Prof. C. P. Schnorr Sommersemester 2011

Kryptographie

Blatt 9, 24.06.2011, Abgabe 01.07.2011

Aufgabe 1 Präzisiere und analysiere folgenden Lösungsalgorithmus für das 2-Summenproblem über $\{0,1\}^n$:
Verteile die $x_1 \in L_1, x_2 \in L_2$ in $2^{n/2}$ Fächer nach den niedrigsten $n/2$ Bits. Suche die Teil-Kollisionen über $\{0,1\}^{n/2}$ nach Kollisionen über $\{0,1\}^n$ ab. Bilde z.B. $L = \{(x_1, x_2, x_1 \oplus x_2) \mid low_{n/2}(x_1) = low_{n/2}(x_2)\}$. Zeige:
Für $|L_1| = |L_2| = 2^{n/2}$ geht das Verfahren in $O(2^{n/2})$ arithm. + Adress-Schritten. Ein $\log n$ Faktor für Sortieren tritt nicht auf.

Aufgabe 2 Löse das 2^t–Summenproblem über $I_n = \{0,1\}^n$ für Listen der Länge $|L_i| \leq 2^{\frac{n}{2t}}$ für $i = 1, \ldots, 2^t$ mit erwarteter Laufzeit $O(2^t 2^{n/t})$.
Hinweis: Ändere die erste Stufe von Wagner's Alg. ab zu

$$L'_i := L_{2i-1} \oplus L_{2i} \qquad \text{für} \quad i = 1, \ldots, 2^{t-1} \quad .$$

Aufgabe 3 Zeige: Wenn das k–Summen Problem über der zyklischen Gruppe $G = \langle g \rangle$ in Zeit T lösbar ist, dann ist das DL–Problem zu $\log_g$ in Zeit O(T) lösbar.

Hinweis: Theorem 2, D. Wagner, Crypto 2002.

Punktzahl pro Aufgabe 5.