Prof. C. P. Schnorr Sommersemester 2009

Gitter und Kryptographie

Blatt 1, 17.04.2009, Abgabe 24.04.2009

Aufgabe 1. Beweise Lemma 1 zur Micciancio-Vadhan Identifikation.
(Korrektheit)

Aufgabe 2. Beweise Lemma 2 zur Micciancio-Vadhan Identifikation.
(die triviale Betrugsws. von $\mathcal{P}^*$ ist $1/2$)

Aufgabe 3. Beweise Lemma 3 zur Micciancio-Vadhan Identifikation.
(soundness)