Prof. C. P. Schnorr Sommersemester 2011

Kryptographie

Blatt 10, 01.07.2011, Abgabe 08.07.2011

Aufgabe 1 Beispiel zum Paillier Schema

Setze $N = 143 = 11 \cdot 13$.

Berechne ein $\alpha \in \mathbb{Z}_{N^2}^*$ mit $\mathrm{ord}(\alpha) = \lambda(N^2)$. Kodiere $m = 2$ zu

$\mathrm{cip} = E_\alpha(2, r)$ und dekodiere cip.

Seien $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^m$ linear unabhängig und $\mathcal{L} = \mathbf{b}_1\mathbb{Z} + \mathbf{b}_2\mathbb{Z}$ das Gitter mit Basis $\mathbf{b}_1, \mathbf{b}_2$. Die Menge aller Basen von $\mathcal{L}$ ist $[\mathbf{b}_1, \mathbf{b}_2]\mathrm{GL}_2(\mathbb{Z})$.

Aufgabe 2 Zeige: Es gibt eine „reduzierte" Basis $\mathbf{b}_1, \mathbf{b}_2$ von $\mathcal{L}$, so dass

$$\|\mathbf{b}_1\| = \lambda_1, \ |\langle \mathbf{b}_1, \mathbf{b}_2 \rangle| \leq \tfrac{1}{2} \|\mathbf{b}_1\|^2.$$

Aufgabe 3 Zeige: Für jede reduzierte Basis $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^2$ von $\mathcal{L} \subset \mathbb{R}^2$ mit Grundmasche $= \{r_1\mathbf{b}_1 + r_2\mathbf{b}_2 \mid 0 \leq r_1, r_2 \leq 1\} \subset \mathbb{R}^2$ gilt

1. $\det \mathcal{L} \leq \lambda_1 \cdot \lambda_2$.

2. $\lambda_1^2 \leq \sqrt{\frac{4}{3}} \det \mathcal{L}$

Hinweis: $\det \mathcal{L} = |\det[\mathbf{b}_1, \mathbf{b}_2]| = \mathrm{vol}$ (Grundmasche).

Punktzahl pro Aufgabe 5.