Assignment 4

In this practice, we will practice bootstrapping for the CKKS scheme.

q1. (10%) Install the OpenFHE package

q2. (20%) Use bootstrapping to reduce the noise caused by the arithmetic operations and report your observation. Please modify this file to see how bootstrapping helps reduce noise.

Hint: You can design a computation path that leads to large noise, then apply the bootstrapping.

q3. (20%) practice matrix-vector multiplication in CKKS.

Download the sample code from here. In the repo, there is a neural network implemented by C++ that inferences MNIST images but are not yet finished.

Please complete the function mat_vec_mul. The inputs are an *m* x n matrix **M** and a ciphertext **ctx** that encrypts an array with size *m*. The output is a ciphertext **ctx'** that encrypts the multiplication result of **M** and **ctx**.

Hint: Since the required matrix-vector multiplication with encrypted input is really different from the plaintext matrix-vector multiplication, it is highly recommended to take a look at the section **Linear Layer** in this tutorial before implementing it.

q4. (30%) Write down your implementation details and experiments in English.

The font size is 12, and the page limit is 3 pages.

Submission Guideline

Please submit your report named `{SID}_a4.pdf` (SID in upper case) to the COOL System, such as `D111111_a4.pdf`

Supplementary Materials

OpenFHE Installation