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

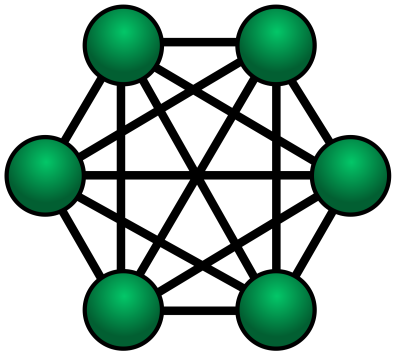
Thesis B.Sc.

Thesis M.Sc.

ECDSA Signatures for Efficient Byzantine Fault Tolerant Consensus in C++

Motivation

State-machine-replication (SMR) is used to build fault tolerant systems such as airplanes, cars, and industrial control systems. SMR consists of multiple machines (replicas), which agree on a common value even in case of faulty behaviour of single machines. In SMR, there are two main fault models, namely crash fault tolerance (CFT) and byzantine fault tolerance (BFT). For CFT systems, a replica runs as specified or it crashes. In BFT, a replica may behave arbitrarily (drop/send wrong values/messages).



In this thesis, we work on the BFT consensus protocol HotStuff [1]. The original authors provide a freely available C/C++ implementation of the protocol. While the specification demands the usage of threshold signatures to optimize communication complexity, this feature is neither implemented nor measured by the original authors. The main objective of this thesis is to add this functionality and measure the resulting performance impact.

Your Tasks

- Familiarize yourself with the HotStuff protocol and implementation
- Familiarize yourself with ECDSA threshold signatures
- Identify and implement the necessary code changes
- Measure the performance impact of your changes
- Evaluate the results

References

[1] Yin, Maofan, et al. ”Hotstuff: Bft consensus with linearity and responsiveness.” Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing. 2019.

Prerequisites

- Experience with Linux-based operating systems and networking
- Experience with C/C++ programming

Contact

Richard von Seck seck@net.in.tum.de
Filip Rezabek frezabek@net.in.tum.de