



Floating-Point meets Fixed-Point: Exploring non-integer Multiplication Methods for Homomorphic Encryption

Advisor: **Florian Krieger**

DATE: November 20, 2024





Motivation

Homomorphic encryption (HE) raises huge attention since it offers superior privacy. However, HE still has a significant performance drawback. One reason for this drawback is the involved complex number arithmetic in \mathbb{C} which is costly in hardware and software implementations.

Goals and Tasks

The goal of this project is to enhance FHE efficiency by finding the optimal complex number multiplication method. We will evaluate different existing methods and find the best trade-off between computational effort and accuracy.

The main steps will be:

-  Get familiar with floating-point and fixed-point number formats
-  Evaluate the performance of different multiplication methods (for Software, Microcontroller, and FPGA)
-  Estimate the approximation error caused by the multiplication
-  Select the best suited multiplication method to support efficient HE

Literature

- > **J. Wang et al.**
A Compact and Efficient Hardware Accelerator for RNS-CKKS En/Decoding and En/Decryption
[IEEE Transactions on Circuits and Systems II: Express Briefs 2024](#)
<https://ieeexplore.ieee.org/abstract/document/10663672>

Courses & Deliverables

- Introduction to Scientific Working**
Short report on background
Short presentation
- Bachelor Project**
Project code and documentation
- Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

- CS
- ICE
- SEM

Prerequisites

- > Interest in the topic area, and basic knowledge of programming in Python/C

Advisor Contact

florian.krieger@iaik.tugraz.at