Exercise Set 2

Prof. Kenny Paterson
Kien Tuong Truong

Problem 1. Consider $n = 2$ and $\underline{b}_1 = (5, 1), \underline{b}_2 = (29, 6)$. Describe the lattice $\mathcal{L}$ generated by $\{\underline{b}_1, \underline{b}_2\}$. (Hint: think about $\det(\mathcal{L})$.)

Problem 2. (Solving this problem will be useful in the lab, since the `fpylll` package has limitations on the format of input basis matrices.)

Consider B, an $n \times n$ basis matrix for some full-rank lattice $\mathcal{L}_B$. Suppose C is formed by multiplying every entry in B by some non-zero constant $c \in \mathbb{R}$. Let $\mathcal{L}_C$ denote the lattice corresponding to C. We speak of $\mathcal{L}_C$ as being a *scaled version* of $\mathcal{L}_B$.

- How do the lattice vectors in $\mathcal{L}_C$ relate to those in $\mathcal{L}_B$?
- How does $\det(\mathcal{L}_C)$ relate to $\det(\mathcal{L}_B)$?
- Suppose B contains entries that are all rational numbers, say $b_{ij} = a_{ij}/q_{ij}$ where $a_{ij}, q_{ij} \in \mathbb{Z}$ for $1 \leq i, j \leq n$. Explain how to compute a constant c so that C obtained by scaling B contains only *integer* entries.
- What can you say about the hardness of solving CVP/SVP problems in $\mathcal{L}_B$, given efficient CVP/SVP solvers for C with integer entries?
- What constant c would you use to scale the matrix B arising in the CVP formulation of the HNP to have only integer entries? Recall:

$$B = \begin{bmatrix} q & 0 & 0 & \cdots & 0 & 0 \\ 0 & q & 0 & \cdots & 0 & 0 \\ 0 & 0 & q & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & q & 0 \\ t_1 & t_2 & t_3 & \cdots & t_n & 1/2^{L+1} \end{bmatrix}$$

  Write down the final matrix C.

Problem 3. Recall the Gaussian heuristic from the lecture: this states that, for a "random" lattice $\mathcal{L}$ in n dimensions, we have:

$$\lambda_1 \approx \sqrt{\frac{n}{2\pi e}} \cdot \det(\mathcal{L})^{1/n}.$$

Consider the matrix B' of the form arising in Kannan's embedding:

$$\begin{bmatrix} B & 0 \\ \underline{w} & M \end{bmatrix}$$

where B is the $(n+1) \times (n+1)$ array arising in the CVP formulation of the HNP, namely:

$$\begin{bmatrix} q & 0 & 0 & \cdots & 0 & 0 \\ 0 & q & 0 & \cdots & 0 & 0 \\ 0 & 0 & q & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & q & 0 \\ t_1 & t_2 & t_3 & \cdots & t_n & 1/2^{L+1} \end{bmatrix}$$

Compute the determinants of B and B' (in the latter case, the result is a function of M), and from this, the expected value of λ_1 for the corresponding lattices (under the Gaussian heuristic).

Problem 4. (Solving this problem will again be useful in the lab, especially for implementing the last steps in the solution using the Kannan embedding technique and SVP.)

Recall that, in the Kannan embedding approach to solving CVP, a shortest vector in the lattice $\mathcal{L}'$ is expected to be of the form $(\underline{f}, M)$ where $\underline{f} = \underline{w} - \underline{v}$. Here $\underline{w}$ is the target input vector for CVP, and $\underline{v}$ is the solution.. Recall also that in our specific application to breaking ECDSA, $\underline{w}$ is of the form $(u_1, u_2, \ldots, u_n, 0)$ while $\underline{v}$ is likely to be of the form $(-\ell_1, -\ell_2, \ldots, -\ell_n, x) \cdot B = (u_1 + e_1, u_2 + e_2, \ldots, u_n + e_n, x/2^{L+1})$ (since we showed that this $\underline{v}$ is close to $\underline{w}$).

- Given this information, show that $\underline{f} = (-e_1, -e_2, \ldots, -e_n, -x/2^{L+1})$.
- Given what you know (from class) about the size of the e_i, compute an upper bound on the norm of $(\underline{f}, M) \in \mathcal{L}'$.
- Compare the result in the previous part to what you obtained in the previous problem using the Gaussian heuristic. What does this suggest about how to set M in order to ensure the success of the Kannan embedding approach to solving CVP in this case?
- By considering $(-t_1, -t_2, -t_3, \ldots, -t_n, q, 0) \cdot B'$, show that $\mathcal{L}'$ also contains the vector $\underline{z} = (0, 0, \ldots, 0, q/2^{L+1}, 0)$. Compute the norm of $\underline{z}$ and compare to the bound you obtained on the norm of $(\underline{f}, M)$ earlier, showing that it is typically about $\sqrt{n+1}$ times smaller (irrespective of the choice of M).

This problem shows that $\mathcal{L}'$ contains unusually short vectors, so solving SVP will not directly yield a solution to the original CVP for the particular lattices we have constructed here. On the other hand, perhaps the required solution will appear elsewhere in the basis obtained from performing lattice reduction on $B' \ldots$