Introduction to Homomorphic Cryptosystems
Exercise Sheet 4: CKKS Encoding & Decoding

Task 1 – More examples for encoding and decoding

Use the algorithms from the lecture and apply CKKS encoding and decoding in the following two subtasks. Write down your intermediate results for z, p, m, h and the final result.

a) Input: $v = \begin{pmatrix} 23 \\ 15 \end{pmatrix}$

b) Input: $v = \begin{pmatrix} 4 \\ -3 \end{pmatrix}$

c) What do you observe when looking at the result from the decoding algorithm? How does this observation correspond to the original input for the encoding?

d) Bonus: Implement the encoding and decoding algorithms in a programming language of your choice.

Task 2 – Polynomial interpolation using the Vandermonde matrix

As already mentioned in the lecture, the CKKS encoding algorithm is basically a polynomial interpolation operation. To do this in the general case you can use the Vandermonde matrix and write the problem like this:

$$V(\vec{x}) * \vec{z} \stackrel{!}{=} \vec{y}$$

$\vec{x}$ are the x coordinates for which we evaluate the resulting polynomial and $\vec{y}$ are the y coordinates we want to receive ($\vec{x}, \vec{z}, \vec{y}$ are n-dimensional vectors). We now need to solve for $\vec{z}$ to get the coefficients of the polynomial that interpolates the points.

Find a polynomial that interpolates the points $(4, -6), (-3, 2), (5, 1)$ using the above equation.