



Efficient Implementation of the CORDIC Algorithm on FPGAs

Advisor: **Florian Krieger**

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.

The CORDIC algorithm is a compelling alternative to compute the FFT. Therefore, we aim to efficiently implement the CORDIC algorithm and to integrate the design in the open-source Aloha-HE project.

Goals and Tasks

Some specific goals of this project are:

- > Investigate the CORDIC algorithm and its hardware implementation aspects.
- > Implement CORDIC on resource-constrained FPGAs.
- > Find efficient energy or power trade-offs
- > Implement side-channel countermeasures + experimental evaluation
-  Investigate the CORDIC algorithm and its hardware implementation aspects.
-  Implement and optimize CORDIC for resource-constrained FPGAs.
-  Integrate your design into Aloha-HE.
-  Compare your results to related works

Literature

- > [J. E. Volder](#)
The CORDIC Trigonometric Computing Technique, in IRE TEC, 1959
[doi:10.1109/TEC.1959.5222693](https://doi.org/10.1109/TEC.1959.5222693)
- > [F. Krieger et al.](#)
Aloha-HE: A Low-Area Hardware Accelerator for Client-Side Operations in Homomorphic Encryption
DATE 2024
[doi:10.23919/DAT58400.2024.10546608](https://doi.org/10.23919/DAT58400.2024.10546608)

Courses & Deliverables

- ☒ **Master Project**
Project code
Report
Presentation

– OR –
- ☒ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- > Interest in efficient hardware design
- > Cryptography on Hardware Platforms course is highly recommended

Advisor Contact

florian.krieger@tugraz.at