# TPMPC 2019 Program

## Monday 17 June

**8:15 Registration opens**

9:25 Welcome – Yehuda Lindell

Session chair – Yehuda Lindell

9:30 Invited talk: Tal Malkin - Garbled Neural Networks are Practical

10:20 Liina Kamm: Applying MPC for Genotype Analysis While Considering Population Stratification

**10:45 Coffee**

Session chair – Carmit Hazay

11:15 Thomas Attema: Secure multiparty PageRank algorithm for collaborative fraud detection

11:40 Invited talk: Marina Blanton - Efficient building blocks for secure computation based on secret sharing

**12:30 Lunch**

Session chair – Benny Pinkas

14:00 Invited talk (replacement): Yehuda Lindell - Two-Thirds Honest-Majority MPC for Malicious Adversaries at Almost the Cost of Semi-Honest

14:50 Tamer Mour: Trapdoor Hash Functions and Applications: Rate-1 OT and More

15:15 Samuel Ranellucci: Reducing the Memory Overhead of Garbled Circuits

**15:40 Coffee**

Session chair – Carsten Baum

16:10 Avishay Yanai: SpOT-Light: Lightweight Private Set Intersection from Sparse OT Extension

16:35 Peter Scholl: MPC with Silent Preprocessing (or: Two-Round OT Extension from LPN)

17:00 Daniel Masny: Two-Round Oblivious Transfer from CDH or LPN

**17:25 End of day**

## Tuesday 18 June

Session chair – Yehuda Lindell

9:30 Invited talk: Ran Canetti - Fully Deniable Encryption and Multiparty Computation

10:20 Frank Blom: Efficient Secure Ridge Regression from Randomized Gaussian Elimination

**10:45 Coffee**

Session chair – Ariel Nof

11:15 Irene Giacomelli: MonZa: Fast Maliciously-Secure Two-Party Computation on the ring $\mathbb{Z}_2^k$

11:40 Invited talk: Marcella Hastings - Lessons from a survey of general-purpose frameworks for secure multi-party computation

**12:30 Lunch**

Session chair – Carmit Hazay

14:00 Invited talk: Ivan Damgård - Communication Lower Bounds for Statistically Secure MPC, with or without Preprocessing

14:50 abhi shelat: Adaptively Secure MPC with Sublinear Communication Complexity

**15:15 Coffee**

Session chair – Avishay Yanai

15:45 Chen-Da Liu-Zhang: Robust MPC: Asynchronous Responsiveness yet Synchronous Security

16:10 Aarushi Goel: Two Round Information-Theoretic MPC with Malicious Security

16:35 Daniel Escudero: New Primitives for Actively-Secure MPC over Rings with Applications to Private Machine Learning

**17:00 Break and Beer**

**18:00 Workshop dinner**

## Wednesday 19 June

Session chair – Rafael Dowsley

9:30 Invited talk: Shai Halevi - Compressible FHE with Applications to PIR

10:20 Emmanuela Orsini: Overdrive2k: Efficient Secure MPC over $\mathbb{Z}_2^k$ from Somewhat Homomorphic Encryption

**10:45 Coffee**

Session chair – Carsten Baum

11:15 Dragos Rotaru: MArBled Circuits: Mixing Arithmetic and Boolean Circuits with Active Security

11:40 Invited talk: Elette Boyle – Beaver Meets FSS: Secure Computation with Preprocessing via Function Secret Sharing

**12:30 Lunch**

Session chair – Benny Pinkas

14:00 Invited talk: Thomas Schneider - Private Function Evaluation - From Functions to Data to Code

14:50 James Bell: The Privacy Blanket of the Shuffle Model

**15:15 Coffee**

Session chair – Tore Frederiksen

15:45 Vlad Kolesnikov: Covert Security with Public Verifiability: Faster, Leaner, and Simpler

16:10 Daniel Tschudi: Overview on Topology-Hiding Computation

16:35 Rafael Dowsley: Efficient UC Commitment Extension with Homomorphism for Free (and Applications)

**17:00 Break**

Rump session chair – Carmit Hazay

17:30 Rump Session part 1

**18:30 Dinner**

19:00 Rump session part 2

**20:00 Dessert**

## Thursday 20 June

Session chair – Yehuda Lindell

9:30 Invited talk: Arpita Patra - The Round Complexity Landscape of Secure Computation

10:20 Ariel Nof: Concretely-Efficient Zero-Knowledge Arguments for Arithmetic Circuits and Their Application to Lattice-Based Cryptography

**10:45 Coffee**

Session chair – Benny Pinkas

11:15 Daniele Cozzo: Using TopGear in Overdrive: A more efficient ZKPoK for SPDZ

11:40 Sabine Oechsner: On Writing and Reading MPC Security Proofs: An Explorational Study of State Separation

12:05 Hayim Shaul: Secure Data Retrieval on the Cloud: Homomorphic Encryption meets Coresets

**12:30 Lunch**

Session chair – Carsten Baum

14:00 Max Leibovich: Setup-Free Secure Search on Encrypted Data: Faster and Post-Processing Free

14:25 Phillipp Schoppmann: Make Some ROOM for the Zeros: Data Sparsity in Secure Distributed Machine Learning

14:50 Sophia Yakoubov: Turning HATE Into LOVE: Homomorphic Ad Hoc Threshold Encryption for Scalable MPC

15:15 Kris Shrishak: Transputation: Transport Framework for Secure Computation

**15:40 End of workshop - See you next year!**