UNIVERSITY OF CHICAGO
DEPARTMENT OF COMPUTER SCIENCE
PRESENTS:

"Randomness Extraction and Privacy Amplification"

Eshan Chattopadhyay
Simons Institute for the Theory of Computing

Abstract:
Randomness is a powerful resource in computer science, with applications in areas like cryptography, algorithms, and more. A fundamental problem here is to produce high quality random bits from naturally occurring defective sources of randomness. Indeed, this is an important task since using low quality random bits poses the danger of leakage of securely encrypted data or incorrect executions of randomized algorithms. This motivates the notion of a randomness extractor, which is an algorithm that produces purely random bits given access to low quality random sources.

It is known that it is impossible to produce purely random bits from a single defective source. An important open question in this area was that of extracting purely random bits from 2 independent weak sources of randomness (this was raised in [Chor-Goldreich, 1985]). In joint work with David Zuckerman, we provide an almost optimal solution to this question, achieving exponential improvements over prior work in terms of the entropy requirements of the weak sources.

Efficient randomness extractors have also found many important applications in cryptography. We construct stronger variants of extractors that lead to almost optimal protocols for privacy amplification, which is a well studied problem in cryptography. Based on joint works with Vipul Goyal and Xin Li.

Bio:
Eshan Chattopadhyay is currently a Research Fellow at the Simons Institute for the Theory of Computing. In Fall '16, he was a Postdoctoral Fellow at the Institute for Advanced Study, Princeton. He finished his PhD at UT Austin in May, 2016 under the supervision of David Zuckerman, where he was awarded the Bert Kay Dissertation Award for the best dissertation in computer science.

His research primarily focuses on the role of randomness in computation, pseudorandomness and cryptography. His research awards include a US Junior Oberwolfach Fellowship, and a best paper award at STOC 2016.

Monday, February 13, 2017
2:30 pm
Ryerson 251
Host: Ketan Mulmuley