יום עיון בקריפטולוגיה

הפקולטה למדעי המחשב, הטכניון, חיפה, יום ג', 30 בדצמבר, 2014

cryptoday.org

תוכנית יום העיון Cryptoday 2014

12:00	התכנסות, כיבוד קל
12:35	דברי פתיחה
12:40	פרופ' יהודה לינדל, אוניברסיטת בר-אילן Cut-and-Choose Based Two-Party Computation in the Online/Offline and Batch Settings
13:30	Dr. Elena Andreeva, אוניברסיטת K.U. Leuven, בלגיה Security Aspects of Authenticated Encryption*
14:20	הפסקה
14:30	פרופ' עדי שמיר, מכון ויצמן למדע (בשיתוף עם הקולוקוויום הפקולטי) How to Reach Unreachable Computers*
15:30	הפסקה והצגת פוסטרים
16:00	דניאל גנקין, הטכניון "אני יודע מה עשית בפעגוח האחרון: התקפות ערוצי צד על מחשבים אישיים"
16:50	דר' גיל שגב, האוניברסיטה העברית בירושלים Functional Encryption: Introduction and Recent Advances
17:40	יניב כרמלי, הטכניון Linear Cryptanalysis of FEAL-8X – Winning the FEAL 25 Years Challenge
18:30	סיום

ההרצאות המסומנות ב-* תתקיימנה באנגלית

אודיטוריום 1, בניין טאוב למדעי המחשב, הטכניון, חיפה

יום העיון מאורגן על-ידי פרופ' אלי ביהם
והמרכז להנדסת מחשבים בטכניון

השתתפות ביום העיון חופשית, אנא הירשמו מראש באתר

ההרצאות תתקיימנה בעברית, פרט להרצאות המסומנות ב-*

סטודנטים מוזמנים להציג תוצאות מחקריות בפוסטרים

תתאפשר כניסה עם רכב לטכניון

פרטים נוספים באתר הכנס
cryptoday.org

Technion Computer Engineering