overset{j\le 2\sqrt{n}-2}{\le} 1 - \frac{j}{n} \le (1-\frac{1}{n})^j$, $(1-\frac{1}{n})e^{-1} \le (1-\frac{1}{n})^n \le e^{-1}$, $\mathbf{Ws}[\mu+\lambda = k] = \frac{k}{n}\prod_{j=1}^{k-1}(1-\frac{j}{n}) \le \frac{k}{n}\, e^{-\binom{k}{2}/n}$ (im Gegensatz zu Knuth, exercise 3.1.11, answer, wo der Faktor k fehlt).

Aufgabe 2. Sei $\mathbf{K}$ Körper, $H_2 = \{h_{A,b} \mid A \in \mathbf{K}^{n\times\ell}, b \in \mathbf{K}^n\}$

$h_{A,b} : x \mapsto Ax + b$, $\mathbf{K}^n \to \mathbf{K}^\ell$. Zeige:

$H_2 \subset (\mathbf{K}^n)^{\mathbf{K}^\ell}$ ist universelle Familie von Hashfunktionen.

Hinweis: $\{(A,b) \mid Ax + b = y, Ax' + b = y'\} \subset \mathbf{K}^{n\ell+n}$ ist zu gegebenen $x, x', y, y' \in \mathbf{K}^n$ mit $x \ne x'$ linearer Raum der Dimension $n\ell - n$.

Aufgabe 3. Sei $H_3 = \{h_{A,b} \mid A \in \mathbf{K}^{n\times\ell}$ Töplitz-M., $b \in \mathbf{K}^n\}$. Zeige :

$H_3 \subset (\mathbf{K}^n)^{\mathbf{K}^\ell}$ ist universelle Familie von Hashfunktionen.

Aufgabe 4. Sei $G_{p,c}$ der Funktionsgraph zu $F(x) := x^2 + c \mod p$. Zeige:

1. Für $c = -1, -3$ hat $G_{p,c}$ für alle $p \in \mathbf{Z}$ eine Z.h.-Komponente mit $\lambda = 2$.
2. Für $p = 1, 7 \mod 8$, p prim, hat diese Z.h.-Komponente mindestens 5 (für $c = -3$ sogar 8 Knoten, wenn zusätzlich $p = 1, 9 \mod 20$ gilt.

Hinweis: $2 \in QR_p$ mit p prim gilt gdw $p = 1, 7 \mod 8$. $5 \in QR_p$ gilt gdw $p = 1, 9 \mod 20$ [Ga, Art. 112-121].