

שם הקורס: סמינר על פסאודו-אקראיות
מספר הקורס: 236804
מרצה: ד"ר רון רוטבלום
דרישות קדם: תורת החישוביות 236343
סמסטר חורף תש"פ

תיאור הקורס:

פסאודו-אקראיות הינה תורה העוסקת בייצור אובייקטים ש"נראים אקראיים" למרות שיוצרו בשימוש במעט מאד אקראיות אמיתית או אפילו באופן דטרמניסטי לחלוטין. הסמינר יתמקד בהגדרת אובייקטים פסאודו-אקראיים, בנייתם, קשרים ביניהם ויישומים בתאוריה של מדעי המחשב. בפרט נעסוק ב:

1. Bounded independence hash functions
2. Small bias generators
3. Expander graphs
4. Randomness extractors
5. Pseudorandom generators

רשימת ספרות:

Salil P. Vadhan (2012), "Pseudorandomness", Foundations and Trends in Theoretical Computer Science: Vol. 7: No. 1–3, pp 1-336.

<https://people.seas.harvard.edu/~salil/pseudorandomness/pseudorandomness-published-Dec12.pdf>

דרישות הקורס:

1. נוכחות בשיעור
2. מתן הרצאה מדעית בנושא שיבחר ע"י המרצה. הנחיות מפורטות תינתנה בהמשך לנרשמים לקורס.

רישום ידני:

נא לשלוח לשלוח שם+ממוצע+ת"ז ל- rothblum@cs.technion.ac.il