Lattices II – SIS and LWE lattice problems

Marcel Šebek

In the following, $n \in \mathbb{N}$ will be the main security parameter and all the remaining parameters will be implicitly functions of n. Let $q \geq 2$ be an integer (not necessarily a prime).

Lemma 1. *Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ be a matrix. Let us interpret is as a group homomorphism $\mathbf{A}\colon \mathbb{Z}^m \to \mathbb{Z}^n$ and similarly $\mathbf{A}^T\colon \mathbb{Z}^n \to \mathbb{Z}^m$. Let $\pi_q\colon \mathbb{Z}^n \to \mathbb{Z}_q^n$ be the natural projection. Then the following sets are full-rank lattices:*

$$\mathcal{L}(\mathbf{A}^T) = \operatorname{Im} \mathbf{A}^T + q\mathbb{Z}^m = \{\mathbf{z} \in \mathbb{Z}^m \mid \exists \mathbf{x} \in \mathbb{Z}^n : \mathbf{z} = \mathbf{A}^T\mathbf{x} \pmod q\} \leq \mathbb{Z}^m$$
$$\mathcal{L}^\perp(\mathbf{A}) = \operatorname{Ker} \pi_q\mathbf{A} = \{\mathbf{z} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{z} = 0 \pmod q\} \leq \mathbb{Z}^m$$

1 SIS – Small Integer Solution

Definition 2 (SIS—matrix version)**.** Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ be given, the SIS problem is to find $\mathbf{z} \in \{-1, 0, 1\}^m$ such that $\mathbf{A}\mathbf{z} = 0 \pmod q$. In other words, $\mathbf{z} \in \mathcal{L}^\perp(\mathbf{A})$ is a short vector.

Proposition 3. *Let $m > n \log q$ and $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ be public description ($\mathbf{A}$ sampled uniformly). Let $\{0,1\}^m \to \mathbb{Z}_q^n$ be defined as $f_\mathbf{A}(\mathbf{z}) = \mathbf{A}\mathbf{z} \bmod q$. Then $f_\mathbf{A}$ is a collision resistant compression function unless SIS problem is easy to solve in the average case. In particular, it is a one-way function.*

Theorem 4 (Worst/Average case reduction)**.** *Assume that SIS is solvable in the average case with a non-negligible success probability. Then there exists an algorithm that finds a short vector in an arbitrary lattice.*

2 LWE – Learning With Errors

Definition 5 (LWE—matrix version)**.** Let χ be a Gaussian distribution over $\mathbb{Z}_q$ and $\mathbf{s} \in \mathbb{Z}_q^n$. Let

$$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m} \qquad \mathbf{e} \leftarrow \chi^m \qquad \mathbf{b} = \mathbf{A}^T\mathbf{s} + \mathbf{e} \pmod q$$

The Search-LWE problem is to find $\mathbf{s}$ given $(\mathbf{A}, \mathbf{b})$. The Decision-LWE problem is to distinguish $(\mathbf{A}, \mathbf{b})$ sampled as above from uniform distribution on $\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$.

Proposition 6. *LWE is easier than SIS.*

Lemma 7 (Secret shifting)**.** *Let $(\mathbf{a}_i, b_i)$ be sampled using $\mathbf{s} \in \mathbb{Z}_q^n$. Then $(\mathbf{a}_i, b_i + \langle \mathbf{a}_i, \mathbf{t} \rangle)$ is sampled using $\mathbf{s} + \mathbf{t}$.*

Proposition 8. *Search-LWE and Decision-LWE problems are equivalent.*