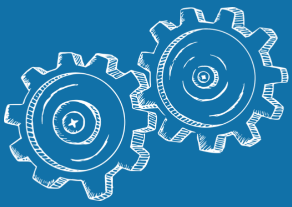


Floating-Point meets Fixed-Point: Exploring non-integer Multiplication Methods for Homomorphic Encryption

Advisor: **Florian Krieger**

DATE: February 5, 2025

Motivation

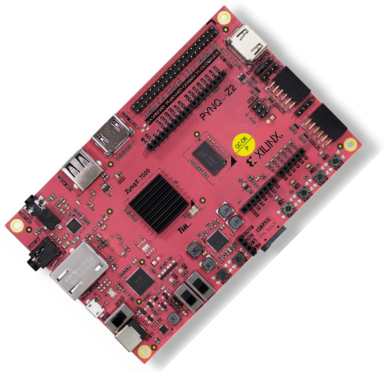
Homomorphic encryption (HE) raises huge attention since it offers superior privacy. However, HE still has a significant performance drawback. One reason for this drawback is the involved Fast Fourier Transformation and its complex number arithmetic in $\mathbb{C}$ which is costly in hardware and software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

Goals and Tasks

The goal of this project is to enhance FHE efficiency by optimizing complex number arithmetic within the FFT. We will focus on constrained platforms (ARM CortexM4 Microcontroller or small FPGAs) and optimize the multiplier specifically for the FFT computation.

The main steps will be:

- Get familiar with floating-point and fixed-point number formats and existing FFT approaches
- Either select a Microcontroller or FPGA as a target platform and implement an optimized complex number multiplier for FFT
- Benchmark your FFT implementation for performance, memory consumption, and approximation error



Literature

- J. Wang et al.
  A Compact and Efficient Hardware Accelerator for RNS-CKKS En/Decoding and En/Decryption, IEEE TCAS-II, 2024
  https://ieeexplore.ieee.org/abstract/document/10663672
- D. Natarajan and W. Dai
  SEAL-Embedded: A Homomorphic Encryption library for the IoT, TCHES 2021
  https://tches.iacr.org/index.php/TCHES/article/view/8991

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
+ DiplomandInnenseminar (CS)
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Basic knowledge of microcontroller or FPGA programming (e.g. Crypto on Software platforms, Digital System Design, etc.)