The 5th BIU Winter School
Advances in Practical Multiparty Computation

School organizers: Yehuda Lindell and Benny Pinkas

Sunday, February 15, 2015 – Tutorials (at Bar-Ilan University)	
9:00 - 9:30	***Registration***
9:30 - 9:35	Opening remarks
9:35 - 11:00	Yehuda Lindell: Definitions and Oblivious Transfer
11:00 - 11:30	*Coffee break*
11:30 - 13:00	Benny Pinkas: Yao's Two-Party Protocol and the BMR Multi-Party Protocol
13:00 - 14:30	*Lunch*
14:30 - 15:30	Benny Pinkas: The GMW Multi-Party Protocols and Oblivious Transfer Extension
15:30 – 15:50	*Coffee break*
15:50 – 16:50	Yehuda Lindell: Efficient Zero-Knowledge
16:50 – 17:10	*Coffee break*
17:10 – 18:10	Yehuda Lindell: Security against Malicious Adversaries
18:10	*Bus to hotel and Tel Aviv*

Monday, February 16, 2015 – Practical 2PC Based on Yao's Protocol	
9:30 – 11:00	Thomas Schneider: Optimizing Yao and GMW for Semi-Honest Adversaries
11:00 – 11:30	*Coffee break*
11:30 – 13:00	abhi shelat: Security for Malicious Adversaries with Yao's Protocol – Part 1
13:00 – 14:30	*Lunch*
14:30 – 16:00	abhi shelat: Security for Malicious Adversaries with Yao's Protocol – Part 2
16:00 – 16:30	*Coffee break*
16:30 – 17:30	abhi shelat: Implementation Issues and Optimizations
19:00	*Bus to Tel Aviv*
Tuesday, February 17, 2015 – The TinyOT Protocol	
9:30 – 11:00	Claudio Orlandi: The TinyOT Protocol – Part 1
11:00 – 11:30	*Coffee break*
11:30 – 13:00	Claudio Orlandi: The TinyOT Protocol – Part 2
13:00	*Lunch, Excursion and Dinner*
Wednesday, February 18, 2015 – SPDZ and Specific Protocols	
9:00 – 10:30	Ivan Damgård: The SPDZ Protocol – Part 1
10:30 – 11:00	*Coffee break*
11:00 – 12:30	Ivan Damgård: The SPDZ Protocol – Part 2
12:30 – 14:00	*Lunch*
14:00 – 15:30	Benny Pinkas: ORAM
15:30 – 16:00	*Coffee Break*
16:00 – 17:30	Benny Pinkas: Set Intersection
19:00	*Bus to Tel Aviv*

Thursday, February 19, 2015 – Workshop: New Results in Practical MPC	
9:30 – 11:00	Ivan Damgård**:** UC Secure Commitments with Optimal Amortized Overhead Gilad Asharov: More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries Elette Boyle: Large-Scale Secure Computation: MPC for Parallel RAM Programs
11:00 – 11:30	*Coffee break*
11:30 – 13:00	Muthuramakrishnan Venkitasubramaniam: Rethinking for Secure Computation – A Greedy Approach Carmit Hazay: Oblivious Polynomial Evaluation and Secure Set-Intersection from Algebraic PRFs Christian Rechberger: Ciphers for MPC and FHE
13:00 – 14:30	*Lunch*
14:30 – 16:00	Yehuda Lindell: A Tutorial on SCAPI Marcel Keller: How to Implement Anything in MPC Michael Zohner: ABY – A Framework for Efficient Mixed-Protocol Secure Two-Party Computation
16:00 – 16:30	*Coffee break*
16:30 – 17:30	Ben Riva: New Consistency Checks and Implementing Online/Offline Yao Claudio Orlandi: Privacy-Free Garbled Circuits with Applications To Efficient Zero-Knowledge
17:30	*Farewell*