Prof. C. P. Schnorr Sommersemester 2007

# Kryptographie

Blatt 10, 22.06.07 Abgabe 29.06.07

**Aufgabe 1** Im Faktorisierungsverfahren FA:$(\widetilde{P}, N, \underline{s}) \to \{p, q\}$ von Satz 3.16 sei $i \leq \ell + 1$ minimal mit $Z^{2^i} = 1 \mod N$. $\widetilde{P}$ ist Angreifer aus dem Stand auf $(P, V)_{OS}$ und $2^k \mid p - 1$. Zeige:
Im Fall $i = 1$ gilt $\mathrm{Ws}_w[Z \neq -1] \geq \frac{1}{2}$.

**Aufgabe 2** Zeige:
$(P, V)_{OS}$ für $2^k \mid p - 1$ ist sicher gegen aktive Angreifer $\mathcal{A}$, d.h.:
Es gibt einen prob. Alg. $\overline{\mathrm{FA}} : (\mathcal{A}, N, \underline{s}) \mapsto \{p, q\}$ mit $\mathrm{E}_w|\mathrm{FA}| = O(k|\mathcal{A}|/\varepsilon)$, sofern $\mathcal{A}$ für zufällige $\underline{v} \in_R (\mathbb{Z}_N^{*2^k})^t$ Erfolgsws $\varepsilon \geq 2^{-tk+1}$ hat.

*Hinweis*: $\overline{FA}$ muss Identifikationen nach Wahl von $\widetilde{P}$ erzeugen durch ZK-Simulation von $(P, \widetilde{V})_{OS}$. Der geheime Schlüssel $\underline{s}$ muss benutzt werden.

**Aufgabe 3** Detailliere das Verfahren $\widetilde{\mathrm{FA}}$ zu Satz 3.18 für $N \in \mathrm{RSA}_m$ im Fall $Z^{2^{i-1}} = -1 \mod N$ und $i \geq 2$.

**Aufgabe 4** Zeige zum Verfahren $\widetilde{\mathrm{FA}}$ von Satz 3.18 für $N \in \mathrm{RSA}_m$:
a) $i \leq m$
b) $\mathrm{E}_w|\widetilde{\mathrm{FA}}| = O(m|\widetilde{P}|/\varepsilon)$, sofern $\widetilde{P}$ für zufällige $\underline{\tilde{v}} \in_R (\mathbb{Z}_N^{*2^m})^t$ Erfolgsws. $\varepsilon \geq 2^{-kt+1}$ hat.