Introduction to Homomorphic Cryptosystems
Exercise Sheet 6: OpenFHE

Task 1 – Performance Comparison

Homomorphic encryption is often called the holy grail of cryptography, as it allows calculations on encrypted data. By using homomorphic encryption, data in clouds could thus be kept encrypted throughout, even during processing, which would give us quasi-perfect security in clouds. However, this security comes at a price, as homomorphic encryption entails a corresponding performance overhead.

a) To measure the performance overhead of the CKKS, initialize a CKKS cryptosystem with the following parameters: multDepth = 10, scaleModSize = 50 and batchSize = 2.

   Measure the execution times of the following operations on your system for the unencrypted and encrypted cases: (i) addition of two numbers and (ii) multiplication of two numbers.

b) Repeat the measurements from a) for the following initializations of the CKKS cryptosystem.

   - multDepth = 10, scaleModSize = 50 and batchSize = 2
   - multDepth = 25, scaleModSize = 50 and batchSize = 2
   - multDepth = 50, scaleModSize = 50 and batchSize = 2
   - multDepth = 10, scaleModSize = 50 and batchSize = 2
   - multDepth = 25, scaleModSize = 50 and batchSize = 16
   - multDepth = 50, scaleModSize = 50 and batchSize = 32

Task 2 – Homomorphic Statistic

The CKKS cryptosystem makes it possible to combine unencrypted numbers with encrypted numbers correctly. We can use this fact to calculate simple statistic metrics homomorphically using only addition and multiplication.

a) The mean value of the numbers $x_1, \ldots, x_n$ can be calculated as follows:

$$\bar{x} = \frac{1}{n} * \sum_{i=1}^{n} x_i$$

   Calculate the mean value for the following numbers, once encrypted and unencrypted: 1, 2, 3. Compare the execution times and accuracy of the calculated value for $\bar{x}$ of the encrypted and unencrypted variants.

b) The variance of the numbers $x_1, \ldots, x_n$ can be calculated as follows:

$$S^2 = \frac{1}{n} * \sum_{i=1}^{n} (x_i - \bar{x})^2$$

Calculate the variance for the following numbers, once encrypted and unencrypted: 1, 2, 3. Compare the execution times of and accuracy of the calculated value for S^2 of the encrypted and unencrypted variants.

c) The standard deviation of the numbers $x_1, \ldots, x_n$ can be calculated as follows:

$$S = \sqrt{S^2}$$

Calculate the standard deviation for the following numbers, once encrypted and unencrypted: 1, 2, 3. Compare the execution times and accuracy of the calculated value for S of the encrypted and unencrypted variant.

Note: In the homomorphic case, you can realize the multiplication with $\frac{1}{n}$ by calculating the inverse of n unencrypted and multiplying the ciphertext by the result. You may use the following approximation to calculate the square root: $\sqrt{x} \approx 1.2728x^3 - 2.784x^2 + 2.5223x$.