Prof. C. P. Schnorr Sommersemester 2017

Kryptographie

Blatt 8, 14.06.2017, Abgabe 21.6.2017

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.

5 Punkte pro Aufgabe