EINDHOVEN UNIVERSITY OF TECHNOLOGY

Department of Mathematics and Computer Science
Coding Theory and Cryptology Group

Secure Sessions for Ad Hoc Multiparty Computation in MPyC

Master thesis

Emil Nikolov

Id nr: 0972305
emil.e.nikolov@gmail.com

Supervisor : Dr. ir. L.A.M. (Berry) Schoenmakers

March 1, 2023

Abstract

The field of Secure Multiparty Computation provides methods for jointly computing functions without revealing their private inputs from multple parties. This master thesis assignment focuses on the MPyC framework for MPC and explores various approaches for connecting the parties via the internet. A technical survey was performed in the preparation phase to identify viable techniques and tools to achieve that. Furthermore a test environment dubbed E^3 was developed to support the exploration process that will take place during the implementation phase of the assignment. It is composed of a combination of physical and virtual machines that are able to execute a multiparty computation together using MPyC. It employs several declarative Infrastructure as Code tools to automate the deployment process and make it reproducible. Specifically, Terraform is used for provisioning NixOS virtual machines on the DigitalOcean cloud provider and Colmena is used for remotely deploying software to them. The reference implementation described in this report uses the Tailscale mesh VPN for connectivity, and a number of additional implementations are planned for the next phase of the project.

Contents

List of Figures

0.1 Testing methodology

During the preparation phase of the project we developed the Extensible Evaluation Environment (E^3) framework which simplifies and automates the process of deploying machines in different georgraphical regions, connecting them in an overlay network and executing MPC computations between them, where each machine represents a different party. During the thesis assignment we will look at a number of solutions for ad hoc MPC sessions and compare them in terms of performance, security and usability.

0.1.1 Performance

Each solution will be deployed using the E^3 framework and the performance will be quantitatively measured in terms of the speed of execution of a number of pre-selected MPyC demos of different round complexities and message sizes:

- secret santa - high round complexity
-