# Evaluation of different types of Memory Transfers on Xilinx Alveo datacenter FPGAs

Advisor: **Florian Hirner**

**DATE:** June 26, 2023

## Motivation

The increasing demand for high-performance data processing in various domains has driven the adoption of Field-Programmable Gate Arrays (FPGAs) as powerful acceleration devices. Xilinx Alveo Datacenter FPGAs, known for their exceptional computational capabilities, offer multiple interfaces and memory resources to facilitate efficient data transfers. There are different memory transfer techniques, including PCIe-based transfers, DDR4 memory interfacing, HBM2 memory interfacing, and Ethernet transfers that can be explored.

The main objective of this thesis is to investigate and implement various memory transfer methods on Xilinx Alveo Datacenter FPGAs. The student will have the opportunity to work with the latest and highest-performance Xilinx Alveo datacenter accelerator cards.

**NOTE: This thesis can be done by 1 or 2 students (Student 1: HBM2 + DDR4; Student 1: PCIe + Ethernet)**

## Goals and Tasks

- Get familiar with memory interfaces on Xilinx Alveo FPGAs and the AMBA AXI Protocol. [1-Month]
- Implementation of different memory transfer techniques for PCIe, DDR4, or HBM2. [2-Month]
- Evaluation and Benchmarking of the performance and speed on actual an FPGA. [1-Month]
- Recommendations optimizations for different type of memory transfers


## Literature


- R. Shi et al.
  Exploiting HBM on FPGAs for Data Processing
  https://doi.org/10.1145/3491238
- X. Docs
  Using Alveo Accelerator Cards
  https://tinyurl.com/7tysjuj5


## 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

- Interest in the topic area
- Basic knowledge of C/C++ and Verilog

## Advisor Contact

florian.hirner@iaik.tugraz.at

# Implement fast polynomial multiplications based on Radix-$2^n$ MDC using FPGAs

Advisor: **Florian Hirner**

**DATE:** June 26, 2023

## Motivation

Data privacy is a critical topic in today's digital world since nobody wants to have their data leaked. However, in certain cases, like medical image evaluation, these data need to be given in an unencrypted format to perform these evaluations. Homomorphic encryption (HE) enables computations on encrypted data to mitigate leakage.

HE requires certain operations like polynomial multiplications with large polynomials. Yet, it is relatively costly in terms of latency to perform one. A more advanced multiplication algorithm like the Fast-Fourier Transformation (FFT) and Number Theoretic Transform that can be used to reduce the latency from $O(n^2)$ to $O(n \cdot logn)$. There are different approaches to perform NTT, like Radix-$2^n$ NTT.

The goal of this project/thesis is to implement a hardware-based solution to perform different versions different Radix-$2^n$ FFT/NTT. The student will have the opportunity to work with the latest and highest-performance Xilinx Alveo data-center accelerator cards. The student should have an affinity towards VHDL/Verilog. Another goal is to find potential improvements within different Radix-$2^n$ versions to make them more efficient.

## Goals and Tasks

- Get familiar with the Fast Fourier Transformation and Number Theoretic Transform. [2-Weeks]
- A quick research of existing Radix-$2^n$ architectures. [2-Weeks]
- Extend a base version of Radix-$2^n$ to support higher degrees of Radix-$2^n$ , like Radix-4, Radix-8, ..., Radix-32 [2-Month]
- Suggest ways to accelerate these computations via different options like unrolling, pipeling, etc.
- Analyse and evaĺuate your implementations. [1-Month]

## Literature


- Matthias J. Kannwischer
  Polynomial Multiplication for Post-Quantum Cryptography
  https://kannwischer.eu/thesis/phd-thesis-print-version.pdf
- M. Garrido
  A Survey on Pipelined FFT Hardware Architectures
  https://doi.org/10.1007/s11265-021-01655-1


## 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 python or C/C++ and Verilog (e.g DSD ord SIP lecture)

## Advisor Contact

florian.hirner@iaik.tugraz.at