Survey on Oblivious Data Structures for Secure Multiparty Computation

Bachelor’s Thesis

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

Secure multiparty computation (MPC) enables a group to jointly perform a computation without disclosing any participant’s private inputs. The participants agree on a function to compute, and then can use an MPC protocol to jointly compute the output of that function on their secret inputs without revealing them. Typically, to this end functions are represented as circuits. This is not well-suited to programs relying on random access to memory. For example, executing a simple array access where the index is a private variable requires a circuit that scales linearly in the size of the array. This method, where every element of a data structure is touched to perform an oblivious read or an update, is known as linear scan.

This thesis is intended to provide an overview of the different approaches for ORAM and to pay special attention to methods that are suitable for combination with MPC. Likewise, an overview of special Oblivious Data Structures, such as stacks or queues, which can be realized more efficiently than by using general ORAMs, will be given.

Scope of the work

The student is expected to write a survey on oblivious RAM and oblivious data structures with a focus on secure multiparty computation. 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:

- Basic knowledge of cryptography
- Experience with working with a reference 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


