

Communications/ICWS Seminar



Title: “Extremal Mechanisms for Local Differential Privacy”

Speaker: Peter Kairouz
Grad Research Assistant
UIUC - ECE/CSL

Date: Monday, February 16, 2015

Time: 4:00 PM

Location: 141 CSL

Abstract:

Local differential privacy has recently surfaced as a strong measure of privacy in contexts where personal information remains private even from data analysts. Working in a setting where both the data providers and data analysts want to maximize the utility of statistical analyses performed on the released data, we study the fundamental trade-off between local differential privacy and utility. This trade-off is formulated as a constrained optimization problem: maximize utility subject to local differential privacy constraints. For a given utility function and privacy level, the outcome of this constrained maximization problem is the optimal privatization mechanism that maximizes utility while achieving the desired level of privacy. We identify the combinatorial structure of the family of optimal privatization mechanisms for a broad class of information theoretic utilities that includes mutual information and all f -divergences as special cases. We further prove that for a given utility function and privacy level, solving the privacy-utility maximization problem is equivalent to solving a finite-dimensional linear program. However, solving this linear program can be computationally expensive since it has a number of variables that is exponential in the size of the alphabet the data lives in. To account for this, we show that two simple privatization mechanisms are universally optimal in the high and low privacy regimes, and well approximate the intermediate regime.

Bio:

Peter Kairouz is a PhD student at the University of Illinois at Urbana-Champaign (UIUC). He received his MS in ECE from UIUC in 2012 and his BE in ECE from the American University of Beirut (AUB) in 2010. He was a research intern at Qualcomm Inc. from May 2012 to August 2012 and May 2013 to August 2013. He has received numerous scholarships and awards including the Roberto Padovani Scholarship from Qualcomm's Research Center in 2012, the Distinguished Graduating Student Award from AUB's ECE department in 2010, and the Benjamin Franklin Scholarship from the United States Agency for International Development in 2007. His research interests include anonymous communication, statistical data privacy and security, machine learning, and big data.