Prof. C. P. Schnorr Sommersemester 2004

Kryptographische Algorithmen

Blatt 5 26.05.2004, Abgabe 02.06.2004

Aufgabe 1. Sei $k \geq 2^t$. Zeige:
Das k-Summen Problem kann als 2^t-Summenproblem in erwarteter Schrittzahl $O(k\, 2^{\frac{n}{t+1}})$ gelöst werden.

Aufgabe 2. Sei $q \in \mathbf{N}$, die Liste L_i, $i = 1, \ldots, 4$, bestehe aus $x_j^{(i)} \in_R \mathbf{Z}_q = [q]$, $j = 1, \ldots, \lceil q^{1/3} \rceil$. Definiere geeignete Operationen $\bowtie, \bowtie'$ so dass für $L_1' := L_1 \bowtie L_2$, $L_2' := L_3 \bowtie L_4$, $L := L_2' \bowtie' L_2'$ gilt:

1. Jedes $x \in L$ liefert $x_i \in L_i$ $i = 1, \ldots, 4$ mit $\sum_i x_i = 0 \bmod q$.

2. $|L| = \Omega(1)$, $|L_i'| = \Omega(q^{1/3})$ gilt für die erwartete Listengrösse.

Hinweis: O.b.d.A. sei $q^{1/3} = 2^s$.

Aufgabe 3. Zu $F_n \in_R [n]^{[n]}$ mit Funktionsgraph G_n und $\alpha_i = \#$ Z.h.-Komponenten mit $\lambda = i$. Bestimme $\mathbf{E}[\alpha_i]$ $i = 1, 2, \ldots$ für $n \to \infty$.

Aufgabe 4. Sei $I_n = \{0,1\}^n$ und $H_0, H_1 \in_R I_{n+1}^{I_n}$ stat. unabh. und $F \in I_{n+1}^{I_{n+1}}$ erklrt durch $F(x_0, ..., x_n) := H_{x_0}(x_1, ..., x_n)$. Zeige:

1. $F \in_R I_{n+1}^{I_{n+1}}$
2. $\mathbf{E}[\mu + \lambda] = \Theta(2^{\frac{n+1}{2}})$ gilt für $x_{i+1} = F(x_i)$
3. $\mathbf{Ws}[lsb(x_{\mu-1} \oplus x_{\mu+\lambda-1}) = 1] = \frac{1}{2}$.

Motivation: $lsb(x_{\mu-1} \oplus x_{\mu+\lambda-1}) = 1$ gdw $H_{\nu'}(x_{\mu-1}) = x_\mu = x_{\mu+\lambda} = H_\nu(x_{\mu+\lambda-1})$ für $\nu' \neq \nu$.