Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis B.Sc. | Thesis M.Sc. | IDP, Guided Research

Benchmarking Secure Multiparty Computation Protocols

Motivation

Secure Multiparty Computation (SMC) [1] enables multiple parties to evaluate a function over their private inputs and reveal nothing but the function's result. Potential applications for SMC are privacy-preserving auctions, private voting, and private data analysis among multiple parties. While the first general SMC protocols were developed in the 1980s, implementations have just been starting to get practical for complex applications. Currently, there are over a dozen state-of-the-art protocols for general SMC that are built on similar building blocks and provide different security guarantees. However, there is little understanding of the performance of SMC protocols for different kinds of use cases. Thus, there is a need for a systematic benchmark to compare different SMC protocols against each other and measure network and CPU parameters during the function evaluation.

Your Task

- Assess the performance of state-of-the-art SMC protocols for different reference use cases.
- Explore how performance differs when comparing protocols with different adversary models.
- Analyze how network bandwidth, latency, and processing capabilities impact the performance of different protocols.
- The relevant protocols have already been implemented in an open-source project [2]. Therefore you do not have to implement protocols yourself.

Prerequisites

- Experience in C/C++ programming.

Sources

[1] https://eprint.iacr.org/2020/300
[2] https://github.com/data61/MP-SPDZ

Contact

Christopher Harth-Kitzerow christopher.harth-kitzerow@tum.de