Fully Homomorphic Encryption Back-End for CirC
Milestone Report 1
07-400, Spring 2022

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

February 1, 2022

1 Progress Report

Most of my work during the past few weeks was focused on familiarizing myself with the CirC codebase, and integrating a new FHE backend to the CirC infrastructure. I am participating in weekly meetings with the CirC circuit compilation team. Additionally, I am have set up weekly check-up meetings with PhD student Edward Chen and monthly meetings with professor Wenting Zheng. Below is a list of my progress in constructing the FHE backend.

Winter Break Progress.

- Familiarized myself with the Rust language and the CirC codebase
- Set up access to the Neptune server[1] with Edward's help
- Added the SEAL library and new FHE mode to CirC

In-semester Progress:

- Began constructing the FHE Backend
- Determined structure of FHE code output. The output file will consist of two functions: *main* and *server*, each with different data access privileges
- Implemented the generation of the *main* and *server* function calls and SEAL parameter generation code
- Compiled a simple program and tested the compiled code with SEAL library
- Began implementing the compilation of Boolean functions

[1] I was not able to compile and test CirC locally on my Mac, so I have to work on the Neptune server instead.

2 Reflection on Initial Plan

2.1 Major changes:

There have been no major changes.

2.2 Meeting your milestone:

I have met the milestones I set for Feb. 1st on my project proposal. I am currently a bit ahead of the planned schedule, as I have already begun incorporating binary operations.

2.3 Surprises:

I ran into errors when trying to build the CirC codebase on my local machine. Fortunately, my mentor and I were able to resolve this issue by connecting my computer to a shared server.

2.4 Revisions to your 07-400 milestones:

There are no new revisions.

2.5 Resources needed:

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