Fully Homomorphic Encryption Back-End for CirC
Milestone Report 6
07-400, Spring 2022

William Seo
https://northrim.github.io/07400-s22/mainpage.html

April 20, 2022

1 Progress Report

My work during the last two weeks was focused on looking into potential optimizations to add to the FHE compiler and beginning to implement them. More specifically, did the following:

- Read the HECO [1] paper to get an understanding of the type of optimizations used by the state of the art FHE compilers
- Decided with my project mentors to begin by adding Same Instruction Multiple Data (SIMD) optimizations to our backend
- Updated backend and SEAL interpreter to support vectorized inputs and computation by utilizing batch encoding

Additionally, I began working on a draft of my poster for the Meeting of the Minds presentation.

2 Reflection on Initial Plan

2.1 Major changes:

There are no major changes.

2.2 Meeting your milestone:

I am meeting my milestones.

2.3 Surprises:

There were no surprises.

2.4 Revisions to your 07-400 milestones:

I did not make revisions.

2.5 Resources needed:

For this section, nothing has changed from my original proposal.

References

[1] Alexander Viand, Patrick Jattke, Miro Haller, and Anwar Hithnawi. HECO: automatic code optimizations for efficient fully homomorphic encryption. *CoRR*, abs/2202.01649, 2022.