Existing systems for anonymous messaging are all either not scalable, vulnerable to long term traffic analysis without unrealistic assumptions, or impose system-wide band- width restrictions that reduce usability and performance. These restrictions most often require that users send a fixed-length message once per system-defined round interval or else be vulnerable to traffic analysis. This is unrealistic in mobile environments where devices may go offline, but also imposes a global bandwidth rate that increases network overhead when users have no real messages to send and latency when users must defer additional messages subsequent rounds. Prior evaluations of systems have focused narrowly on the active processing of messages and have ignored performance costs due to these more complicated features of deployed systems.

We show that these assumptions can be relaxed significantly without compromising the central property that prevents traffic analysis: *input/output independence*. Leveraging this observation we design a fundamentally new ideal anonymity system, which we call *asynchronous variable retrieval (AVT)*. AVT resists traffic analysis under realistic user assumptions even if the adversary can observe the system indefinitely. While AVT could be implemented in existing implementation models (*e.g.*, mixnets, FHE, MPC), it requires new, more complicated primitives in systems that already suffer from poor scalability. Sparta is an implementation of AVT using trusted execution environments.

We show that Sparta can support high message throughput. Beyond this, we provide a new type of evaluation explicitly considering impact of system parameters, assumptions, and user behavior on system performance. We find that for guaranteed message delivery under one minute our model can improve the traffic requirements for long-term traffic analysis resistance and by 3400−54× compared to prior models. This corresponds to less than 1KBps user download rates which is cheaper than audio streaming.