THE WEIZMANN INSTITUTE OF SCIENCE
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
Faculty Seminar

on Monday, May 25, 2020at 17:30

Zoom meeting: https://weizmann.zoom.us/j/99368552173

Rotem Arnon-Friedman UC Berkeley

Randomness extraction and amplification in the quantum world

Abstract:

Randomness is an essential resource in computer science. In most applications perfect, and sometimes private, randomness is needed, while it is not even clear that such a resource exists. It is well known that the tools of classical computer science do not allow us to create perfect randomness from a single weak source of randomness - a fact that initiated the study of special functions called randomness extractors.
The first part of the talk will be focused on the performance of randomness extractors in the presence of a quantum adversary and present a new model for two-source extractors, termed the quantum Markov model.
In the second part of the talk I will describe a task called "randomness amplification and privatization", where a single and public Santha-Vazirani source of randomness is being transformed into uniform and private randomness - a cryptographic task that cannot be accomplished using the tools of classical computer science. I will then present a protocol that builds on the extractors discussed in the first part of the talk and explain the main ingredients of its security proof.

Zoom meeting : https://weizmann.zoom.us/j/99368552173