

Cybersecurity Research Acceleration Workshop and Showcase

October 11, 2017 | Indianapolis, IN

Protection of Data Privacy via Differentially Private Multiple Synthesis

challenge

Seek better ways to protect individual privacy in big data without compromising the accuracy of population-level information for research and public use

approaches and scientific merits

- ❖ bring a statistician's viewpoint to the utility question in differential privacy (DP).
- ❖ Develop innovative techniques and tools to create synthetic "surrogate datasets" that
 - have the same structure and similar statistical properties as the original dataset, but satisfying differential privacy.
 - are amenable to and accommodate various statistical analysis in real-life data
- ❖ Evaluates against both simulated data and real life studies Develops and release as open source tools for dataset creation.
- ❖ Leverages differential privacy and establishes an original framework to integrate DP with statistical modelling and inferences.

broader impacts

- ❖ Helps to increase the efficiency of data collection and dissemination cycle, without concerns on individual information breach, leading to better decision making and more transformative discoveries based on data of higher quality
- ❖ Promote awareness of data privacy in the general public & stimulates interests in STEM careers among K-12 students.

research results and future plan

- ❖ Have developed
 - modips (model-based differentially private data synthesis /dips)
 - mwas (dips via multiplicative weighting with adaptive selection of queries)
 - SAFE (Statistical allocation of Epsilon)
 - GGM (generalized Gaussian mechanism)
 - Noninformative bounding
- ❖ Have compared some of the dips methods in data utility via empirical studies
- ❖ Have applied some of the methods in the Current Population Survey and the American Housing Survey
- ❖ Future: methods for better utility in released data, development of practical tools/software

NSF BIGDATA: F: #1546373

University of Notre Dame

PI: Fang Liu (fang.liu.131@nd.edu)

Team: Claire Bowen, Evercita Eugenio, Yinan Li, Ashley Ahimbisibwe