

פרופסור רפאל פס

המחלקה למדעי המחשב
אוניברסיטת קורנל וקורנל טק
ניו יורק, ארה"ב

Professor Rafael Pass

Department of Computer Science
Cornell University and Cornell Tech
New York, USA

הרצאה במסגרת הקולוקוויום במדעי המחשב

Lecture in the framework of the Computer Science colloquium

CRYPTOGRAPHY FROM THE HARDNESS OF KOLMOGOROV COMPLEXITY

Abstract

Whether one-way functions (OWFs) exist is the most important outstanding problem in Cryptography. We will survey a recent thread of work (Liu-Pass, FOCS'20, Liu-Pass, STOC'21, Liu-Pass, Crypto'21) showing the equivalence of the existence of OWFs and (mild) average-case hardness of various problems related to time-bounded Kolmogorov complexity that date back to the 1960s. These results yield the first natural, and well-studied, computational problems characterizing the feasibility of the central private-key primitives and protocols in Cryptography.

Based on joint works with Yanyi Liu.

The Lecture will be held on Sunday
7 November 2021, at 11:10
Seminar Room 420, Checkpoint Building
Tel Aviv University, Ramat-Aviv

ההרצאה תתקיים ביום ראשון
7 בנובמבר 2021, בשעה 11:10
חדר סמינרים 420, בניין צ'ק פוינט
אוניברסיטת תל-אביב, רמת-אביב

כיבוד קל יוגש לפני ההרצאה | Light refreshments will be served before the lecture