Abstract:

Local differential privacy (LDP) is a model where users send privatized data to an untrusted central server whose goal it to solve some data analysis task. In the non-interactive version of this model the protocol consists of a single round in which a server sends requests to all users then receives their responses. This version is deployed in industry due to its practical advantages and has attracted significant research interest. Our main result is an exponential lower bound on the number of samples necessary to solve the standard task of learning a large-margin linear separator in the non-interactive LDP model. Via a standard reduction this lower bound implies an exponential lower bound for stochastic convex optimization and specifically, for learning linear models with a convex, Lipschitz and smooth loss. These results answer the questions posed in \citep{SmithTU17,DanielyF18}. Our lower bound relies on a new technique for constructing pairs of distributions with nearly matching moments but whose supports can be nearly separated by a large margin hyperplane. These lower bounds also hold in the model where communication from each user is limited and follow from a lower bound on learning using non-adaptive \textit{statistical queries}.

Link: https://arxiv.org/abs/1911.04014