



Prime Minister's Office
National Cyber Directorate
National Cyber Bureau



Center for Research in Applied
Cryptography and Cyber Security



The 9th BIU Winter School on Cryptography on Zero Knowledge

School organizers: Yehuda Lindell and Benny Pinkas

Monday, February 18, 2019

Part 1 – Foundations of ZK

8:15 - 8:45	Registration
8:45 - 9:00	Opening remarks
9:00 - 10:00	Alon Rosen: Introduction to Zero Knowledge
10:00 - 10:15	Coffee break
10:15 - 11:15	Alon Rosen: Zero knowledge for all NP
11:15 - 11:45	Coffee break
11:45 - 13:15	Yehuda Lindell: Proofs of knowledge
13:15 - 14:45	Lunch
14:45 - 15:45	Alon Rosen: Constant-round zero-knowledge proofs
15:45 - 16:00	Coffee break
16:00 - 17:00	Alon Rosen: Witness indistinguishability and constant-round arguments
16:30 - 17:00	Coffee break
17:00 - 18:00	Ron Rothblum: Non-interactive zero-knowledge
19:00	Bus to Tel Aviv

Tuesday, February 19, 2019

Part 1 – Foundations of ZK (cont.) & Part 2 - Techniques for efficient ZK

9:00 - 10:00	Ron Rothblum: The Fiat-Shamir transform
10:00 - 10:15	Coffee break
10:15 - 11:45	Alon Rosen: Lower bounds and limitations on zero knowledge
11:45 - 12:15	Coffee break
12:15 - 13:15	Alon Rosen: Non black-box zero knowledge (Barak's protocol)

13:15 – 14:45	Lunch
14:45 – 15:45	Ron Rothblum: New directions and/or advanced topics in the foundations of ZK
15:45 – 16:00	Coffee break
16:00 – 17:00	Benny Pinkas: Sigma protocols (part1)
19:00	Bus to Tel Aviv

Wednesday, February 20, 2019

Part 2 - Techniques for efficient ZK

9:00 – 10:00	Benny Pinkas: Sigma protocols (part2)
10:00– 10:15	Coffee break
10:15 – 11:15	Yuval Ishai: MPC in the head – compilers for ZK: an overview
11:15 – 11:45	Coffee break
11:45 – 12:45	Carmit Hazay: MPC in the head – ZK from MPC: constructions and applications
12:45	Excursion

Thursday, February 21, 2019

Part 2 - Techniques for efficient ZK

9:00 – 10:00	Jens Groth: ZK and NIZK from Bilinear maps (part 1)
10:00 – 10:15	Coffee break
10:15 – 11:15	Jens Groth: ZK and NIZK from Bilinear maps (part 2)
11:15 – 11:45	Coffee break
11:45 – 12:45	Jens Groth: ZK and NIZK from Bilinear maps (part 3)
12:45 – 14:15	Lunch
14:15 – 15:15	Eli Ben-Sasson: Short ZK – SNARKs and STARKs (part 1)
15:15 – 15:30	Coffee break
15:30 – 16:30	Eli Ben-Sasson: Short ZK – SNARKs and STARKs (part 2)
16:30 – 17:00	Coffee break
17:00 – 18:00	Eli Ben-Sasson: Short ZK – SNARKs and STARKs (part 3)
18:00	Farewell

This winter school is graciously sponsored by the BIU Center for Research in Applied Cryptography and Cyber Security in conjunction with the Israel National Cyber Bureau in the Prime Minister's Office, the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013)/ERC Grant Agreement n. 615172 (HIPS) and the Alter family.

