Statistics and Data Science Seminar

Perturbed M-Estimation: Ideas from Robust Statistics for Differential Privacy

Roberto Molinari (Auburn University)

Abstract: Differential privacy (DP) provides an elegant mathematical framework for defining a provable disclosure risk in the presence of arbitrary adversaries: it guarantees that whether an individual is in a database or not, the results of a DP procedure should be similar in terms of their probability distribution. While DP mechanisms are provably effective in protecting privacy, they often negatively impact the utility of the query responses, statistics, and/or analyses that come as outputs from these mechanisms. To address this problem, we use ideas from the area of robust statistics, which aims at reducing the influence of outlying observations on statistical inference. Based on the preliminary known links between differential privacy and robust statistics, we modify the objective perturbation mechanism by making use of a new bounded function and define a bounded M-Estimator with adequate statistical properties. The resulting privacy mechanism, named “Perturbed M-Estimation”, shows important potential in terms of improved statistical utility of its outputs as suggested by some preliminary results. These results motivate the current work which is being made in this direction.

Wednesday, October 5 at 4:00 PM in 636 SEO