Prof. C. P. Schnorr Sommersemester 2011

# Kryptographie

Blatt 6, 25.05.2011, Abgabe 03.06.2011

**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: die einfache ($t = 1$) Fiat–Shamir Identifikation $(\mathcal{P}, \mathcal{V})_{\mathrm{FS}}$ ist perfekt zeroknowledge. Gib einen prob. pol. Zeit Simulator an.

**Aufgabe 3** Der betrügerische Prover $\widetilde{\mathcal{P}}$ zur einfachen (t=1) Fiat-Shamir Identifikation habe Erfolgsws. $\varepsilon > \frac{1}{2}$. Die Ws bezieht sich auf die Münzwürfe von $\widetilde{\mathcal{P}}, \mathcal{V}$ und $s \in_R \mathbf{Z}_N^*$. Gib einen Algorithmus an, der $N$ mittels $\widetilde{\mathcal{P}}$ in Laufzeit $O(|\widetilde{\mathcal{P}}|/\varepsilon)$ zerlegt.

**Punktzahl pro Aufgabe 5.**