2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS 2018)

Paris, France
7-9 October 2018

Pages 1-496

IEEE Catalog Number: CFP18053-POD
ISBN: 978-1-5386-4231-3

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP18053-POD
ISBN (Print-On-Demand):	978-1-5386-4231-3
ISBN (Online):	978-1-5386-4230-6
ISSN:	1523-8288

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

2018 IEEE 59th Annual Symposium on Foundations of Computer Science

FOCS 2018

Table of Contents

FOCS 2018 Preface ..... **xv**
FOCS 2018 Organizing Committee and Sponsors ..... **xvi**
FOCS 2018 Program Committee ..... **xvii**
FOCS 2018 External Reviewers ..... **xviii**
FOCS 2018 Awards ..... **xxii**

Session 1.1.A

Balancing Vectors in Any Norm 1
Daniel Dadush (Centrum Wiskunde & Informatica), Aleksandar Nikolov (University of Toronto), Kunal Talwar (Google Brain), and Nicole Tomczak-Jaegermann (University of Alberta)

Metric Sublinear Algorithms via Linear Sampling 11
Hossein Esfandiari (Google Research) and Michael Mitzenmacher (Harvard University)

Approximating the Permanent of a Random Matrix with Vanishing Mean 23
Lior Eldar (N/A) and Saeed Mehraban (Massachusetts Institute of Technology)

Log-Concave Polynomials, Entropy, and a Deterministic Approximation Algorithm for Counting Bases of Matroids 35
Nima Anari (Stanford University), Shayan Oveis Gharan (University of Washington), and Cynthia Vinzant (North Carolina State University)

Session 1.1.B

A Short List of Equalities Induces Large Sign Rank 47
Arkadev Chattopadhyay (Tata Institute of Fundamental Research) and Nikhil Mande (Tata Institute of Fundamental Research)

Simple Optimal Hitting Sets for Small-Success RL 59
William Hoza (University of Texas at Austin) and David Zuckerman (University of Texas at Austin)

Hardness Magnification for Natural Problems 65
Igor Carboni Oliveira (University of Oxford) and Rahul Santhanam (University of Oxford)

Counting t-Cliques: Worst-Case to Average-Case Reductions and Direct Interactive Proof Systems 77
Oded Goldreich (Weizmann Institute of Science) and Guy Rothblum (Weizmann Institute of Science)

Session 1.2.A

A Faster Isomorphism Test for Graphs of Small Degree 89
Martin Grohe (RWTH Aachen University), Daniel Neuen (RWTH Aachen University), and Pascal Schweitzer (TU Kaiserslautern)

Graph Sketching against Adaptive Adversaries Applied to the Minimum Degree Algorithm 101
Matthew Fahrbach (Georgia Institute of Technology), Gary L. Miller (Carnegie Mellon University), Richard Peng (Georgia Institute of Technology), Saurabh Sawlani (Georgia Institute of Technology), Junxing Wang (Carnegie Mellon University), and Shen Chen Xu (Facebook)

Faster Exact and Approximate Algorithms for k-Cut 113
Anupam Gupta (Carnegie Mellon University), Euiwoong Lee (New York University), and Jason Li (Carnegie Mellon University)

Session 1.2.B

Delegating Computations with (Almost) Minimal Time and Space Overhead 124
Justin Holmgren (Massachusetts Institute of Technology) and Ron Rothblum (Massachusetts Institute of Technology and Northeastern University)

Computational Two-Party Correlation: A Dichotomy for Key-Agreement Protocols 136
Iftach Haitner (Tel Aviv University), Kobbi Nissim (Georgetown University), Eran Omri (Ariel University), Ronen Shaltiel (University of Haifa), and Jad Silbak (Tel Aviv University)

PPP-Completeness with Connections to Cryptography 148
Katerina Sotiraki (Massachusetts Institute of Technology), Manolis Zampetakis (Massachusetts Institute of Technology), and Giorgos Zirdelis (Northeastern University)

Session 1.3.A

Hölder Homeomorphisms and Approximate Nearest Neighbors 159
Alexandr Andoni (Columbia University), Assaf Naor (Princeton University), Aleksandar Nikolov (University of Toronto), Ilya Razenshteyn (Microsoft Research), and Erik Waingarten (Columbia University)

Near-Optimal Approximate Decremental All Pairs Shortest Paths 170
Shiri Chechik (Tel-Aviv University)

Bloom Filters, Adaptivity, and the Dictionary Problem 182
Michael A. Bender (Stony Brook University), Martin Farach-Colton (Rutgers University), Mayank Goswami (Queens College, CUNY), Rob Johnson (VMware Research), Samuel McCauley (Wellesley College), and Shikha Singh (Wellesley College)

Session 1.3.B

MDS Matrices over Small Fields: A Proof of the GM-MDS Conjecture 194
Shachar Lovett (University of California San Diego)

Deterministic Document Exchange Protocols, and Almost Optimal Binary Codes for Edit Errors..... 200
Kuan Cheng (Johns Hopkins University), Zhengzhong Jin (Johns Hopkins University), Xin Li (Johns Hopkins University), and Ke Wu (Johns Hopkins University)

Improved Decoding of Folded Reed-Solomon and Multiplicity Codes 212
Swastik Kopparty (Rutgers University), Noga Ron-Zewi (University of Haifa), Shubhangi Saraf (Rutgers University), and Mary Wootters (Stanford University)

Session 1.4.A

An Improved Bound for Weak Epsilon-Nets in the Plane 224
Natan Rubin (Ben-Gurion University of the Negev)

Session 1.4.B

The Complexity of General-Valued CSPs Seen from the Other Side 236
Clément Carbonnel (University of Oxford), Miguel Romero (University of Oxford), and Stanislav Živný (University of Oxford)

Session 1.5

Non-Black-Box Worst-Case to Average-Case Reductions within NP 247
Shuichi Hirahara (University of Tokyo)

Classical Verification of Quantum Computations 259
Urmila Mahadev (University of California, Berkeley)

Session 2.1.A

Contextual Search via Intrinsic Volumes 268
Renato Paes Leme (Google Research) and Jon Schneider (Princeton University)

Towards Learning Sparsely Used Dictionaries with Arbitrary Supports 283
Pranjal Awasthi (Rutgers University) and Aravindan Vijayaraghavan (Northwestern University)

Learning Sums of Independent Random Variables with Sparse Collective Support 297
Anindya De (Northwestern University), Philip M. Long (Google), and Rocco A. Servedio (Columbia University)

Recharging Bandits 309
Robert Kleinberg (Cornell University) and Nicole Immorlica (Microsoft Research)

Session 2.1.B

A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device 320
Zvika Brakerski (Weizmann Institute), Paul Christiano (Open AI), Urmila Mahadev (University of California, Berkeley), Umesh Vazirani (University of California, Berkeley), and Thomas Vidick (California Institute of Technology)

Classical Homomorphic Encryption for Quantum Circuits 332
Urmila Mahadev (University of California, Berkeley)

Classical Lower Bounds from Quantum Upper Bounds 339
Shalev Ben-David (University of Waterloo), Adam Bouland (University of California, Berkeley), Ankit Garg (Microsoft Research), and Robin Kothari (Microsoft Research)

Quantum Algorithm for Simulating Real Time Evolution of Lattice Hamiltonians 350
Jeongwan Haah (Microsoft Research), Matthew Hastings (Microsoft Research), Robin Kothari (Microsoft Research), and Guang Hao Low (Microsoft Research)

Session 2.2.A

Graph Sparsification, Spectral Sketches, and Faster Resistance Computation, via Short Cycle Decompositions 361
Timothy Chu (Carnegie Mellon University), Yu Gao (Georgia Institute of Technology), Richard Peng (Georgia Institute of Technology), Sushant Sachdeva (University of Toronto), Saurabh Sawlani (Georgia Institute of Technology), and Junxing Wang (Carnegie Mellon University)

A Matrix Chernoff Bound for Strongly Rayleigh Distributions and Spectral Sparsifiers from a few Random Spanning Trees 373
Rasmus Kyng (Harvard University) and Zhao Song (Harvard University)

Spectral Subspace Sparsification 385
Huan Li (Fudan University) and Aaron Schild (University of California, Berkeley)

Session 2.2.B

Near-Optimal Communication Lower Bounds for Approximate Nash Equilibria 397
Mika Göös (Harvard University) and Aviad Rubinstein (Harvard University)

An End-to-End Argument in Mechanism Design (Prior-Independent Auctions for Budgeted Agents) 404
Yiding Feng (Northwestern University) and Jason D. Hartline (Northwestern University)

The Sample Complexity of Up-to- Multi-Dimensional Revenue Maximization 416
Yannai A. Gonczarowski (Hebrew University of Jerusalem and Microsoft Research) and S. Matthew Weinberg (Princeton University)

Session 2.3.A

Improved Online Algorithm for Weighted Flow Time 427
Yossi Azar (Tel Aviv University) and Noam Touitou (Tel Aviv University)

Fusible HSTs and the Randomized k-Server Conjecture 438
James R. Lee (University of Washington)

An ETH-Tight Exact Algorithm for Euclidean TSP 450
Mark de Berg (Eindhoven University of Technology), Hans L. Bodlaender (Eindhoven University of Technology and Utrecht University), Sándor Kisfaludi-Bak (Eindhoven University of Technology), and Sudeshna Kolay (Eindhoven University of Technology)

0/1/All CSPs, Half-Integral A-Path Packing, and Linear-Time FPT Algorithms 462
Yoichi Iwata (National Institute of Informatics), Yutaro Yamaguchi (Osaka University), and Yuichi Yoshida (National Institute of Informatics)

On Subexponential Parameterized Algorithms for Steiner Tree and Directed Subset TSP on Planar Graphs 474
Dániel Marx (Hungarian Academy of Sciences), Marcin Pilipczuk (University of Warsaw), and Michał Pilipczuk (University of Warsaw)

Session 2.3.B

Deterministic Factorization of Sparse Polynomials with Bounded Individual Degree 485
Vishwas Bhargava (Rutgers University), Shubhangi Saraf (Rutgers University), and Ilya Volkovich (University of Michigan, Ann Arbor)

Testing Graph Clusterability: Algorithms and Lower Bounds 497
Ashish Chiplunkar (EPFL), Michael Kapralov (EPFL), Sanjeev Khanna (University of Pennsylvania), Aida Mousavifar (EPFL), and Yuval Peres (Microsoft Research)

Finding Forbidden Minors in Sublinear Time: A n^1/2+o(1)-Query One-Sided Tester for Minor Closed Properties on Bounded Degree Graphs 509
Akash Kumar (Purdue University), C. Seshadhri (University of California, Santa Cruz), and Andrew Stolman (University of California, Santa Cruz)

Privacy Amplification by Iteration 521
Vitaly Feldman (Google), Ilya Mironov (Google), Kunal Talwar (Google), and Abhradeep Thakurta (University of California, Santa Cruz and Google)

Revealing Network Structure, Confidentially: Improved Rates for Node-Private Graphon Estimation 533
Christian Borgs (Microsoft Research), Jennifer Chayes (Microsoft Research), Adam Smith (Boston University), and Ilias Zadik (Massachusetts Institute of Technology)

Session 2.4.A

Perfect Lp Sampling in a Data Stream 544
Rajesh Jayaram (Carnegie Mellon University) and David P. Woodruff (Carnegie Mellon University)

The Sketching Complexity of Graph and Hypergraph Counting 556
John Kallaugher (University of Texas at Austin), Michael Kapralov (École Polytechnique Fédérale de Lausanne), and Eric Price (University of Texas at Austin)

Session 2.4.B

EPTAS for Max Clique on Disks and Unit Balls 568
Marthe Bonamy (Université de Bordeaux), Édouard Bonnet (Université de Lyon and Université Claude-Bernard), Nicolas Bousquet (CNRS, G-SCOP Laboratory, Grenoble-INP), Pierre Charbit (Université Paris Diderot - IRIF), and Stéphan Thomassé (Université de Lyon and Université Claude-Bernard)

Limits on All Known (and Some Unknown) Approaches to Matrix Multiplication 580
Josh Alman (Massachusetts Institute of Technology) and Virginia Vassilevska Williams (Massachusetts Institute of Technology)

Session 2.5

Pseudorandom Sets in Grassmann Graph Have Near-Perfect Expansion 592
Khot Subhash (New York University), Dor Minzer (Tel Aviv University), and Muli Safra (Tel Aviv University)

Session 2.6

Knuth Prize Lecture: On the Difficulty of Approximating Boolean Max-CSPs 602
Johan Håstad (Royal Institute of Technology)

Session 3.1.A

Dispersion for Data-Driven Algorithm Design, Online Learning, and Private Optimization 603
Maria-Florina Balcan (Carnegie Mellon University), Travis Dick (Carnegie Mellon University), and Ellen Vitercik (Carnegie Mellon University)

Efficient Density Evaluation for Smooth Kernels 615
Arturs Backurs (Massachusetts Institute of Technology), Moses Charikar (Stanford University), Piotr Indyk (Massachusetts Institute of Technology), and Paris Siminelakis (Stanford University)

Efficiently Learning Mixtures of Mallows Models 627
Allen Liu (Massachusetts Institute of Technology) and Ankur Moitra (Massachusetts Institute of Technology)

Efficient Statistics, in High Dimensions, from Truncated Samples 639
Constantinos Daskalakis (Massachusetts Institute of Technology), Themis Gouleakis (Massachusetts Institute of Technology), Chistos Tzamos (University of Wisconsin-Madison), and Manolis Zampetakis (Massachusetts Institute of Technology)

Session 3.1.B

Planar Graph Perfect Matching Is in NC 650
Nima Anari (Stanford University) and Vijay V. Vazirani (University of California, Irvine)

On Derandomizing Local Distributed Algorithms 662
Mohsen Ghaffari (ETH Zurich), David G. Harris (University of Maryland, College Park), and Fabian Kuhn (University of Freiburg)

Parallel Graph Connectivity in Log Diameter Rounds 674
Alexandr Andoni (Columbia University), Zhao Song (Harvard University), Clifford Stein (Columbia University), Zhengyu Wang (Harvard University), and Peilin Zhong (Columbia University)

A Faster Distributed Single-Source Shortest Paths Algorithm 686
Sebastian Forster (University of Salzburg) and Danupon Nanongkai (KTH Royal Institute of Technology)

Session 3.2.A

1-Factorizations of Pseudorandom Graphs 698
Asaf Ferber (Massachusetts Institute of Technology) and Vishesh Jain (Massachusetts Institute of Technology)

Sublinear Algorithms for Local Graph Centrality Estimation 709
Marco Bressan (Sapienza Università di Roma), Enoch Peserico (Università degli Studi di Padova), and Luca Pretto (Università degli Studi di Padova)

Efficient Polynomial-Time Approximation Scheme for the Genus of Dense Graphs 719
Bojan Mohar (Simon Fraser University) and Yifan Jing (Simon Fraser University)

Session 3.2.B

Low-Degree Testing for Quantum States, and a Quantum Entangled Games PCP for QMA 731
Anand Natarajan (Massachusetts Institute of Technology) and Thomas Vidick (California Institute of Technology)

Constant Overhead Quantum Fault-Tolerance with Quantum Expander Codes 743
Omar Fawzi (Universite de Lyon), Antoine Grospellier (Inria), and Anthony Leverrier (Inria)

Spatial Isolation Implies Zero Knowledge Even in a Quantum World 755
Alessandro Chiesa (University of California, Berkeley), Michael Forbes (University of Illinois at Urbana–Champaign), Tom Gur (University of California, Berkeley), and Nicholas Spooner (University of California, Berkeley)

Session 3.3.A

Beating the Integrality Ratio for s-t-Tours in Graphs 766
Vera Traub (University of Bonn) and Jens Vygen (University of Bonn)

Constant Factor Approximation Algorithm for Weighted Flow Time on a Single Machine in Pseudo-Polynomial Time 778
Jatin Batra (IIT Delhi), Naveen Garg (IIT Delhi), and Amit Kumar (IIT Delhi)

Random Order Contention Resolution Schemes 790
Marek Adamczyk (University of Warsaw) and Michał Włodarczyk (University of Warsaw)

Strong Coresets for k-Median and Subspace Approximation: Goodbye Dimension 802
Christian Sohler (TU Dortmund) and David P. Woodruff (Carnegie Mellon University)

Epsilon-Coresets for Clustering (with Outliers) in Doubling Metrics 814
Lingxiao Huang (École Polytechnique Fédérale de Lausanne), Shaofeng Jiang (Weizmann Institute of Science), Jian Li (Tsinghua University), and Xuan Wu (Tsinghua University)

Session 3.3.B

Non-Malleable Codes for Small-Depth Circuits 826
Marshall Ball (Columbia University and IDC Herzliya), Dana Dachman-Soled (University of Maryland), Siyao Guo (Northeastern University), Tal Malkin (Columbia University), and Li-Yang Tan (Stanford University)

Tighter Bounds on Multi-Party Coin Flipping via Augmented Weak Martingales and Differentially Private Sampling 838
Amos Beimel (Ben-Gurion University), Iftach Haitner (Tel Aviv University), Nikolaos Makriyannis (Tel Aviv University), and Eran Omri (Ariel University)

Cryptographic Hashing from Strong One-Way Functions (Or: One-Way Product Functions and Their Applications) 850
Justin Holmgren (Massachusetts Institute of Technology) and Alex Lombardi (Massachusetts Institute of Technology)

Laconic Function Evaluation and Applications 859
Willy Quach (Northeastern University), Hoeteck Wee (CNRS and ENS), and Daniel Wichs (Northeastern University)

PanORAMa: Oblivious RAM with Logarithmic Overhead 871
Sarvar Patel (Google LLC), Giuseppe Persiano (Google LLC and University of Salerno), Mariana Raykova (Google LLC and Yale University), and Kevin Yeo (Google LLC)

Session 3.4.A

Efficient Algorithms for Tensor Scaling, Quantum Marginals, and Moment Polytopes 883
Peter Bürgisser (Technische Universität Berlin), Cole Franks (Rutgers University), Ankit Garg (Microsoft Research Bengaluru), Rafael Oliveira (University of Toronto), Michael Walter (University of Amsterdam and QuSoft), and Avi Wigderson (Institute for Advanced Study)

Solving Directed Laplacian Systems in Nearly-Linear Time through Sparse LU Factorizations 898
Michael B. Cohen (Massachusetts Institute of Technology), Jonathan Kelner (Massachusetts Institute of Technology), Rasmus Kyng (Harvard University), John Peebles (Massachusetts Institute of Technology), Richard Peng (Georgia Institute of Technology), Anup B. Rao (Adobe), and Aaron Sidford (Stanford University)

The Diameter of the Fractional Matching Polytope and Its Hardness Implications 910
Laura Sanità (University of Waterloo)

Coordinate Methods for Accelerating ℓ_∞ Regression and Faster Approximate Maximum Flow 922
Aaron Sidford (Stanford University) and Kevin Tian (Stanford University)

Session 3.4.B

A Near-Optimal Depth-Hierarchy Theorem for Small-Depth Multilinear Circuits 934
Suryajith Chillara (IIT Bombay), Christian Engels (IIT Bombay), Nutan Limaye (IIT Bombay), and Srikanth Srinivasan (IIT Bombay)

Pseudorandom Generators for Read-Once Branching Programs, in Any Order 946
Michael A. Forbes (University of Illinois at Urbana-Champaign) and Zander Kelley (University of Illinois at Urbana-Champaign)

Indistinguishability by Adaptive Procedures with Advice, and Lower Bounds on Hardness Amplification Proofs 956
Aryeh Grinberg (University of Haifa), Ronen Shaltiel (University of Haifa), and Emanuele Viola (Northeastern University)

Near Log-Convexity of Measured Heat in (Discrete) Time and Consequences 967
Mert Salam (University of Washington)

Session 3.5

Approximating Edit Distance within Constant Factor in Truly Sub-Quadratic Time 979
Diptarka Chakraborty (Charles University), Debarati Das (Charles University), Elazar Goldenberg (Academic College of Tel Aviv-Yaffo), Michal Koucky (Charles University), and Michael Saks (Rutgers University)

Author Index