We investigate the use of trusted execution environments (TEEs, such as Intel's SGX) for an anonymous communication infrastructure over untrusted networks. For this, we present the general idea of exploiting trusted execution environments for the purpose of anonymous communication, including a continuous-time security framework that models strong anonymity guarantees in the presence of an adversary that observes all network traffic and can adaptively corrupt a constant fraction of participating nodes. In our framework, a participating node can generate a number of unlinkable pseudonyms. Messages are sent from and to pseudonyms, allowing both senders and receivers of messages to remain anonymous. We introduce a concrete construction, which shows viability of our TEE-based approach to anonymous communication. The construction draws from techniques from cryptography and overlay networks. Our techniques are very general and can be used as a basis for future constructions with similar goals.

In this talk, we outline our construction and the main technical ideas used in our work. We supplement this by an overview of Intel SGX and describe how we implemented a prototype of our anonymous communication infrastructure using SGX.