



Interested in privacy? Look up MPC!

Advisor: **Fabian Schmid**

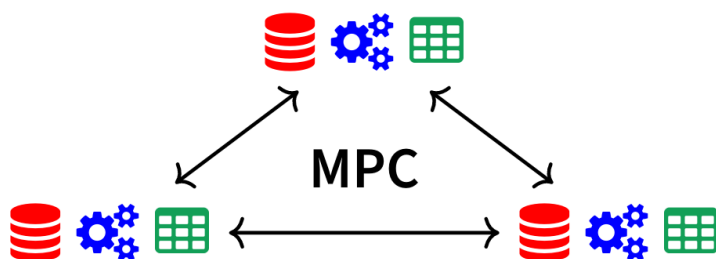
Motivation

In Secure Multi-Party Computation (MPC), parties collaborate to evaluate a function on their private inputs without revealing anything other than the final result. With this powerful primitive, data-driven use cases can be brought to privacy-sensitive data domains. However, many MPC schemes are limited in the concrete operations that can be performed on the protected data, rendering complex applications infeasible. In recent advancements, several works propose protocols to evaluate a lookup table within MPC. These building blocks allow for arbitrary function evaluation, though they impose considerable performance costs.

In this thesis, you will learn about MPC, secure computation, and modern protocols. In particular, you will bring these novel lookup table constructions into uncharted territory, testing the applicability in less studied MPC schemes.

Goals and Tasks

-  Study the basics of MPC and secure computations.
-  Understand novel lookup table constructions and get a feeling of underlying trade-offs.
-  Implement a lookup table construction in a novel setting and explore a related use case.



Overview of an MPC network collaboratively computing a function.

Literature

- > [F. Meisingseth, C. Rechberger, and F. Schmid](#)
Accelerating Multiparty Noise Generation Using Lookups
[Cryptography ePrint Archive 2025](#)
- > [H. Morita et al.](#)
{MAESTRO}:{Multi-Party}{AES} Using Lookup Tables
[34th USENIX Security Symposium \(USENIX Security 25\)](#)

Courses & Deliverables

- ☒ **Introduction to Scientific Working**
Short report on background
Short presentation
- ☒ **Bachelor Project**
Project code and documentation
- ☒ **Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- > Interest cryptography and privacy, motivation to implement modern protocols.

Advisor Contact

fabian.schmid@tugraz.at