Prof. C. P. Schnorr Wintersemester 2008/09

Kryptographie

Blatt 6, 21.11.2008, Abgabe 28.11.2008

Aufgabe 1 Eine Zeile der Erfolgsmatrix zum Extraktor AL von Satz 2 heiße k-schwer, wenn sie mindestens $2^t\,\varepsilon/k$ viele Einsen enthält. Zeige:

1. Der Anteil A_k der Einsen in k-schweren Zeilen ist $\geq 1 - 1/k$.
2. A_1 kann beliebig klein sein.

Aufgabe 2 Zeige: das Protokoll $(\mathcal{P}^k, \mathcal{V}^k)$ der k-fach sequentiellen DL-Identifikation ist „perfect zero-knowledge“, falls 2^t polynomial ist, d.h. $t = O(\log(\log q))$ für Eingaben der Länge $\log_2 q$.

Skizziere einen perfekten Simulator $\mathcal{S} : (\tilde{V}, h) \mapsto (\bar{\mathbf{g}}, \mathbf{c}, \mathbf{y})$ mit
$\mathrm{E}|\mathcal{S}(\tilde{V}, h)| \leq (|\mathcal{P}^k| + |\tilde{V}|)2^t$.

Aufgabe 3 Beschreibe einen probabilistischen Extraktor $\mathrm{AL} : (\tilde{P}, h) \mapsto \log_g h$ zu (P^k, V^k) mit erwarteter Laufzeit $O(|\tilde{P}|/\varepsilon)$, sofern $\widetilde{P}$ mit Ws $\varepsilon > 2^{-tk+1}$ Erfolg hat.