Prof. C. P. Schnorr Wintersemester 2013/14

Kryptographie

Blatt 7, 17.01.2014, Abgabe 24.01.2014

Aufgabe 1 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 2 Der betrügerische Prover $\widetilde{\mathcal{P}}$ zur einfachen (t=1) Fiat-Shamir Identifikation habe Erfolgsws. $\varepsilon > 0$. 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 $O(|\widetilde{\mathcal{P}}|/\varepsilon)$ zerlegt.

Aufgabe 3 Zeige Satz 2 für die $(P, V)_{OS}$ Identifikation im Fall 3
$m_q \leq m_p < t, \mathbf{v} = \tilde{\mathbf{s}}^{2^{m_p}}$ mit $\tilde{\mathbf{s}} \in_R (\mathbb{Z}_N^*)^k$ für $\widetilde{P}$ aus dem Stand mit Erfws $\varepsilon \geq 2^{-tk+1}$. Kann man 2^{m_p} zu $2^{m_p \pm i}$, $i > 0$ vergrössern bzw. verkleinern?

Punktzahl pro Aufgabe 5