



ulm university universität



Implementation and Evaluation of Secure Shortest Path Algorithms

This project's goal is to implement and benchmark several secure shortest path algorithms. Suppose a service provider is in possession of a graph. A client would like to know the distance between two vertices A and B in this graph. However, the service provider does not want to reveal its graph to the client, and neither does the client want to reveal A and B to the service provider.

Previous work by different authors has proposed several algorithms that can achieve this. However, the evaluation of these algorithms has not been consistent, because different software frameworks and experimental setups were used.

For this reason, this project's task is to implement several secure shortest distance algorithms using a suitable framework for Secure Multiparty Computation (e.g. MP-SPDZ). In a second step, these implementations should be used to benchmark the performance of the considered algorithms.
 Project
 8/16

Suitable for all students who are interested in Privacy Enhancing Technologies, Secure Multiparty Computation, or Cryptography. Programming will play a large role in this project, so programming skills are a plus.

Juri Dispan | juri.dispan@uni-ulm.de | 027-3209

If your are interested or you need additional details, feel free to contact me or drop by for a non-binding chat.

