The Weizmann Institute of Science
Faculty of Mathematics and Computer Science

Foundations of Computer Science Seminar

Room 155, Ziskind Building
on Monday, Jul 01, 2024
at 11:15

Noam Mazor
Cornell Tech

will speak on

Incompressibility and Next-Block Pseudoentropy

Abstract:
A distribution is k-incompressible, Yao [FOCS '82], if no efficient compression scheme compresses it to less than k bits. While being a natural measure, its relation to other computational analogs of entropy such as pseudoentropy (Hastad, Impagliazzo, Levin, and Luby [SICOMP 99]), and to other cryptographic hardness assumptions, was unclear.

We advance towards a better understating of this notion, showing that a k-incompressible distribution has (k-2) bits of next-block pseudoentropy, a refinement of pseudoentropy introduced by Haitner, Reingold, and Vadhan [SICOMP '13]. We deduce that a samplable distribution X that is (H(X) + 2)-incompressible, implies the existence of one-way functions.

Joint work with Iftach Haitner and Jad Silbak.