M2-ENSL (2024-25): Homework

Notations: Given a power-of-two integer $N > 1$ and an integer $q > 1$, we define $\mathcal{R}_N = \mathbb{Z}[X]/(X^N + 1)$ and $\mathcal{R}_{q,N} = \mathbb{Z}_q[X]/(X^N + 1)$.

1. (**RLWE Security**)
   (a) Let $\iota : \mathcal{R}_{q,N} \to \mathcal{R}_{q,2N}$ be defined as $\iota(p(X)) = p(X^2)$. Show that ι is a ring homomorphism.
   (b) Let $\mathsf{ct} = (b, a) \in \mathcal{R}_{q,N}^2$ be an RLWE ciphertext. Check that $\iota(\mathsf{ct}) = (\iota(b), \iota(a)) \in \mathcal{R}_{q,2N}^2$ can be regarded as an RLWE ciphertext over $\mathcal{R}_{q,2N}$. What is the difference between regular RLWE over $\mathcal{R}_{q,2N}$ and the one constructed with ι?

2. (**Rescale**)
   (a) Let $p, q > 1$ be integers. Let $\mathsf{InvRescale} : \mathcal{R}_{q,N}^2 \to \mathcal{R}_{pq,N}^2$ be defined as $(b, a) \mapsto (pb, pa)$ and let $\mathsf{Rescale} : \mathcal{R}_{pq,N}^2 \to \mathcal{R}_{q,N}^2$ be a rescaling by p. Check that $\mathsf{Rescale} \circ \mathsf{InvRescale} = \mathsf{id}$ and $\mathsf{InvRescale} \circ \mathsf{Rescale} \neq \mathsf{id}$.
   (b) Let $p, r > 1$ be integers and $q > 1$ be an odd integer. Let $\mathsf{Rescale}_{pq} : \mathcal{R}_{pqr,N}^2 \to \mathcal{R}_{r,N}^2$ be a rescaling by pq, $\mathsf{Rescale}_p : \mathcal{R}_{pqr,N}^2 \to \mathcal{R}_{qr,N}^2$ be a rescaling by p, and $\mathsf{Rescale}_q : \mathcal{R}_{qr,N}^2 \to \mathcal{R}_{r,N}^2$ be a rescaling by q. Show that $\mathsf{Rescale}_{pq} = \mathsf{Rescale}_q \circ \mathsf{Rescale}_p$.

3. (**Key Switching**)
   (a) Let $\mathsf{KeySwitch}_{s_1 \to s_2}$ be a key switching from secret key s_1 to s_2. Check that the key switching error is independent from the underlying plaintext.
   (b) Let $\mathsf{swk} \in \mathcal{R}_{qp,N}^2$ be an RLWE switching key from secret key s_1 to s_2. Let $\varphi : \mathcal{R}_N \to \mathcal{R}_N$ be an automorphism (e.g., an evaluation in X^5 or X^{-1}). Check that swk can be interpreted as a switching key from $\varphi(s_1)$ to $\varphi(s_2)$.
   (c) Let $\mathsf{ct} = (c_0, c_1, c_2, c_3, c_4)$ be a ciphertext that decrypts with a secret key $\mathsf{sk} = (1, s_1, \varphi(s_1), s_2, \varphi(s_2))$, i.e., such that $c_0 \cdot 1 + c_1 \cdot s_1 + c_2 \cdot \varphi(s_1) + c_3 \cdot s_2 + c_4 \cdot \varphi(s_2) \approx \Delta \cdot m$. Check that one can convert it to a ciphertext encrypting the same plaintext and decrypts with $(1, s_2)$, using two switching keys and three key switchings.

4. (**CKKS Operations**) Let $Q_L = q_0 q_1 \cdots q_L$ be a chain of moduli such that $q_1, q_2, \ldots, q_L \simeq \Delta$. Suppose that we start with a scaling factor Δ at level L.
   (a) Let Δ_ℓ be a scaling factor at level ℓ. Show that $\Delta_{\ell-1} = \Delta_\ell^2 / q_\ell$.
   (b) Let $0 \leq \ell < \ell' \leq L$. Discuss how to add two ciphertexts ct_1 at level ℓ and ct_2 at level ℓ'.
   (c) In order to multiply two ciphertexts, one may consider two options $\mathsf{Rescale} \circ \mathsf{Relin} \circ \mathsf{Tensor}$ and $\mathsf{Relin} \circ \mathsf{Rescale} \circ \mathsf{Tensor}$. Compare two options in terms of efficiency and precision.

5. (**Bootstrapping Components**)
   (a) Given an integer $k > 1$, let $N = 2^{2k+1}$. Let A be a $2^{2k} \times 2^{2k}$ complex matrix and $\mathsf{ct} \in \mathcal{R}_{q,N}^2$ be a CKKS ciphertext encrypting a complex vector $\vec{z}$ of dimension 2^{2k}. Check that one can evaluate $A \cdot \vec{z}$ homomorphically with $2^{k+1} - 2$ rotations. (Hint: baby-step giant-step)
   (b) Check that one can evaluate $A \cdot \vec{z}$ homomorphically with the same number of rotations in (a) and with only 2 rotation keys.

(c) Let $p(x) = \sum_{i=0}^{2^k-1} a_0 x^i$ be a complex polynomial and $\mathsf{ct} \in \mathcal{R}_{q,N}^2$ be a CKKS ciphertext at level $\ell \geq k$. Show that one can perform element-wise polynomial evaluation of p homomorphically with at most k levels. That is, there is an instantiation of homomorphic evaluation of p such that the output ciphertext is at level $\ell - k$.

(d) Let $p(x)$ be a complex polynomial of degree 15. Find an algorithm for homomorphic evaluation of $p(x)$ while minimizing the number of relinearizations.