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 7, 2023

Contents

List of Abbreviations

E^3 Extensible Evaluation Environment. 1

List of Figures

Chapter 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.

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 - Convolutional Neural Network (CNN) MNIST classifier - low round complexity, large message size

1.2 Security

We will analyze aspects such as - key distribution - trust model - are there any trusted third parties and what would be the consequences if they are corrupted or breached -

1.3 Usability

Each solution will be analyzed in terms of the actions that need to be taken by the parties in order to perform a multiparty computation.

Chapter 2

Wireguard

Wireguard is a simple VPN protocol built with the Noise Protocol Framework.