Data Science Seminar

Hosted by the Department of Mathematics and Statistics

- Date: Tuesday, March 26, 2024
- Time: 12:00pm – 1:00pm
- Room: Whitney Hall 100E
- Speaker: Dr. Zeyu Ding (Department of Computer Science at Binghamton University)
- Title: Differential Privacy in Practice: How the US Government Protects Your Sensitive Information in the 2020 Census.

Abstract

Differential privacy (DP) is a de facto standard for data collectors to publish information about sensitive datasets while protecting the confidentiality of individuals who contribute data. It provides strong privacy protection against powerful adversaries by ensuring that any individual's data has very little influence on the released outcome. It is widely adopted by industry to collect sensitive information from users on the internet, as well as by some government agencies to publish population statistics. The most complex deployment of DP to date is for the 24th US census, the 2020 Census of Population and Housing. In this talk, I will give an introduction to the TopDown Algorithm, the disclosure avoidance system that was used to produce the 2020 Census Redistricting Data (P.L. 94-171) Summary File. The algorithm ingests the final, edited version of the 2020 Census data and creates noisy answers of key queries on the data, referred to as measurements. Privacy mechanisms that provide unbiased noisy answers to linear queries (such as marginals) are known as matrix mechanisms. I will also discuss our recent work called Residual Planner, a matrix mechanism for marginals that can optimize for a wide variety of convex objective functions and return solutions that are guaranteed to be optimal under Gaussian noise.

Biography of the speaker: Dr. Ding is an Assistant Professor in the Department of Computer Science at Binghamton University. He received his Ph.D. in Computer Science from Penn State University and B.S. in Mathematics from Zhejiang University. His research interests lie in the intersection of privacy, security, machine learning and algorithmic fairness. His current research focuses on differential privacy and its interactions with software security, formal verification, statistical inference and numerical optimization. His work has been published at top venues and has won one best paper award (CCS'18), two best paper runner-up awards (CCS'20, CCS'21) and the Caper Bowden PET Award Runner-up (2019).