Title:

New local differentially private protocols for frequency and mean estimation

Abstract:

Consider the following examples of distributed applications: a texting app wants to train ML models for autocomplete based on text history residing on-device across millions of devices, or the developers of some other app want to understand common app settings by their users. In both cases, and many others, a third party wants to understand something in the aggregate about a large distributed database but under the constraint that each individual record requires some guarantee of privacy. Protocols satisfying so-called *local differential privacy* have become the gold standard for guaranteeing privacy in such situations, and in this talk I will discuss new such protocols for two of the most common problems that require solutions in this framework: frequency estimation, and mean estimation.

Based on joint works with subsets of Hilal Asi, Vitaly Feldman, Huy Le Nguyen, and Kunal Talwar.