TD 3 Advanced cryptography 2024

Léo Colisson Palais

Exercice 1: Basics on lattices

1. Is the 1D lattice generated by $\begin{pmatrix}1\end{pmatrix}$ and $\begin{pmatrix}\sqrt{2}\end{pmatrix}$ a valid lattice?
   Hint: consider the sequence $(\sqrt{2}-1)^l$
2. Let $\mathbf{B}$ be a basis of the lattice $\mathcal{L}$ and $\mathbf{U} \in \mathbb{Z}^{k\times k}$ be an invertible matrix s.t. $\mathbf{U}^{-1} \in \mathbb{Z}^{k\times k}$. Show that $\mathbf{B}\cdot\mathbf{U}$ is also a basis of $\mathcal{L}(\mathbf{B})$.
3. Show an efficient algorithm to check if a vector v belongs to a full-rank lattice given a basis B. Hint: consider B^{-1}.
4. Building on the previous question, propose an efficient algorithm to decide if two lattices $\mathcal{L}(B_0)$ and $\mathcal{L}(B_1)$ are equal.

Exercice 2: LLL

1. Let $r \coloneqq 1.9100446$ be a root of an unknown polynomial of the form ax^3+bx^2+cx+d, where a, b, c and d are small integers. The goal is to determine a, b, c and d.
   (a) Can you propose a first algorithm based on the attack against the Merkle-Hellman cryptosystem?
   (b) Are all solutions to your above algorithm necessary polynomials such that r is a root of this polynomial? If not, can you propose a fix to arbitrarily increase the chance of finding a solution where r is actually a root of your polynomial.
   (c) Implement your algorithm in sagemath (you may want to use matrices over `QQ`).
2. Run the LLL algorithm manually for $\delta = \frac{3}{4}$ on the basis vectors $\begin{pmatrix}201\\37\end{pmatrix}$ and $\begin{pmatrix}1648\\297\end{pmatrix}$.