

TCC 2019 Rump Session Program

18.00	Opening	Lisa Kohl
18.03	Privately Learning Thresholds: Closing the Exponential Gap	Moni Naor Haim Kaplan Katrina Ligett Yishay Mansour Uri Stemmer
18.10	Generalizations of Balogh et al.'s Private PEZ Protocol	Mitsugu Iwamoto Yoshiki Abe Kazua Ohta
18.15	State Separation for Simulation-Based Proofs	Chris Brzuska Sabine Oechsner
18.22	Hairy Graphs	Lukas Zobernig
18.27	Broadcast-Optimal Two-Round MPC	Ran Cohen Juan Garay Vassilis Zikas
18.32	Groups with Infeasible Inversion from Isogeny Volcanoes	Yilei Chen Salim Ali Altuğ
18.37	On the Complexity of Decomposing Perfect Randomized Encodings, or: How Friendly Can a Garbling Friendly PRF be?	Marshall Ball Justin Holmgren Yuval Ishai Tianren Liu Tal Malkin
