Introduction to Homomorphic Cryptosystems
Exercise Sheet 8: Binary Step Function

Task 1 – Homomorphic Implementation of the Binary Step Function

Now that we have implemented both the inverse and the root function homomorphically in exercise sheet 7, we want to use them to calculate the binary step BS function homomorphically. As a reminder, the following calculation rule was given in the lecture for the implementation of the BS function:

$$BS = \frac{1}{2} * (x * \frac{1}{\sqrt{x^2}} + 1) \tag{1}$$

Specifically, we want to implement the BS function homomorphically on the interval $[-1, 1]$.

a) To calculate the binary step function on this interval, the calculation of $\sqrt{x^2}$ is required.

   i) Specify the range of values on which we must be able to calculate the root to implement the BS function.

   ii) Configure your implementation of the root using the previously determined interval. Then, divide this interval into 100 evenly distributed points and calculate the root for these points once homomorphically and once in plain text. Plot both the homomorphically and non-homomorphically calculated root values in one figure.

b) To calculate the binary step function on this interval, the calculation of $\frac{1}{\sqrt{x^2}}$ is required.

   i) Specify the range of values on which we must be able to calculate the inverse to implement the BS function.

   ii) Configure your implementation of the inverse using the previously determined interval. Then, divide this interval into 100 evenly distributed points and calculate the inverse for these points once homomorphically and once in plain text. Plot both the homomorphically and non-homomorphically calculated inverse values in one figure.

c) Next, implement the BS function using the previously determined inverse and root calculation intervals.

d) Divide the interval $[-1, 1]$ into 100 evenly distributed points and calculate the BS function homomorphically for these points. Plot the calculated values against the real BS function.

λ	c
-0.5	8
0.5	3

Task 2 – Homomorphic Selection of the key with the lowest value

Determining the key with the lowest value is an important step that must be calculated in many machine-learning applications. For example, in the Box-Cox transformation, one must determine the λ value with the lowest c value. In this task, we therefore consider the following exemplary situation during a Box-Cox transformation, in which we have the following tuples:

Determine the λ value with the lowest c value.

a) In the lecture, the calculation of the minimum function was defined as follows:

$$min(a, b) = a + b - max(a, b) \tag{2}$$

$$max(a, b) = \frac{a + b}{2} + \frac{\sqrt{(a - b)^2}}{2} \tag{3}$$

   i) To calculate the minimum, it is necessary to calculate the root. Determine the interval on which we must be able to calculate the root. For this task, you can assume that the c values come from the interval $[0, 10]$.

   ii) Implement the minimum function homomorphically using the previously determined interval for the root function.

   iii) Calculate the lowest value of c homomorphically and compare it with the value that would have been determined in plain text.

b) If we apply the calculation rule from the lecture for determining the key with the smallest value to our example, we get:

$$\lambda_{min} = 2 * \sum_{i=1}^{2} BS(c_{min} - c_i) * \lambda_i \tag{4}$$

Implement this calculation rule homomorphically. Then, homomorphically determine the value of λ with the lowest c value and compare it with the value that would have been determined in plain text.