HARVARD UNIVERSITY
17 Oxford Street
Cambridge, MA 02138

Mathematical Picture Language Seminar

Tuesday, October 5, 2021, at 9:30 a.m. EST

For Harvard affiliates, join us in ***Jefferson 453***

Zoom at https://harvard.zoom.us/j/779283357?pwd=MitXVm1pYUlJVzZqT3lwV2pCT1ZUQT09

Differential Privacy: The Mathematical Bulwark Against Reidentification and Reconstruction

Cynthia Dwork, Harvard Data Science Initiative,
Harvard University School of Engineering and Applied Science

Abstract: Differential privacy is a mathematically rigorous definition of privacy tailored to statistical analysis of large datasets. Differentially private systems simultaneously provide useful statistics to the well-intentioned data analyst and strong protection against arbitrarily powerful adversarial system users—without needing to distinguish between the two. Differentially private systems "don't care" what the adversary knows, now or in the future. Finally, differentially private systems can rigorously bound and control the cumulative privacy loss that accrues over many interactions with the confidential data. These unique properties, together with the abundance of commercial data sources and the surprising ease with which they can be deployed by a privacy adversary, led the US Census Bureau to adopt differential privacy as the disclosure avoidance methodology of the 2020 decennial census. The technology is also widely deployed in industry.