

שם הקורס – הוכחות אפס מידע

מספר הקורס – 236601

סמסטר – חורף תשפ"ב

מרצה:	ד"ר רון רוטבלום
מתרגל/בודק תרגילים:	
שעות הרצאה:	
דרישות קדם:	תורת החישוביות 236343
אתר הקורס: (כתובת האתר)	

תיאור הקורס

הוכחות אפס מידע מאפשרות להוכיח את נכונותן של טענות מבלי לחשוף אך פרט מעבר לנכונות של הטענה. להוכחות אפס מידע ישנם השפעות מרחיקות לכת בקריפטוגרפיה וסיבוכיות. קורס זה, שהינו קורס מבוא למחקר בתחום, יעסוק באספקטים רבים של הוכחות אפס מידע, למשל:

1. אפס מידע: הגדרות ובניות בסיסיות.
2. הוכחות אפס מידע לכל NP.
3. הוכחות אפס מידע סטטיסטי (statistical zero-knowledge): אפיון ובעיות שלמות.
4. הוכחות אפס מידע: מספר סיבובים.
5. Non-interactive zero-knowledge
6. ועוד...

תוצרי למידה

סטודנטים שישלימו את הקורס בהצלחה יבינו לעומק את הנושא של הוכחות אפס מידע. בפרט, יהיו ערוכים ומוכנים לקריאת מאמרים עדכניים בתחום וביצוע מחקר בנושא

דרישות הקורס

הקורס: כ-3 תרגילי בית ומבחן קל.