4th BIU Winter School: Symmetric Cryptography

Location: Wohl Center, Bar-Ilan University

School organizers: Yehuda Lindell and Benny Pinkas

Monday, January 27, 2014 – Theoretical Foundations	
9:00 am to 9:30 am	***Registration***
9:30 am to 9:35 am	Opening remarks
9:35 am to 11:00 am	One-way functions and hard-core predicates (Goldreich-Levin) Lecturer: Iftach Haitner
11:00 am to 11:30 pm	*Coffee break*
11:30 am to 1:00 pm	Pseudorandom generators (definitions and constructions; the hybrid method) Lecturer: Benny Applebaum
1:00 pm to 2:30 pm	*Lunch*
2:30 pm to 3:45 pm	Pseudorandom functions and permutations (definitions and constructions) Lecturer: Iftach Haitner
3:45 pm to 4:15 pm	*Coffee break*
4:15 pm to 6:00 pm	Symmetric encryption and MACs (definitions and constructions) Lecturer: Benny Applebaum
6:00 pm	*Bus to hotel and Tel Aviv*
Tuesday, January 28, 2014 – Cryptanalysis	
9:30 am to 11:00 am	Generic Cryptanalytic Techniques Lecturer: Orr Dunkelman
11:00 am to 11:30 am	*Coffee break*
11:30 am to 1:00 pm	Differential Cryptanalysis Lecturer: Eli Biham
1:00 pm to 2:30 pm	*Lunch*
2:30 pm to 4:00 pm	Cryptanalysis of Hash Functions Lecturer: Eli Biham
4:00 pm to 4:30 pm	*Coffee break*
4:30 pm to 6:00 pm	Cryptanalysis of Triple Modes of Operation and Related-Key Attacks Lecturer: Eli Biham and Orr Dunkelman
6:00 pm	*Bus to hotel and Tel Aviv*

Wednesday, January 29, 2014 – Advanced Symmetric Schemes	
9:00 am to 10:30 am	Tweakable PRP and PRFs, shuffling constructions Lecturer: Thomas Ristenpart
10:30 am to 11:00 am	*Coffee break*
11:00 am to 12:30 pm	Format-preserving encryption and special cases (disk sector encryption) Lecturer: Thomas Ristenpart
12:30 pm to 2:00 pm	*Lunch*
2:00 pm to 3:00 pm	Authenticated encryption (generic composition) Lecturer: Thomas Ristenpart
3:00 pm to 3:30 pm	*Coffee break*
3:30 pm to 4:30 pm	Misuse-resistant AE / deterministic AE Lecturer: Thomas Ristenpart
4:30 pm	*Excursion (Zichron Yaakov)*
8:00 pm	*Dinner*
Thursday, January 30, 2014 – Advanced Attacks	
9:30 am to 11:00 am	Introduction (secure channels, generic composition, basic attacks) Lecturer: Kenny Paterson
11:00 am to 11:30 am	*Coffee break*
11:30 am to 1:00 pm	Symmetric encryption in IPsec and ASP.NET: the perils of unauthenticated encryption Lecturer: Kenny Paterson
1:00 pm to 2:30 pm	*Lunch*
2:30 pm to 4:00 pm	Symmetric encryption in TLS and DTLS: BEAST, Lucky13 and RC4 attacks; security proofs for TLS Lecturer: Kenny Paterson
4:00 pm to 4:30 pm	*Coffee break*
4:30 pm to 6:00 pm	Symmetric encryption in SSH: attacks and new security models for fragmented decryption Lecturer: Kenny Paterson
6:00 pm	*Farewell and bus to hotel*

We thank the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 239868 (LAST), the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n. 609611 (PRACTICE), Bar-Ilan University, and the Check Point Institute for Information Security for their financial support.