APPLIED MATHEMATICS COLLOQUIUM

"Computational Complexity in Differential Privacy"

Salil Vadhan
(Harvard University)

Abstract:
An exciting recent line of work in theoretical computer science has developed a new notion of privacy for computing on databases with sensitive information, known as "differential privacy." It requires that no individual's data should have a significant influence on the distribution of the (randomized) output. This is a strong privacy notion that is robust to auxiliary information available to an adversary, yet it has been shown to require only a small cost in accuracy for many computations of interest.

In this talk, I will describe how computational resource constraints can affect the achievability of differential privacy. We will consider both resource constraints on the data curator (making privacy harder to achieve) and on the adversary (making privacy easier to achieve). For the former, we show that it is computationally intractable to generate differentially private "synthetic data" that preserves even very simple statistics (2-way marginals), even though much more is possible without computational constraints. For the latter, we show that a computational relaxation of differential privacy (where we only consider computationally bounded adversaries) allows for significantly more accurate 2-party protocols for estimating the Hamming distance between two binary vectors.

Based on joint works with Cynthia Dwork, Andrew McGregor, Ilya Mironov, Moni Naor, Omer Reingold, Guy Rothblum, Omkant Pandey, Toni Pitassi, Kunal Talwar, and Jon Ullman.

Monday April 11th, 2011
4:30 PM
Building 2, Room 105
Refreshments are available in Building 2, Room 290
(Math Common Room) between 3:30 – 4:30 PM

Applied Math Colloquium: http://www-math.mit.edu/amc/spring11
Mathematics Department: http://www-math.mit.edu
To sign up for Applied Mathematics Colloquium announcements, please contact avisha@math.mit.edu

Massachusetts Institute of Technology
Department of Mathematics
Cambridge, MA 02139