

GTACS – Bar-Ilan University

November 23, 2016

LOCATION Chemistry building (no. 211), room no. 112

PROGRAM

09:00-09:30 Coffee & Registration

09:30-10:30 **Niv Gilboa**, *Function Secret Sharing: Improvements and Extensions*

10:30-11:00 Coffee break

11:00-11:30 **Ariel Nof**, *High-Throughput Secure Three-Party Computation with an Honest Majority*

11:30-12:00 **Carsten Baum**, *Efficient Commitments and Zero-Knowledge Protocols from Ring-SIS with Applications to Lattice-based Threshold Cryptosystems*

12:00-13:30 Lunch

13:30-14:30 **Nathan Keller**, *Memory-Efficient Algorithms for Finding Needles in Haystacks*

14:30-15:00 Coffee break

15:00-16:00 **Moni Naor**, *Grand Challenges in Cryptography – Discussion Session*