Prof. C. P. Schnorr Sommersemester 2007

Kryptographie

Blatt 8, 08.06.07 Abgabe 15.06.07

Aufgabe 1 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 2 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.

Aufgabe 3 Zeige:

1. für p prim, $p = 3 \bmod 4$, $a \in \mathrm{QR}_p$ gilt: $\mathrm{sqrt}(a) = \pm a^{\frac{p+1}{4}}$.

2. für p prim, $p = 5 \bmod 8$, $a \in \mathrm{QR}_p$ gilt: $\mathrm{sqrt}(a) \in \{\pm a^{\frac{p+3}{8}}, \pm 2a(4a)^{\frac{p-5}{8}}\}$.

Hinweis: $2 \in \mathrm{QNR}_p$ für $p = 5 \mod 8$, sowie Handbook of Applied Cryptography.

Aufgabe 4 **1.** Zeige: Alg. 3.34 berechnet $\mathrm{sqrt}(a) \mod p$.

2. Berechne mit Alg. 3.34 ein b so dass $(\frac{b}{101}) = -1$ und $\mathrm{sqrt}(-1) \mod 101$.