Prof. C. P. Schnorr Wintersemester 2008/09

# Kryptographie

Blatt 9, 12.12.2008, Abgabe 19.12.2008

Es bezeichne $\mathrm{RSA}_m$ die Menge der RSA–Moduln $N = pq$ mit
$p - 1 = 2^m \bmod 2^{m+1},\ q - 1 \neq 0 \mod 2^{m+1}$.

**Aufgabe 1** Zeige für $N \in \mathrm{RSA}_m$:

a) $\mathbf{Z}_N^{*2^m} = \mathbb{Z}_N^{*2^{m+1}}$,

b) $-1 \notin \mathbf{Z}_N^{*2^m}$,

c) $x \mapsto x^2$ permutiert $\mathbf{Z}_N^{*2^m}$.

**Aufgabe 2** Zeige: die einfache ($t = 1$) Fiat–Shamir Identifikation $(\mathcal{P}, \mathcal{V})_{\mathrm{FS}}$ ist perfekt-ZK. Gib einen prob. pol. Zeit Simulator an.

**Aufgabe 3** Der betrügerische Prover $\widetilde{\mathcal{P}}$ zur einfachen (t=1) Fiat-Shamir Identifikation habe Erfolgsws. $\geq \frac{1}{2} + \varepsilon, \varepsilon > 0$. 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 $O(|\widetilde{\mathcal{P}}|\varepsilon^{-1} \log N)$ zerlegt.