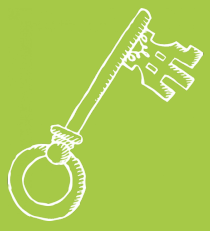


Improving Distributed ORAM

Advisor: **Verena Schröppel**

Motivation

Secure multi-party computation (MPC) lets several parties compute on secret-shared data that none of them can see. But looking up an element at a secret index requires touching the entire array, a linear cost that makes data-intensive applications impractical.

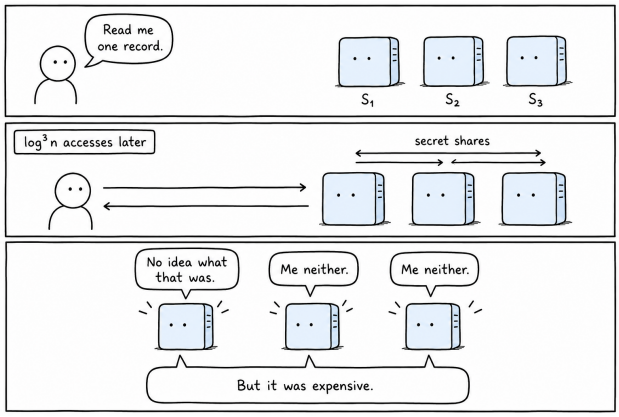
Distributed Oblivious RAM (DORAM) replaces this scan with a sublinear protocol that hides the access pattern: the parties learn nothing about which element was accessed.

Good asymptotics do not always mean good performance in practice. For some constructions the bottleneck is communication, for others local computation or the periodic rebuilding of the data structure, and which one hurts most depends on the setting.

In this thesis you will study the main ideas behind DORAM, benchmark existing constructions, locate their bottlenecks, and prototype an improvement.

Goals and Tasks

- Study MPC, ORAM, and how the two combine in distributed ORAM.
- Compare the constructions and locate the bottlenecks that dominate concrete cost.
- Benchmark existing DORAMs and prototype an improvement in preprocessing or rebuild cost.



Literature

- E. Stefanov et al.
  Path ORAM: An Extremely Simple Oblivious RAM Protocol
  ACM CCS 2013
- X. Wang, T.-H. H. Chan, and E. Shi
  Circuit ORAM: On Tightness of the Goldreich–Ostrovsky Lower Bound
  ACM CCS 2015

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in MPC and oblivious algorithms
- Motivation to implement modern protocols

Advisor Contact

verena.schroeppel@tugraz.at