Week 1 Progress

Analysing 3 main papers

Paper 1: Accelerating Fully Homomorphic Encryption Through Microarchitecture-Aware Analysis and Optimization.
Paper 2: Over 100x Faster Bootstrapping in Fully Homomorphic Encryption through Memory-centric Optimization with GPUs
paper 3: HEAAN Demystified Accelerating Fully Homomorphic Encryption

They are couple of problems related to GPU and Professor Jung Hee Cheon proposed couple of solutions to solve those problems and through memory -centric optimization bottle neck problem is solved and by using microarchitecture-aware optimization the gpu speed is improved by more than 41%. All these 2 improvements are the upgrades of architecture-centric optimization which was causing high stress and bottle neck on gpu's.

Main Challenge:

The main problem I have noticed is that all the experiments were carried out on AVX-512 for all 3 papers and testing this proposed methods is highly necessary on other gpu's.

Solution:

Bootstrapping in Fully Homomorphic Encryption has results in high success rate and I will have to run their program on our available gpu to check the compatibility and the differences in speed as it is mention in the papers.

Next week 2

I will be working on getting the source code so as for me to test it and record results. This is going to give high picture of what needs improvements and how to improve it.