11:30–12:30 Invited Talk I  
Block Ciphers: From Practice back to Theory  
John P. Steinberger  
(chair: Yevgeniy Dodis)

12:30–14:00 Lunch (provided)  
Multiparty Computation  
(chair: Martin Hirt)

14:40–15:00 Ben Fisch, Daniel Freund, Moni Naor: Secure Physical Computation using Disposable Circuits  
15:00–15:20 Gilad Asharov, Marno Beimel, Nikolaos Makriyannis, Eran Omri: Complete Characterization of Fairness in Secure Two-Party Computation of Boolean Functions  
15:20–15:40 Vladimir Kolesnikov, Payman Mohassel, Ben Riva, Mike Rosulek: Richer Efficiency/Security Trade-offs in 2PC  
15:40–16:10 Coffee Break  
Concurrent and Resettable Security  
(chair: Yuval Ishai)

16:10–16:30 Vipul Goyal, Huihua Lin, Omkant Pandey, Rafael Pass, Amit Sahai: Round-Efficient Concurrently Composable Secure Computation via a Robust Extraction Lemma  
16:30–16:50 Susumu Kiyoshima: An Alternative Approach to Non-black-box Simulation in Fully Concurrent Setting  
16:50–17:10 Nico Döttling, Daniel Kraschewski, Jörn Müller-Quade, Tobias Nilges: General Statistically Secure Computation with Bounded-Resettable Hardware Tokens  
17:10–17:30 Rafael Ostrovsky, Alessandra Scafuro, Muthuramakrishnan Venkitasubramaniam: Resettable Sound Zero-Knowledge Arguments from OWFs — the (semi) Black-Box way

Tuesday, March 24

9:00–9:20 Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, Manoj Prabhakaran: A Rate-Optimizing Compiler for Non-malleable Codes Against Bit-wise Tampering and Permutations  
9:20–9:40 Divesh Aggarwal, Stefan Dziembowski, Tomasz Kazana, Maciej Obrenski: Leakage-resilient non-malleable codes  
9:40–10:00 Dana Dachman-Soled, Feng-Hao Liu, Elaine Shi, Hong-Sheng Zhou: Locally Decodable and Updatable Non-Malleable Codes and Their Applications  
10:00–10:20 Zahir Jafargholi, Daniel Wichs: Tamper Detection and Continuous Non-Malleable Codes  
10:20–10:40 Ronald Cramer, Carles Padro, Xiaoping Xing: Optimal Algebraic Manipulation Detection Codes in the Constant-Error Model  
10:40–11:10 Coffee Break  
Privacy Amplification  
(chair: Yevgeniy Dodis)

11:10–11:30 Xin Li: Non-Malleable Condensers for Arbitrary Min-Entropy, and Almost Optimal Protocols for Privacy Amplification  
11:30–12:30 Invited Talk II  
Wyn’s Wire-Tap Channel, Forty Years Later  
Leonid Reyzin  
(chair: Yevgeniy Dodis)

12:30–14:00 Lunch (provided)  
Encryption and Key Exchange  
(chair: Stefano Tessaro)

14:00–14:20 Sandro Coretti, Ueli Maurer, Björn Tackmann, Daniele Venturi: From Single-Bit to Multi-Bit Public-Key Encryption via Non-Malleable Codes
Wednesday, March 25

Proofs and Verifiable Computation
(chair: Carmit Hazay)

9:20–9:40 Giulia Alberini, Tal Moran, Alon Rosen: Public Verification of Private Effort
9:40–10:00 Moni Naor, Asaf Ziv: Primary-Secondary-Resolver Membership Proof Systems
10:00–10:20 Kai-Min Chung, Rafael Pass: Tight Parallel Repetition Theorems for Public-Coin Arguments using KL-divergence
10:40–11:10 Coffee Break

Differential Privacy
(chair: Omer Paneth)

11:10–11:30 Edward Lui, Rafael Pass: Outlier Privacy

Functional Encryption
(chair: Omer Paneth)

11:30–11:50 Zvika Brakerski, Gil Segev: Function-Private Functional Encryption in the Private-Key Setting
12:10–12:30 Ilan Komargodski, Gil Segev, Eylon Yogev: Functional Encryption for Randomized Functionalities in the Private-Key Setting from Minimal Assumptions
12:30–14:00 Lunch (provided)