CSE 206A: Lattice Algorithms and Applications Winter 2016

Variants of SIS and LWE

Instructor: *Daniele Micciancio* UCSD CSE

1 q-ary lattices

Modern lattice cryptography is based on the following family of lattices.

Definition 1 *For any positive integers $k \leq n$ and q, and matrix $\mathbf{A} \in \mathbb{Z}_q^{k \times n}$ define the following n-dimensional lattices*

$$\begin{aligned} \Lambda^\perp(\mathbf{A}) &= \{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{A}\mathbf{x} \bmod q = \mathbf{0}\} \\ \Lambda(\mathbf{A}) &= \{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{x} \bmod q = \mathbf{A}^t\mathbf{s} \text{ for some } \mathbf{s} \in \mathbb{Z}_q^k\}. \end{aligned}$$

For any matrix $\mathbf{A}$, these lattices are dual up to scaling: $\Lambda(\mathbf{A}) = q \cdot \widehat{\Lambda^\perp(\mathbf{A})}$ and $\Lambda^\perp(\mathbf{A}) = q \cdot \widehat{\Lambda(\mathbf{A})}$. In particular, $\det(\Lambda(\mathbf{A})) \cdot \det(\Lambda^\perp(\mathbf{A})) = q^n$.

Lemma 2 *For any q and $\mathbf{A} \in \mathbb{Z}_q^{k \times n}$, the following conditions are equivalent:*

1. $\det(\Lambda_q^\perp(\mathbf{A})) = q^k$
2. $\det(\Lambda_q(\mathbf{A})) = q^{n-k}$
3. $\mathbf{A}\mathbb{Z}_q^n = \mathbb{Z}_q^k$

Moreover, if $\mathbf{A} \in \mathbb{Z}_q^{k \times n}$ is chosen uniformly at random, then it satisfies any of the above conditions with probability at least $1 - 1/q^{n-k}$.

Proof. ... □

2 SIS and LWE

The SIS and LWE problems can be defined as follows:

Definition 3 *For any positive integers $k \leq n$ and q, the* Short Integer Solution *problem $\mathrm{SIS}_q(k, n, \beta)$, given a (random) matrix $\mathbf{A} \in \mathbb{Z}_q^{k \times n}$ asks to find a nonzero vector $\mathbf{x} \in \Lambda^\perp(\mathbf{A})$ of length $\|\mathbf{x}\| \leq \beta$.*

Definition 4 *For any positive integers $k \leq n$ and q, and probability distribution $\mathcal{X}$ over $\mathbb{Z}^n$, the* Learning With Errors *problem* $\mathrm{LWE}(k, n, \mathcal{X})$*, given a random matrix $\mathbf{A} \in \mathbb{Z}_q^{k \times n}$, asks to distinguish the distribution $\{\mathbf{v} + \mathbf{x} \mid \mathbf{v} \leftarrow (\Lambda(\mathbf{A}) \bmod q), \mathbf{x} \leftarrow \mathcal{X}\}$ from the uniform distribution over $\mathbb{Z}_q^n$.*

In the standard SIS and LWE problems, the matrix $\mathbf{A}$ is chosen uniformly at random from $\mathbb{Z}_q^{k \times n}$. Another common distribution, often useful as an optimization in cryptographic applications, is setting $\mathbf{A} = [\mathbf{I}, \bar{\mathbf{A}}]$ for a uniformly random $\bar{\mathbf{A}} \in \mathbb{Z}_q^{k \times (n-k)}$. Notice that matrices of the form $\mathbf{A} = [\mathbf{I}, \bar{\mathbf{A}}]$ have the property that $\mathbf{A}\mathbb{Z}_q^n = \mathbb{Z}_q^k$, i.e., their columns generate the whole $\mathbb{Z}_q^k$ as an abelian group. Below, we consider a wider class of restrictions on $\mathbf{A}$ that includes both $\mathbf{A} = [\mathbf{I}, \bar{\mathbf{A}}]$ and $\mathbf{A}\mathbb{Z}_q^n = \mathbb{Z}_q^k$ as special cases.

Definition 5 *For any $d \leq k \leq l \leq n$, let $\mathbb{Z}_q^{k,n}[d, l]$ be set of all matrices $\mathbf{A} \in \mathbb{Z}_q^{k \times n}$ for the form*

$$\mathbf{A} = \left[\begin{array}{cc|c} \mathbf{I}_d & \mathbf{A}_0 & \\ \mathbf{O} & \mathbf{A}_1 & \mathbf{A}_2 \end{array}\right]$$

with $\mathbf{A}_0 \in \mathbb{Z}_q^{d \times (l-d)}$, $\mathbf{A}_1 \in \mathbb{Z}_q^{(k-d) \times (l-d)}$ and $\mathbf{A}_2 \in \mathbb{Z}_q^{k \times (n-l)}$, such that $\mathbf{A}_1 \mathbb{Z}_q^{l-d} = \mathbb{Z}_q^{k-d}$. Let also $\mathbb{Z}_q^{k,n}[d, \infty]$ be the set of matrices of this form, but without the requirement that $\mathbf{A}_1 \mathbb{Z}_q^{l-d} = \mathbb{Z}_q^{k-d}$.

As special cases, we get the set $\mathbb{Z}_q^{k,n}[0, \infty] = \mathbb{Z}_q^{k \times n}$ of all matrices, the set $\mathbb{Z}_q^{k,n}[k, k]$ of all matrices of the form $[\mathbf{I}, \bar{\mathbf{A}}]$, and the set $\mathbb{Z}_q^{k,n}[0, n]$ of all matrices such that $\mathbf{A}\mathbb{Z}_q^n = \mathbb{Z}_q^k$. Also, it immediately follows from the definition that for any $[d, l] \subseteq [d', l']$ the corresponding sets of matrices satisfy $\mathbb{Z}_q^{k,n}[d, l] \subseteq \mathbb{Z}_q^{k,n}[d', l']$.

We write $\mathrm{SIS}_q^{[d,l]}(k, n, \beta)$ and $\mathrm{LWE}_q^{[d,l]}(k, n, \mathcal{X})$ for the $\mathrm{SIS}_q(k, n, \beta)$ and $\mathrm{LWE}_q(k, n, \mathcal{X})$ problems where $\mathbf{A}$ is chosen uniformly at random from $\mathbb{Z}_q^{k,n}[d, l]$. In order to relate these problems, we introduce a dual formulation for the SIS and LWE problems.

Definition 6 *For any positive integers $k \leq n$ and q, the* Dual SIS *problem $\widehat{\mathrm{SIS}}_q(k, n, \beta)$, given a (random) matrix $\mathbf{A} \in \mathbb{Z}_q^{k \times n}$ asks to find a nonzero vector $\mathbf{x} \in \Lambda(\mathbf{A})$ of length $\|\mathbf{x}\| \leq \beta$.*

Definition 7 *For any positive integers $k \leq n$ and q, and probability distribution $\mathcal{X}$ over $\mathbb{Z}^n$, the* Dual LWE *problem $\widehat{\mathrm{LWE}}(k, n, \mathcal{X})$, given a random matrix $\mathbf{A} \in \mathbb{Z}_q^{k \times n}$, asks to distinguish the distribution $\{\mathbf{A}\mathbf{x} \pmod q \mid \mathbf{x} \leftarrow \mathcal{X}\}$ from the uniform distribution over $\mathbb{Z}_q^k$.*

We write $\widehat{\mathrm{SIS}}_q^{[d,l]}(k, n, \beta)$ and $\widehat{\mathrm{LWE}}_q^{[d,l]}(k, n, \mathcal{X})$ for the dual $\widehat{\mathrm{SIS}}_q(k, n, \beta)$ and $\widehat{\mathrm{LWE}}_q(k, n, \mathcal{X})$ problems where $\mathbf{A}$ is chosen uniformly at random from $\mathbb{Z}_q^{k,n}[d, l]$.

Theorem 8 *For any $d \leq k \leq l \leq n$, the problems $\mathrm{SIS}^{[d,l]}(k, n, \beta)$ and $\widehat{\mathrm{SIS}}^{[n-l,n-d]}(n-k, n, \beta)$ are computationally equivalent.*

Theorem 9 *For any $d \leq k \leq l \leq n$, the problems $\mathrm{LWE}^{[d,l]}(k, n, \beta)$ and $\widehat{\mathrm{LWE}}^{[n-l,n-d]}(n - k, \beta)$ are computationally equivalent.*

Theorem 10 *If $(l - d) \log q \geq \omega(\log n)$, then the uniform distributions over $\mathbb{Z}_q^{k,n}[l, d]$ and $\mathbb{Z}_q^{k,n}[l, \infty]$ are statistically close.*