FHE-MPC Notes

Lecturer: Nigel Smart
Scribe: Enrique Larraia

Lecture #2

---

q-ary lattices

These are lattices of particular interest in lattice-based cryptography. Let a lattice $\mathcal{L}$ embedded in $\mathbb{Z}^n$, we say $\mathcal{L}$ is a q-ary lattice for some integer q, if $q\mathbb{Z} \subseteq \mathcal{L}$. Since any lattice is closed under addition, the vector $x \in \mathbb{Z}^n$ is in the q-ary lattice $\mathcal{L}$ if and only if $x \bmod q$ is also in the lattice.

Let integers n, m, there exist a one-to one correspondence between linear codes in $\mathbb{Z}_q^n$ and q-ary lattices. Let a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, consider two m-dimensional q-ary lattices,

$$\begin{aligned} \Lambda_q(\boldsymbol{A}) &= \{\boldsymbol{y} \in \mathbb{Z}^m : \boldsymbol{y} = \boldsymbol{A}^T\boldsymbol{s} \bmod q \text{ for some } s \in \mathbb{Z}^n\} \\ \Lambda_q^{\perp}(\boldsymbol{A}) &= \{\boldsymbol{y} \in \mathbb{Z}^m : \boldsymbol{A}\boldsymbol{y} = \boldsymbol{0} \bmod q\}. \end{aligned}$$

The first lattice is the linear code generated by the rows of $\boldsymbol{A}$ ($\bmod q$), the second lattice corresponds to the linear code with parity check matrix equal to $\boldsymbol{A}$ ($\bmod q$).

Given an arbitrary lattice $\mathcal{L}$, the *dual* lattice $\mathcal{L}^*$ is defined to be the lattice whose vectors $\boldsymbol{x}$ are such that $\langle \boldsymbol{x}, \boldsymbol{y}\rangle \in \mathbb{Z}$ for all $\boldsymbol{y} \in \mathcal{L}$. It is not difficult to see that the above two lattices are dual in some sense, $\Lambda_q^{\perp}(\boldsymbol{A}) = q \cdot \Lambda_q(\boldsymbol{A})^*$ and $\Lambda_q(\boldsymbol{A}) = q \cdot \Lambda_q^{\perp}(\boldsymbol{A})^*$.

Short vectors in q-ary lattices

Consider the following problem: we are given a random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, and we want to find a vector $\boldsymbol{y}$ with minimal length over $\Lambda_q^{\perp}(\boldsymbol{A})$. An heuristic estimate of the length of short vectors in $\Lambda_q^{\perp}(\boldsymbol{A})$ which *seems* to apply very good is given by Micciancio and Regev in their paper *Lattice-based Cryptography*. They approach the smallest vector length, $\lambda_1(\Lambda_q^{\perp}(\boldsymbol{A}))$, as the radius of a ball whose volume is $\mathrm{vol}(\mathcal{L})$. Assume q is prime, if m is big enough with respect to n, the rows of $\boldsymbol{A}$ are linearly independent over $\mathbb{Z}_q$ with high probability. In such case, there are exactly q^{n-m} vectors of $\mathbb{Z}_q^m$ belonging to $\Lambda_q^T(\boldsymbol{A})$, since the kernel of the linear function $A : \mathbb{Z}_q^m \mapsto \mathbb{Z}_q^n : \boldsymbol{y} \mapsto \boldsymbol{A}\boldsymbol{y}$ has dimension $m - n$. From this it follows that $\mathrm{vol}(\mathcal{L}) = \det \Lambda_q^{\perp}(\boldsymbol{A}) = q^n$. Using the formula for the volume of a ball in m dimensions they conclude,

$$\lambda_1(\Lambda_q^{\perp}(\boldsymbol{A})) \approx q^{n/m} \cdot ((m/2)!)^{1/m}/\sqrt{\pi} \approx q^{n/m} \cdot \sqrt{\frac{m}{2\pi e}}.$$

On the other hand, Gama and Nguyen experimented with a large range of lattices distributions and observed, via BKZ algorithm, that the shortest length vector for m-dimensional lattices $\mathcal{L}$ seemed to be $(\det \mathcal{L})^{(1/m)}\delta^m$, where the parameter δ depends on the algorithm used. This (allegedly) estimate also works for q-ary lattices, but now we need to take $\min\{q, q^{(n/m)}\delta^m\}$ (recall $q\mathbb{Z} \subseteq \Lambda_q^{\perp}(\boldsymbol{A})$, therefore we can always produce a vector of length q).

Let us think now about the role m plays in the problem. We can reformulate the problem as a set of n equations on m variables ($\bmod q$). In this setting we want to find a

"short" solution $\boldsymbol{y}$. The first observation is that increasing the value of m does not make the problem any harder. We can always set some of the coordinates of $\boldsymbol{y}$ to be 0 (alternatively, deleting columns from $\boldsymbol{A}$), and hence reducing the size of the original m. But also for the same reason, we can add columns to $\boldsymbol{A}$ (adding zero coordinates to $\boldsymbol{y}$), increasing in this way the dimension m of the lattice. As we can see in the above given estimates, m has something to say in the length of the smallest vector. So the question is, what is the best choice for the size of m?. Micciancio and Regev, by finding the minimun of $q^{n/m}\delta^m$ as a function of m, set the optimal value to be $m = \sqrt{n \log q / \log \delta}$ (the value of m for the minimum of the above function, which turns out to be $2^{2\sqrt{n \log q \log \delta}}$). Therefore with the current state of the art on lattice reduction algorithms, the shortest vector one can find is at least of length $\min\{q, 2^{2\sqrt{n \log q \log \delta}}\}$, where δ is no less than 1.01.

The NTRU cryptosystem

We present the lattice NTRU version given by Micciancio and Regev. Originally it was described using rings by Hoffstein, Pipher and Silverman (*NTRU: a ring based public key cryptosystem, Proceedings of ANTS-III, vol 1423 of LNCS*).The lattices used by NTRU are *convolutional modular* lattices, living in even dimension $2n$. They are q-ary lattices, (so the memebership of a vector $\boldsymbol{v}$ only depends on $\boldsymbol{v}$ mod q), and they are closed under the linear transformation that maps the vector ($\boldsymbol{x}$,$\boldsymbol{y}$) (where $\boldsymbol{x}$ and $\boldsymbol{y}$ are n-dimensional vectors) to the vector ($\boldsymbol{x'}$, $\boldsymbol{y'}$) obtained by cyclically rotating the coordinates of $\boldsymbol{x}$ and $\boldsymbol{y}$. Consider the matrix

$$\boldsymbol{T} = \left[\begin{array}{ccc} & \mathbf{0}^T & 1 \\ \hline \ddots & & \\ & \boldsymbol{I} & \mathbf{0} \\ & & \ddots \end{array}\right].$$

This matrix when applied to a vector $\boldsymbol{v} \in \mathbb{Z}^n$ rotates its coordinates cyclically. Define the matrix

$$\boldsymbol{T}^*\boldsymbol{v} = [\boldsymbol{v}, \boldsymbol{T}\boldsymbol{v}, \ldots, \boldsymbol{T}^{n-1}\boldsymbol{v}],$$

which is the matrix obtained by succesively rotate the coordinates of $\boldsymbol{v}$. Given $\boldsymbol{v} = (\boldsymbol{x}, \boldsymbol{y})$, it can be proved that the smallest convolutional modular lattice containing $\boldsymbol{x}$ and $\boldsymbol{y}$ is $\Lambda_q((\boldsymbol{T}^*\boldsymbol{x}, \boldsymbol{T}^*\boldsymbol{g})^T)$.

The NTRU system parameters are a prime dimension n, an integer modulus q, a small integer p and an integer weight bound b_f. The details are as follows:

Private key The private key is set to be a short vector $(\boldsymbol{f}, \boldsymbol{g})$ subject to the restrictions:

1. the matrix $[\boldsymbol{T}^*\boldsymbol{f}]$ should be invertible modulo q.
2. $f \in \boldsymbol{e}_1 + p\boldsymbol{u}$ and $g \in p\boldsymbol{v}$, where $\boldsymbol{u}, \boldsymbol{v} \in \{-1, 0, 1\}$, and $\boldsymbol{f}, \boldsymbol{g}$ are randomly chosen polynomials (we have given their coefficients) such that $\boldsymbol{f} - \boldsymbol{e}_1$ and $\boldsymbol{g}$ have exactly $d_f + 1$ positive entries, and d_f negative ones.

Public key The public is the *Hermite Normal Form* (HNF) of the convolutional modular lattice $\Lambda_q((\boldsymbol{T}^*\boldsymbol{x}, \boldsymbol{T}^*\boldsymbol{g})^T)$. Due to the structure of convolutional modular lattices, we have a nice form of HNF, namely

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{I} & \boldsymbol{O} \\ \boldsymbol{T}^*\boldsymbol{h} & q \cdot \boldsymbol{I} \end{bmatrix} \qquad \text{where } \boldsymbol{h} = [\boldsymbol{T}^*\boldsymbol{f}]^{-1}\boldsymbol{g} \bmod q.$$

Note that it can be stored only as the vector $\boldsymbol{h}$ since q is a system parameter.

Encryption The message space are the vectors $\boldsymbol{m} \in \{-1, 0, 1\}^n$ with exaclty d_f+1 positive entries and d_f negative ones. Then a random vector $\boldsymbol{r}$ is chosen from the message space, with the same structure as $\boldsymbol{m}$. The ciphertext is $\boldsymbol{c} = (-\boldsymbol{r}, \boldsymbol{m}) \bmod \boldsymbol{H}$. It can be shown that

$$\boldsymbol{c} = (\boldsymbol{0}, (\boldsymbol{m} + [\boldsymbol{T}^*\boldsymbol{h}]\boldsymbol{r}) \bmod q). \tag{1}$$

Decryption We divide the decryption process in two stages: First we multiply the ciphertext $\boldsymbol{c}$ by the matrix $[\boldsymbol{T}^*\boldsymbol{f}]$ modulo q, obtaining:

$$[\boldsymbol{T}^*\boldsymbol{f}]\boldsymbol{c} \bmod q = [\boldsymbol{T}^*\boldsymbol{f}][\boldsymbol{m} + [\boldsymbol{T}^*\boldsymbol{f}][\boldsymbol{T}^*\boldsymbol{h}]\boldsymbol{r} \bmod q = [\boldsymbol{T}^*\boldsymbol{f}]\boldsymbol{m} + [\boldsymbol{T}^*\boldsymbol{g}]\boldsymbol{r} \bmod q,$$

which follows from equation (1), and the identity $[\boldsymbol{T}^*\boldsymbol{f}][\boldsymbol{T}^*\boldsymbol{h}] = [\boldsymbol{T}^*([\boldsymbol{T}^*\boldsymbol{f}]\boldsymbol{h})]$. Then, having in mind that $[\boldsymbol{T}^*\boldsymbol{f}] = \boldsymbol{I}(\text{mod}p)$ and $[\boldsymbol{T}^*\boldsymbol{g}] = (\text{mod}p)$ (using the restrictions given in the Private Key), we only need to reduce modulo p to obtain:

$$[\boldsymbol{T}^*\boldsymbol{f}]\boldsymbol{m} + [\boldsymbol{T}^*\boldsymbol{g}]\boldsymbol{r} \bmod p = \boldsymbol{I} \cdot \boldsymbol{m} + \boldsymbol{O} \cdot \boldsymbol{r} = m.$$

The NTRU cryptosystem is homomorphic for both addition and multiplication operations. The additive homomorphic property is clear, whereas the multiplication of two ciphertexts yields to quadratic terms in the resulting product $\boldsymbol{c}' = \boldsymbol{c}_1\boldsymbol{c}_2$. We obtain an "almost" legal ciphertext. This problem can be solved by slightly modify the ciphertext structure. This is similar to the situation in the scheme by Brakerski and Vaikuntanathan in the paper *Fully Fomomorphic Encryption from Ring-LWE and Security for Key Dependent Messages*.