Announcement of a Bachelor or Master Thesis in Cooperation with Fraunhofer AISEC, Garching

Secure Set Operations using Garbled Circuits

Motivation and Topic

Data analysis is widely used to gain useful information from vast data sets. Usage of this information varies widely and can include recommendation systems for streaming services or navigation systems with real-time traffic information. When the data is owned by one party and the analysis is done by another party both parties need to cooperate to gain these insights. But this cooperation carries risks for both parties. The data analyst might copy large portions or even the entire data set, gaining more information than intended. Similarly, the data owner might learn details about the analytic algorithms, which have been developed by the data analyst and are his assets.

Secure Computation offers a solution to this scenario, such that the two parties can compute basically any function without revealing either the input nor the details of the computation with each other. One of the most important protocols for this task are Yao's Garbled Circuits. In this protocol one party creates the garbled circuit and the other party evaluates the circuit. The protocol requires as input a boolean circuit representing the function to be computed.

The goal of this thesis is to first research the current state of the art in generating boolean circuits, especially in the context of Secure Computation with Yao’s Garbled Circuits. In a second step, one approach for generating boolean circuits ready for Secure Computation will be implemented further limited to circuits on set operations, such as intersection and complement.

Requirements

- Programming skills (Java, Python)
- Interest in Secure Computation, Cryptography
- Ability to work self-directed and systematically

The thesis can be written in English or German.

Contact

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Mark Gall
Email: mark.gall@aisec.fraunhofer.de
Phone: +49 89 322-9986-124