Women in Mathematics

Advanced Course Review Session 3 : Homomorphic Encryption

24 mai 2018

Let $R = \mathbb{Z}[X]/\langle X^n + 1\rangle$ and $R_q = R/qR = \mathbb{Z}_q[X]/\langle X^n + 1\rangle$ and let χ be an error distribution over R_q. The parameters n, q and χ are public. An additional parameter of the scheme is an integer $D \in N$ that is related to the maximal degree of homomorphism allowed. Given two elements $r_1, r_2 \in R_q^D$ we define

$$\langle r_1, r_2 \rangle = \sum_{i=0}^{n-1} r_{1i} r_{2i}$$

. We define the norm of $r(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \in R_q$ as $||r|| = max|a_i|$.

The RLWE somewhat homomorphic symmetric encryption scheme with message space $R_t = \mathbb{Z}_t[X]/\langle X^n + 1\rangle$ works as follows :

1. Generate the secret key $s \in R_q$ (chosen uniformly at random) and let

$$\mathbf{s} = (1, s, s^2, \ldots, s^D) \in R_q^{D+1}.$$

2. To encrypt a message m, sample $(a, b = as + te) \in R_q^2$, where $a \leftarrow R_q$ and $e \leftarrow \chi$. Compute

$$c_0 = b + m \in R_q \qquad \text{and} \qquad c_1 = -a,$$

   and output the ciphertext $c = (c_0, c_1) \in R_q^2$. We say that $c \in RLWE(m, \beta)$, where β is the error bound.

3. The decryption algorithm, on input the secret key $\mathbf{s}$, outputs $m = \langle \mathbf{c}, \mathbf{s} \rangle \pmod{t}$.

Questions

1. Show that the ciphertexts are correctly decrypted, provided that $\beta \leq \frac{q}{2t}$.
2. Given $\mathbf{c}_1 \in RLWE(m_1, \beta)$ and $\mathbf{c}_2 \in RLWE(m_2, \beta)$, show that $c_1 + c_2$ is an encryption of $(m_0 + m_1) \pmod{t}$ and compute its error bound.

In order to be able to multiply ciphertexts, we will consider a general form for our ciphertexts :

$$\mathbf{c} = (c_0, \ldots, c_d) \in R_q^{d+1}.$$

with $d \leq D$.

We then decrypt by computing $m = \langle \mathbf{c}, \mathbf{s} \rangle \pmod t$, where $\mathbf{c} = (c_0, \ldots, c_D)$ is obtained from c by padding with 0. Given two ciphertexts $\mathbf{c} = (c_0, \ldots, c_d)$ and $\mathbf{c}' = (c'_0, \ldots, c'_{d'})$, we define

$$\mathbf{c}_{mult} = (\hat{c}_0, \ldots, \hat{c}_{d+d'}),$$

where $\hat{c}_i = \sum_{i=k+j} c_k c'_j$, for $i \in \{0, \ldots, d + d'\}$.

Questions

3. Show that c_{mult} decrypts to $m_1 m_2$ and compute the error growth.
4. Let $s \in R$. Under the canonical embedding $\sigma(R) \subset \mathbb{Z}^n$, write down a matrix for the ideal lattice $\sigma(< s >)$.