Fully Homomorphic Encryption Back-End for CirC
Milestone Report 4
07-400, Spring 2022

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

March 23, 2022

1 Progress Report

My work during the last few weeks was focused on finalizing the addition of the "Map" operation to the CirC. I made a GitHub pull request, reviewed the changes with my PhD mentors, and debugged some issues. Finally, we merged the pull request into the main GitHub branch of CirC.

Additionally, I have made progress in implementing implementing a SEAL interpreter which utilizes VM bytecode. To be more specific, I did the following:

- Forked the SEAL GitHub repository, and implemented a SEAL interpreter within it. So far, my implementation supports bytecode instructions for Boolean N-ary AND, OR and XOR operations
- Began updating the FHE backend in CirC to support the new compiling strategy of utilizing bytecode and a SEAL interpreter

2 Reflection on Initial Plan

2.1 Major changes:

There are no major changes.

2.2 Meeting your milestone:

With the revised updated milestones, I am on track.

2.3 Surprises:

There were no surprises.

2.4 Revisions to your 07-400 milestones:

We have revised the milestones to account for the following things:

- The original milestone did not take into account spring break
- The Map IR and SEAL Interpreter are taking longer than originally planned

2.5 Resources needed:

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