CS641: Endsem Examination

May 1, 2022

Submission Deadline: May 4, 2022; 11:55 hrs **Maximum Marks**: 50

Consider the following public-key encryption algorithm based on integer lattices.

Key Generation. Let $L \in \mathbb{Z}^{n \times n}$, be the matrix defined as:

$$L = n \cdot I = \begin{bmatrix} n & 0 & 0 & \cdots & 0 \\ 0 & n & 0 & \cdots & 0 \\ 0 & 0 & n & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & n \end{bmatrix}.$$

Let $U \in \mathbb{Z}^{n \times n}$ be a *unitary* matrix, that is, $\det U = 1$. Let $R \in \mathbb{Q}^{n \times n}$ be a *rigid rotation* matrix, that is, $R \cdot R^T = I$. Define $\hat{L} = U \cdot L \cdot R$. Public key is the matrix $\hat{L}$ and private key is the matrix R.

Encryption. Given an n-bit long message m, view it as a vector in $\mathbb{Z}^n$ with binary entries. Pick a random vector $v \in \mathbb{Z}^n$ and compute the vector $c = v \cdot \hat{L} + m$. Output c.

Decryption. Given a vector $c \in \mathbb{Q}^n$, compute vector $d = c \cdot R^T$. Reduce every entry of d modulo n so that the entry becomes $< n/2$ in absolute value. Let the resulting vector be $\hat{d}$. Compute $m = \hat{d} \cdot R$.

Prove that:

- Lattice generated by $\hat{L}$ has a basis consisting of n orthogonal vectors, each of length n. **(10 marks)**
- Decryption works correctly. **(15 marks)**

Analyze the security of the cryptosystem. In particular, show that if any orthogonal basic of $\hat{L}$ can be found, then the security is broken **(15 marks)**. Are there other ways to break the security? **(10 marks)**