



"It was it for me to kill the heir-apparent"

שחזור של Turing Bombe בכלצ'לי פארק

יום ציון בקריפטולוגיה

הפקולטה למדעי המחשב, הטכניון, חיפה, יום ד', 4 ביולי, 2012

ההרצאות תתקיימנה בעברית
בבניין טאוב, אודיטוריום 1, הטכניון, חיפה
תתאפשר כניסה עם רכב לטכניון

ההשתתפות ביום הציון חופשית
אנא הרשמו מראש באתר

סטודנטים מוזמנים להציג
תוצאות מחקריות בפוסטרים
פרס כספי יוענק לפוסטר הטוב ביותר

תוכנית הכנס:

09: 00 התכנסות, כיבוד קל

09: 30 דברי פתיחה

09: 35 פרופ' אמיר הרצברג, אוניברסיטת בר-אילן
Off-path Interception, Modification and Poisoning Attacks

10: 25 דר' בני אפלכאום, אוניברסיטת תל-אביב
New Advances in Garbling Circuits

11: 15 הפסקה והצגת פוסטרים

11: 50 דר' ערן יהב, הטכניון
Differential Program Analysis for Exploit Generation

12: 40 הפסקה

13: 40 דר' אור דונקלמן, אוניברסיטת חיפה
The Hitchhiker's Guide to the SHA-3 Competition

14: 30 יוסי אורן, אוניברסיטת תל-אביב
The Mechanical Cryptographer: Tolerant Algebraic Side-Channel Attacks using pseudo-Boolean Solvers

15: 20 דר' נתן קלר, אוניברסיטת בר-אילן
Dissect and Conquer: New algorithms for cryptanalysis of multiple encryption, knapsacks and other combinatorial search problems

16: 10 סיום

cryptoday.biham.net