Prime Minister's Office
National Cyber Directorate
National Cyber Bureau

Center for Research in Applied Cryptography and Cyber Security

The 10th BIU Winter School on Information Theoretic Cryptography

School organizers: Benny Applebaum, Carmit Hazay and Benny Pinkas

Monday, February 17, 2020	
Part 1 – PIR + Secret Sharing	
8:15 - 8:45	***Registration***
8:45 - 9:00	Opening remarks
9:00 - 10:00	Benny Applebaum: School Overview
10:00 – 10:15	*Coffee break*
10:15 – 11:15	Gilad Asharov: Threshold Secret Sharing (part 1)
11:15 – 11:30	*Coffee break*
11:30 – 12:30	Gilad Asharov: Threshold Secret Sharing (part 2)
12:30 – 14:00	*Lunch*
14:00 – 15:00	Yuval Ishai: Private Information Retrieval (part 1)
15:00 – 15:15	*Coffee break*
15:15 – 16:15	Yuval Ishai: Private Information Retrieval (part 2)
16:15 – 16:30	*Coffee break*
16:30 – 17:30	Klim Efremenko: Private Information Retrieval (part 3)
19:00	*Bus to Tel Aviv*

Tuesday, February 18, 2020	
Part 2 – Secret Sharing + Consensus	
9:00 – 10:00	Klim Efremenko: Private Information Retrieval (part 4)
10:00 – 10:15	*Coffee break*
10:15 – 11:15	Benny Applebaum: General Secret Sharing + Conditional Disclosure of Secrets (part 1)
11:15 – 11:30	*Coffee break*
11:30 – 12:30	Benny Applebaum: General Secret Sharing + Conditional Disclosure of Secrets (part 2)
12:30 – 14:00	*Lunch*

14:00 – 15:00	Benny Applebaum: General Secret Sharing + Conditional Disclosure of Secrets (part 3)
15:00 – 15:15	*Coffee break*
15:15 – 16:15	Ittai Abraham: Consensus (part 1)
16:15 – 16:30	*Coffee break*
16:30 – 17:30	Ittai Abraham: Consensus (part 2)
19:00	*Bus to Tel Aviv*

Wednesday, February 19, 2020	
Part 3 - Consensus + MPC	
9:00 – 10:00	Ittai Abraham: Consensus (part 3)
10:00– 10:15	*Coffee break*
10:15 – 11:15	Ittai Abraham: Consensus (part 4)
11:15 – 11:45	*Coffee break*
11:45 – 12:45	Yuval Ishai: Introduction to Secure Multi-Party Computation
12:45	*Excursion*

Thursday, February 20, 2020	
Part 4 – MPC	
9:00 – 10:00	Gilad Asharov: Secure Multi-Party Computation (part 1)
10:00 – 10:15	*Coffee break*
10:15 – 11:15	Yuval Ishai: Secure Multi-Party Computation (part 2)
11:15 – 11:30	*Coffee break*
11:30 – 12:30	Yuval Ishai: Secure Multi-Party Computation (part 3)
12:30 – 14:00	*Lunch*
14:00 – 15:00	Niv Gilboa: Fully-Linear PCPs and Their Cryptographic Applications
15:00 – 15:15	*Coffee break*
15:15 – 16:15	Benny Applebaum: Randomized Encoding of Functions and Constant-Round MPC (part 1)
16:15 – 16:30	*Coffee break*
16:30 – 17:30	Benny Applebaum: Randomized Encoding of Functions and Constant-Round MPC (part 2)
17:30	*Farewell*