Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis B.Sc.

Thesis M.Sc.

Evaluating Large Boolean Circuits on a Multicore CPU efficiently

Motivation

Different Secure Multiparty Computation [1] protocols require expressing a function as a boolean circuit. Different compilers (such as CBMC-GC2 [2], emp-toolkit [3]) exist to convert a high-level program written in C or C++ into a boolean circuit stored in the Bristol Fashion [4] file format. However, the Bristol Fashion format is designed to evaluate a circuit sequentially. Also, a boolean circuit stored in Bristol Fashion takes up a lot of disk space. To faster evaluate large boolean circuits on modern multicore CPU, there should be an efficient file format with a low memory and storage footprint that is built for parallel evaluation of a circuit.

Your Task

- Develop a file format to efficiently store all gates of a boolean circuit.
- Develop ways to evaluate a boolean circuit in parallel.
- Develop a compiler that converts boolean circuits stored in Bristol Fashion into your developed file format.

Prerequisites

- Experience in C/C++ programming.

Sources

[1] https://eprint.iacr.org/2020/300
[2] https://gitlab.com/securityengineering/CBMC-GC-2
[3] https://github.com/emp-toolkit
[4] https://homes.esat.kuleuven.be/ nsmart/MPC/

Contact

Christopher Harth-Kitzerow christopher.harth-kitzerow@tum.de