The Weizmann Institute of Science
Faculty of Mathematics and Computer Science

Foundations of Computer Science Seminar

Room 155, Ziskind Building
on Monday, Mar 04, 2024
at 11:15

Ran Canetti
Boston University

will speak on

Towards general-purpose program obfuscation via local mixing

Abstract:
We explore the possibility of obtaining general-purpose program obfuscation for all circuits by way of making only simple, local, functionality-preserving random perturbations in the circuit structure. Towards this goal, we use the additional structure provided by reversible circuits, but no additional algebraic structure.

We start by formulating a new (and relatively weak) obfuscation task regarding the ability to obfuscate random circuits of bounded length. We call such obfuscators Random Input & Output (RIO) obfuscators. We then show how to construct indistinguishability obfuscators for all (unbounded length) circuits given only an RIO obfuscator --- under a new assumption regarding the pseudorandomness of sufficiently long random reversible circuits with known functionality, which in turn builds on a conjecture made by Gowers (Comb. Prob. Comp. '96) regarding the pseudorandomness of bounded-size random reversible circuits. Furthermore, the constructed obfuscators satisfy a new measure of security which is stronger than IO and may be of independent interest.

We then investigate the possibility of constructing RIO obfuscators using local, functionality preserving perturbations. Our approach is rooted in statistical mechanics and can be thought of as locally ``thermalizing'' a circuit while preserving its functionality. We provide candidate constructions along with a pathway for analyzing the security of such strategies.

Given the power of program obfuscation, viability of the proposed approach would provide an alternative route to realizing almost all cryptographic tasks using the computational hardness of problems that are very different from standard ones.

Joint work with Claudio Chamon and Andrei Ruckenstein (BU Physics) and Eduardo Mucciolo (UCF Physics).