CrypTen functions implementation on CryptGPU system

Amithabh A
112101004

July 4, 2024

Introduction

CryptGPU

- A system for privacy-preserving machine learning that implements all operations on the GPU .
- Made on top of CrypTen (which is built on top of PyTorch) for Privacy-preserving Machine Learning
- Detailed slides (prepared based on CrypTen and CryptGPU papers)

Work

- CryptGPU is having only ReLU as activation function. The task is to implement Tanh and Sigmoid functions in CryptGPU

Dependency Tasks

- Update CrypTen library and CryptGPU system, which are outdated
  1. CryptGPU codebase which is being currently updated
  2. CrypTen codebase which has undergone updation
  3. setup scripts for CrypTen and CryptGPU
  4. CrypTen setup in Google Colaboratory

Ongoing Work and Optimal Plan

Ongoing work

- log files link

Goals and Plans

- Setting up of CryptGPU, which is not yet complete and not sure when will it be finished
- Writing up of tanh and sigmoid implementation
- Testing Tanh and sigmoid, further looking of additional functionality implementations, Incorporating changes to CryptGPU source repository

Major challenges

- link

References

- CrypTGPU: Fast Privacy-Preserving Machine Learning on the GPU
- CrypTen: Secure Multi-Party Computation Meets Machine Learning
- CrypTen parent codebase
- CrypTGPU parent codebase
- https://www.youtube.com/watch?v=8tWAxUgO2V0