Fully Homomorphic Encryption Back-End for CirC
Milestone Report 2
07-400, Spring 2022

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

February 15, 2022

1 Progress Report

My work during the past few weeks was focused on implementing new features into the FHE backend, and adding vectorization capabilities to the CirC IR (Intermediate Representation). Below is a more specific list of my progress.

- Completed implementing boolean AND/OR/XOR
- Tested the compiled boolean programs with SEAL
- Cleaned up formatting process by making template file
- Added a new 'Map' operation to the IR

2 Reflection on Initial Plan

2.1 Major changes:

We have decided to take a slight detour before implementing the other operations for the FHE backend. Below are the two tasks that I am aiming to achieve before going back to implementing the backend operations:

- Adding the Map operation to the CirC intermediate representation so that CirC can support vectorization.
- Changing the FHE compilation process to use VM bytecode. This will save significant compilation time from the current approach.

2.2 Meeting your milestone:

I have met the milestones for February 15th.

2.3 Surprises:

There were no surprises

2.4 Revisions to your 07-400 milestones:

I have revised the Feb 15th, March 1st, and March 15th milestones to account for the detour mentioned above.

2.5 Resources needed:

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