

Fully Homomorphic Encryption Back-End for CirC

Milestone Report 2

07-400, Spring 2022

William Seo

<https://northrim.github.io/07400-s22/mainpage.html>

March 1, 2022

1 Progress Report

My work during the last two weeks was focused on adding vectorization capabilities to the CirC IR. I worked on implementing the “Map” operation, which can be used to apply functions on array inputs. To be more specific, I achieved the following:

- Implemented code that evaluates the Map operation in the IR
- Implemented code that typechecks the Map operation

Also, I have begun working on implementing VM Bytecode for SEAL compilation.

2 Reflection on Initial Plan

2.1 Major changes:

There are no major changes.

2.2 Meeting your milestone:

I am slightly behind on my milestone. I had intended to make more progress in implementing the VM Bytecode for SEAL at this point. I am looking to get caught up during Spring Break.

2.3 Surprises:

There were no surprises.

2.4 Revisions to your 07-400 milestones:

There are no revisions.

2.5 Resources needed:

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