

Oblivious RAM: Hiding What You Access

Advisor: **Verena Schröppel**

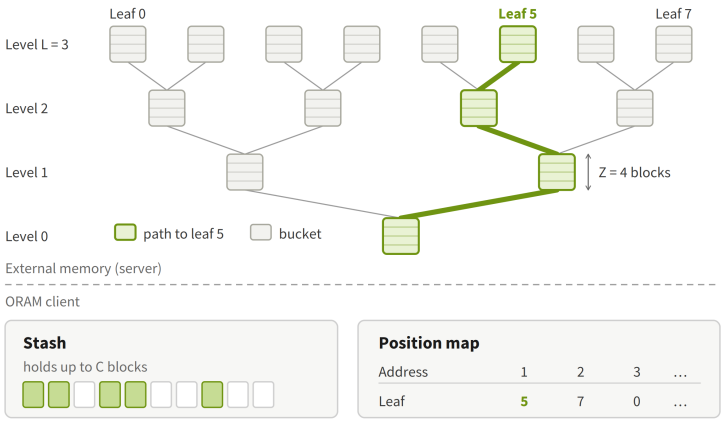
Motivation

Encryption protects the content of your data, but not the way you access it. The server storing it still sees which record you read, how often, and in which order. Such access patterns have been used to recover search queries, database contents, and a program's control flow.

Oblivious RAM (ORAM) closes this gap: every logical memory access is turned into physical accesses that look independent of the address actually requested. One direction we are particularly interested in is ORAM inside secure multi-party computation, so-called *distributed ORAM*.

Goals and Tasks

- Get familiar with existing ORAM constructions and their guarantees.
- Implement and benchmark one or more ORAM schemes.
- Evaluate and analyze the trade-offs of your implementation.



Path ORAM: each access reads and rewrites a whole root-to-leaf path, so the server learns nothing about the address.

Literature

- E. Stefanov et al.
  Path ORAM: An Extremely Simple Oblivious RAM Protocol
  ACM CCS 2013
- S. Jarecki and B. Wei
  3PC ORAM with Low Latency, Low Bandwidth, and Fast Batch Retrieval
  ACNS 2018

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 in privacy-enhancing technologies and efficient data structures.

Advisor Contact

verena.schroeppel@tugraz.at