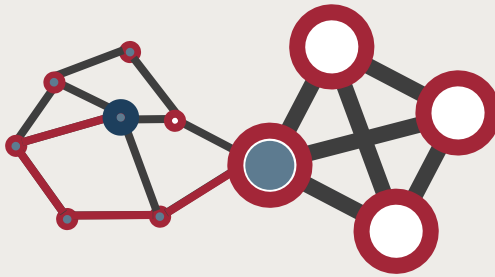


# Privacy Increasing Group Creation for Networks



Peer-to-peer networks sometimes use group based communication protocols. These share messages within a group of participants, e.g., to enhance privacy or provide fault tolerance.

But group-based network protocols are faced with the hard problem of creating suitable communication groups. This problem is especially hard if you want to optimize for privacy.

For privacy-preserving protocols we want communication partners that do not collude. The goal of this thesis is to design a scheme to classify network participants by collusion probability and deduce a suitable group size for minimal collusion.

The result of the thesis should be a proof of concept implementation of the scheme, as well as a theoretical evaluation of the probabilities involved.

Suitable for students with experience in network programming.

*Diese Arbeit kann auch auf Deutsch durchgeführt werden.*

David Mödinger | david.moedinger@uni-ulm.de | 027-3211

If you are interested or you need additional details, feel free to contact me or drop by for a non-binding chat.

