Warsaw Center of Mathematics and Computer Science

Google

Theory of Cryptography Conference 2015

Warsaw, Poland

PROGRAM

Sunday, March 22

17:00–19:00 Welcome Reception

Monday, March 23

8:15-8:45 Registration

8:45-9:00 Opening Remarks

Foundations
(chair: Mohammad Mahmoody)

9:00–9:20 Andrej Bogdanov, Christina Brzuska: *On Basing Size-Verifiable One-Way Functions on NP-Hardness*

9:20–9:40 Yu Yu, Dawu Gu, Xiangxue Li, Jian Weng: *The Randomized Iterate Revisited - Almost Linear Seed Length PRGs from A Broader Class of One-way Functions*

9:40–10:00 Siyao Guo, Tal Malkin, Igor C. Oliveira, Alon Rosen: *The Power of Negations in Cryptography*

10:00–10:20 Kai-Min Chung, Edward Lui, Rafael Pass: *From Weak to Strong Zero-Knowledge and Applications*

10:20–10:40 Yehuda Lindell: *An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-Programmable Random Oracle*

10:40–11:10 Coffee Break

Symmetric Key Cryptography
(chair: Yevgeniy Dodis)

11:10–11:30 Chun Guo, Dongdai Lin: *On the Indifferentiability of Key-Alternating Feistel Ciphers with No Key Derivation*

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)

14:00–14:20 Juan Garay, Ran Gelles, David Johnson, Aggelos Kiayias, Moti Yung: *A Little Honesty Goes a Long Way: The Two-Tier Model for Secure Multiparty Computation*

14:20–14:40 Tal Moran, Ilan Orlov, Silas Richelson: *Topology-Hiding Computation*

14:40–15:00 Ben Fisch, Daniel Freund, Moni Naor: *Secure Physical Computation using Disposable Circuits*

15:00–15:20 Gilad Asharov, Amos 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, Huijia 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 Rafail Ostrovsky, Alessandra Scafuro, Muthuramakrishnan Venkitasubramaniam: *Resettably Sound Zero-Knoweldge Arguments from OWFs — the (semi) Black-Box way*

Tuesday, March 24

Non-malleable Codes and Tampering
(chair: Nico Döttling)

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 Obremski: *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 Zahra Jafargholi, Daniel Wichs: *Tamper Detection and Continuous Non-Malleable Codes*

10:20–10:40 Ronald Cramer, Carles Padro, Chaoping 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
Wyner'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*

14:20–14:40 Takahiro Matsuda, Goichiro Hanaoka: *Constructing and Understanding Chosen Ciphertext Security via Puncturable Key Encapsulation Mechanisms*

14:40–15:00 Brett Hemenway, Rafail Ostrovsky, Alon Rosen: *Non-committing encryption from Phi-hiding*

15:00–15:20 Adam Smith, Ye Zhang: *On the Regularity of Lossy RSA: Improved Bounds and Applications to Padding-Based Encryption*

15:20–15:40 Christoph Bader, Dennis Hofheinz, Tibor Jager, Eike Kiltz, Yong Li: *Tightly-Secure Authenticated Key Exchange*

15:40–16:10 Coffee Break

Pseudorandom Functions and Applications
(chair: Benny Applebaum)

16:10–16:35 Zvika Brakerski, Vinod Vaikuntanathan: *Constrained Key-Homomorphic PRFs from LWE (Or) How to Secretly Embed a Circuit in Your PRF*

Abhishek Banerjee, Georg Fuchsbauer, Chris Peikert, Krzysztof Pietrzak, Sophie Stevens: *Key-Homomorphic Constrained Pseudorandom Functions*

16:35–16:55 Aloni Cohen, Shafi Goldwasser, Vinod Vaikuntanathan: *Aggregate Pseudorandom Functions and Connections to Learning*

16:55–17:15 Carmit Hazay: *Oblivious Polynomial Evaluation and Secure Set-Intersection from Algebraic PRFs*

17:15–17:35 Tibor Jager: *Verifiable Random Functions from Weaker Assumptions*

17:35–19:00 Break

Cocktail (Food and Drinks)

19:00–19:30 Business Meeting and Test of Time Award

19:30–21:30 Rump Session (chair: Krzysztof Pietrzak)

Wednesday, March 25

Proofs and Verifiable Computation
(chair: Carmit Hazay)

9:00–9:20 S. Dov Gordon, Jonathan Katz, Feng-Hao Liu, Elaine Shi, Hong-Sheng Zhou: *Multi-Client Verifiable Computation with Stronger Security Guarantees*

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*

10:20–10:40 Carla Ràfols: *Stretching Groth-Sahai: NIZK Proofs of Partial Satisfiability*

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*

11:50–12:10 Vipul Goyal, Abhishek Jain, Venkata Koppula, Amit Sahai: *Functional Encryption for Randomized Functionalities*

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)

Obfuscation I
(chair: Shai Halevi)

14:00–14:20 Venkata Koppula, Kim Ramchen, Brent Waters: *Separations in Circular Security for Arbitrary Length Key Cycles*

14:20–14:40 Nir Bitansky, Omer Paneth: *ZAPs and Non-Interactive Witness Indistinguishability from Indistinguishability Obfuscation*

14:40–15:00 Christina Brzuska, Pooya Farshim, Arno Mittelbach: *Random-Oracle Uninstantiability from Indistinguishability Obfuscation*

15:00–15:20 Ran Canetti, Yael Tauman Kalai, Omer Paneth: *On Obfuscation with Random Oracles*

15:20–15:40 Ran Canetti, Huijia Lin, Stefano Tessaro, Vinod Vaikuntanathan: *Obfuscation of Probabilistic Circuits and Applications*

15:40–16:10 Coffee Break

Obfuscation II
(chair: Nir Bitansky)

16:10–16:30 Craig Gentry, Sergey Gorbunov, Shai Halevi: *Graph-Induced Multilinear Maps from Lattices*

16:30–16:50 Benny Applebaum, Zvika Brakerski: *Obfuscating Circuits via Composite-Order Graded Encoding*

16:50–17:15
Ran Canetti, Shafi Goldwasser, Oxana Poburinnaya: *Adaptively Secure Two-party Computation From Indistinguishability Obfuscation*

Dana Dachman-Soled, Jonathan Katz, Vanishree Rao: *Adaptively Secure, Universally Composable, Multi-Party Computation in Constant Rounds*

Sanjam Garg, Antigoni Polychroniadou *Two-Round Adaptively Secure MPC from Indistinguishability Obfuscation*

17:15–17:40 Omkant Pandey, Manoj Prabhakaran, Amit Sahai: *Obfuscation-based Non-black-box Simulation and Four Message Concurrent Zero Knowledge for NP*

Yuval Ishai, Omkant Pandey, Amit Sahai *Public Coin Differing-Inputs Obfuscation and Its Applications*