Oblix: An Efficient Oblivious Search Index

Raluca Ada Popa, UC Berkeley

Search indices are fundamental building blocks of many systems, and there is great interest in running them on encrypted data. Unfortunately, many known schemes that enable search queries on encrypted data achieve efficiency at the expense of security, as they reveal access patterns to the encrypted data.

In this talk, I will present Oblix, a search index for encrypted data that is oblivious (provably hides access patterns), is dynamic (supports inserts and deletes), and has good efficiency. Oblix relies on a combination of novel oblivious-access techniques and recent hardware enclave platforms (e.g., Intel SGX). In particular, a key technical contribution is the design and implementation of doubly-oblivious data structures, in which the client's accesses to its internal memory are oblivious, in addition to accesses to its external memory at the server.

We demonstrate the usefulness of Oblix in several applications: private contact discovery for Signal, private retrieval of public keys for Key Transparency, and searchable encryption that hides access patterns and result sizes.