

Theory and Practice of Differential Privacy (TPDP) 2019

November 11 - London, UK - Colocated with CCS 2019

Call for Papers

Differential privacy is a promising approach to privacy-preserving data analysis. Differential privacy provides strong worst-case guarantees about the harm that a user could suffer from participating in a differentially private data analysis, but is also flexible enough to allow for a wide variety of data analyses to be performed with a high degree of utility. Having already been the subject of a decade of intense scientific study, it has also now been deployed in products at government agencies such as the U.S. Census Bureau and companies like Apple and Google.

Researchers in differential privacy span many distinct research communities, including algorithms, computer security, cryptography, databases, data mining, machine learning, statistics, programming languages, social sciences, and law. This workshop will bring researchers from these communities together to discuss recent developments in both the theory and practice of differential privacy.

Specific topics of interest for the workshop include (but are not limited to):

- theory of differential privacy,
- differential privacy and security,
- privacy preserving machine learning,
- differential privacy and statistics,
- differential privacy and data analysis,
- trade-offs between privacy protection and analytic utility,
- differential privacy and surveys,
- programming languages for differential privacy,
- relaxations of the differential privacy definition,
- differential privacy vs other privacy notions and methods,
- experimental studies using differential privacy,
- differential privacy implementations,
- differential privacy and policy making,
- applications of differential privacy.

Submissions

The goal of TPDP is to stimulate the discussion on the relevance of differentially private data analyses in practice. For this reason, we seek contributions from different research areas of computer science and statistics. Authors are invited to submit a short abstract (4 pages maximum) of their work. Submissions will undergo a lightweight review process and will be judged on originality, relevance, interest and clarity. Submission should describe novel work or work that has already appeared elsewhere but that can stimulate the discussion between

different communities at the workshop. Accepted abstracts will be presented at the workshop either as a talk or a poster. The workshop will not have formal proceedings and is not intended to preclude later publication at another venue. Selected papers from the workshop will be invited to submit a full version of their work for publication in a special issue of the Journal of Privacy and Confidentiality.

Submission website: <https://easychair.org/conferences/?conf=tpdp2019>

Important Dates

Submission: June 28 (anywhere on earth)

Notification: August 9

Workshop: 11/11

Program Committee

- Michael Hay (co-chair), Colgate University
- Aleksandar Nikolov (co-chair), University of Toronto
- Aws Albarghouthi, University of Wisconsin–Madison
- Borja Balle, Amazon
- Mark Bun, Boston University
- Graham Cormode, University of Warwick
- Rachel Cummings, Georgia Tech University
- Xi He, University of Waterloo
- Gautam Kamath, University of Waterloo
- Ilya Mironov, Google Research – Brain
- Or Sheffet, University of Alberta
- Uri Stemmer, Ben-Gurion University
- Danfeng Zhang, Penn State University

For more information, visit the workshop website at <https://tpdp.cse.buffalo.edu/2019/>.