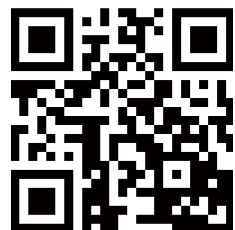


יום עיון בקריפטולוגיה

הפקולטה למדעי המחשב, הטכניון, חיפה, יום ב', 28 בדצמבר, 2015

יום העיון מאורגן על-ידי פרופ' אלי ביהם
מרכז הסייבר בטכניון
והמרכז להנדסת מחשבים בטכניון
ההשתתפות ביום העיון חופשית
אך יש להירשם מראש באתר
רוב ההרצאות תתקיימנה בעברית
סטודנטים מוזמנים להציג
תוצאות מחקריות בפוסטרים
תתאפשר כניסה עם רכב לטכניון
פרטים נוספים באתר הכנס
cryptoday.org



תוכנית יום העיון Cryptoday 2015

09.00	התכנסות, כיבוד קל
09.30	דברי פתיחה
09.35	פרופ' אלי בן-ששון, הטכניון Public-Setup Computational Integrity via Quasi-Linear PCPs - Prospects and Challenges
10.20	איציק מנטין, אימפרבה Bar-Mitzva Attack: Breaking SSL with 13-Year Old RC4 Weakness
11.05	הפסקה
11.15	Keynote Lecture Prof. Bart Preneel, KU Leuven and iMinds, Belgium Crypto Under Siege: New Threat Models Lecture will be given in English - ההרצאה תינתן באנגלית
12.15	תומר אשור, KU Leuven Simon: NSA-Designed Cipher in the Post Snowden World
12.45	הפסקה וארוחת צהריים קלה + הצגת פוסטרים
13.50	דר' צביקה ברקרקסי, מכון וייצמן למדע Fully Homomorphic Encryption
14.35	דר' איתי דינור, אוניברסיטת בן-גוריון On the Security of Concatenating Hash Functions: Classical and New Results
15.20	הפסקה
15.30	מור וייס, הטכניון Looks Matter: Practical Solutions for Format Preserving Encryption
16:15	פרופ' יהודה לינדל, אוניברסיטת בר-אילן Extremely Fast Authenticated Encryption with Full Protection Against Bad Randomness
17.00	דברי סיום

cryptoday.org