Fully Homomorphic Encryption Back-End for CirC
Milestone Report 5
07-400, Spring 2022

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

April 6, 2022

1 Progress Report

My work during the last two weeks was focused on setting up the SEAL interpreter and updating the FHE backend to support the new compilation pipeline. More specifically, I did the following:

- Implemented a SEAL interpreter that supports AND, OR, EQ, ADD, and MUL operations
- Updated the FHE backend in CirC to support the new compiling infrastructure of utilizing bytecode and the SEAL interpreter
- Constructed the automated building and testing infrastructure for the FHE backend
- Successfully tested AND, OR, EQ, ADD, and MUL operations

Additionally, I wrote and submitted my abstract for the Meeting of the Minds pre-registration.

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.