Oblivious Data Structures for Secure Multiparty Computation

Master’s Thesis

While encryption is an established technique for protecting data content, there are several scenarios where access patterns alone reveal sensitive information. Oblivious RAM (ORAM) is a building block that protects data access patterns: A client with limited memory makes requests to a server with large memory. The requested memory addresses are randomly distributed and independent of the data being read or written.

Secure multiparty computation (MPC) allows a group to jointly perform a computation without revealing the private input of any participant. Participants agree on a function to compute and can then use an MPC protocol to jointly compute the output of that function using their secret inputs without revealing them. For this purpose, functions are usually represented as circuits. This is not well suited for programs that rely on random access to memory. For example, performing a simple array access where the index is a private variable requires a circuit that scales linearly with the size of the array. This method, which involves touching each element of a data structure to perform an oblivious read or update operation, is called a linear scan.

This thesis is intended to first provide an overview of the different approaches for ORAM, with a particular focus on methods that are suitable for combination with MPC. Likewise, an overview of special Oblivious Data Structures, such as stacks or queues, that can be implemented more efficiently than with general ORAMs will be given. Based on this, gaps in the existing literature are identified.

Scope of the work

The student is expected to systematize existing literature on oblivious RAM and oblivious data structures with a focus on secure multiparty computation and identify gaps in the current state of the art. The goals of the thesis are to

- research the literature for different approaches to obtain oblivious memory access in the context of secure multiparty computation. Starting points for the literature search are listed in the references below.
- compare the different approaches regarding their trust assumptions, their security models and guarantees, their performance, etc.
- after the current state of the literature has been described and compared in detail, it should be determined in which aspects the current state is in need of improvement and to identify future research challenges.

While the thesis should focus on solutions in the context of secure multiparty computation, a short overview of general oblivious RAM and the challenges when combining it with secure multiparty computation will also be given.

Requirements

Following prior knowledge or skills are useful, but can also be acquired while working on the thesis:

- Familiarity with cryptographic security definitions
- Basic knowledge of MPC
- Experience in using a literature management software (e.g. Citavi, Zotero)

Interest in the topic is strongly recommended.

Contact

In case of interest or for further information, please contact Markus Raiber, markus.raiber@kit.edu
References


