In this thesis, we introduce an unobservable message anonymization protocol, named *MessageVortex*. It bases on the zero trust principle, a distributed peer-to-peer (P2P) architecture, and avoids central aspects such as fixed infrstructures within a global network. It scores over existing work by blending its traffic into suitable existing tranport protocols, thus making it next to impossible to block it without significantly affecting regular users of the tranport medium. No additional protocol-specific infrastructure is required in public networks and allows a sender to control all aspects of a message such as the degree of anonymity, timing, and redundancy of the message transport without disclosing any of these details to the routing or transporting nodes. Part of this work is an RFC document attached in Appendix A describing the protocol. It contains all the necessary information to build protocol nodes. The RFC draft is available through the official RFC channels. Additionally, the RFC document, additional documents, and a reference are available under https://messagevortex.net/.

MessageVortex
Transport Independent and Unlinking Messaging

MessageVortex

Transport Independent and Unlinking Messaging

Inauguraldissertation zur Erlangung der Würde eines Doktors der Philosophie

vorgelegt der Philosophisch-Naturwissenschaftlichen Fakultät der Universität Basel

von

Martin Gwerder (06-073-787) von Glarus GL

December 15, 2019

Original document available on the edoc sever of the university of Basel edoc.unibas.ch.