Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Research Seminar

Towards practical differentially private learning algorithms

Anand Sarwate
Rutgers

2-3pm Wednesday 6th July 2016

Abstract: Differential privacy has become a widely-studied framework for understanding how the results of computation on a database of individuals' private data can reveal information about individual records in the database. In this talk I will describe the differential privacy model and work with collaborators on algorithms for basic machine learning tasks that guarantee differential privacy and illustrate their performance on benchmark data sets. I will then describe ongoing work on designing differentially private algorithms for distributed data and some insights into where differentially private algorithms may provide usable privacy/utility tradeoffs.

Short Bio: Anand D. Sarwate is an Assistant Professor in the Department of Electrical and Computer Engineering at Rutgers, the State University of New Jersey. He received B.S. degrees in Electrical Engineering and Mathematics from MIT in 2002 and a PhD in Electrical Engineering from UC Berkeley in 2008. He is the Online Editor of the IEEE Information Theory Society (2015-) and an Associate Editor for the IEEE Transactions on Signal and Information Processing over Networks (2015-). Prof. Sarwate received the NSF CAREER award in 2015. His interests are in information theory, machine learning, and signal processing, with applications to distributed systems, privacy and security, and biomedical research.

Venue: Large Conference Room, O’Reilly Institute.

Further Details: http://www.scss.tcd.ie/doug.leith/seminars.php

ADAPT
Engaging Content
Engaging People