Prof. C. P. Schnorr Wintersemester 2005/06

Gitter und Kryptographie

Blatt 1, 28.10.2005, Abgabe 04.11.2005

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)

Aufgabe 4. Zeige zum Gitter $\mathcal{L}(B) \subset \mathbf{R}^3$ mit Basismatrix $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ aN & bN \end{bmatrix}, a, b, N \in \mathbf{Z}$:

1. $\det \mathcal{L} = (1 + N^2(a^2 + b^2))^{1/2}$.
2. Für $N > \frac{4}{3}(a^2 + b^2)^{1/2}$ ist jede *reduzierte* Basis $\mathbf{b}_1, \mathbf{b}_2$ von der Form

$$\mathbf{b}_1 = \begin{pmatrix} * \\ * \\ 0 \end{pmatrix}, \ \mathbf{b}_2 = \begin{pmatrix} * \\ * \\ N \cdot \mathrm{ggT}(a, b) \end{pmatrix}.$$

Hinweis. Benutzen Sie dass:

$\det \mathcal{L}(B) =_{def} \mathrm{vol}\, \mathcal{P}(B) = (\det B^t B)^{1/2}$,

$\mathrm{ggT}(a, b) = \min\{|t_1 a + t_2 b| \mid (t_1, t_2) \in \mathbf{Z}^2 \setminus \mathbf{0}\}$ für $a, b \in \mathbf{Z}$,

für jede *reduzierte* Basis $B = [\mathbf{b}_1, \mathbf{b}_2]$ gilt:

$\|\mathbf{b}_1\| = \lambda_1 = \min\{\|\mathbf{b}\| \neq 0 \mid \mathbf{b} \in \mathcal{L}\}, \quad \lambda_1^2 \leq \sqrt{\frac{4}{3}} \det \mathcal{L}$.