# The University of Chicago

# Department of Computer Science & Mathematics

# Combinatorics & Theory Seminar

 **PRESENTS:**

 

**Rahul Santhanam (Oxford)**

**https://www.cs.ox.ac.uk**

**Title:** Pseudorandomness and the Minimum Circuit Size Problem”

**Abstract:** In the Minimum Circuit Size Problem (MCSP), the input is the truth table of a Boolean function f together with a parameter s, and the question is whether f has circuits of size at most s. MCSP is a rare example of a natural problem in NP for which we do not have strong evidence either of easiness or of NP-hardness. In the first half of the talk, I will give motivation and context for the study of MCSP. I will compare and contrast it with SAT, and sketch its relevance to complexity lower bounds, learning and proof complexity. In the second half of the talk, I will sketch some recent results addressing a fundamental question in cryptography: is there a natural problem in NP whose hardness is equivalent to the existence of one-way functions? Under a certain conjecture about universal pseudorandom distributions, I show that the following are equivalent: (i) MCSP is hard on average (ii) One-way functions exist (iii) Cryptographic pseudorandom generators exist (iv) Learning polynomial-size Boolean circuits is hard (v) Natural proofs (as defined by Razborov and Rudich) do not exist.

Tuesday, November 27, 2018

Ry. 251 @ 3:30 pm

(Refreshments will be served prior to the talk in Ry. 255 @ 3:15pm)