

# **2011 IEEE 52nd Annual Symposium on Foundations of Computer Science**

**(FOCS 2011)**

**Palm Springs, California, USA  
22 – 25 October 2011**



**IEEE Catalog Number: CFP11053-PRT  
ISBN: 978-1-4577-1843-4**

# TABLE OF CONTENTS

## TUTORIALS

<b>The Promise of Differential Privacy: A Tutorial on Algorithmic Techniques</b> .....	1
<i>C. Dwork</i>	
<b>Green Computing Algorithmics</b> .....	3
<i>K. Pruhs</i>	
<b>Computing Blindfolded: New Developments in Fully Homomorphic Encryption</b> .....	5
<i>V. Vaikuntanathan</i>	

## SESSION 1A

<b>Min-Max Graph Partitioning and Small Set Expansion</b> .....	17
<i>N. Bansal, V. Nagarajan, U. Feige, J. Naor, R. Krauthgamer, K. Makarychev, R. Schwartz</i>	
<b>The Graph Minor Algorithm with Parity Conditions</b> .....	27
<i>K. Kawarabayashi, B. Reed, P. Wollan</i>	
<b>Separator Theorems for Minor-Free and Shallow Minor-Free Graphs with Applications</b> .....	37
<i>C. Wulff-Nilsen</i>	
<b>A Constant Factor Approximation Algorithm for Unsplittable Flow on Paths</b> .....	47
<i>P. Bonsma, J. Schulz, A. Wiese</i>	

## SESSION 1B

<b>How Bad is Forming Your Own Opinion?</b> .....	57
<i>D. Bindel, J. Kleinberg, S. Oren</i>	
<b>The Complexity of the Homotopy Method, Equilibrium Selection, and Lemke-Howson Solutions</b> .....	67
<i>P. Goldberg, C. Papadimitriou, R. Savani</i>	
<b>Welfare and Profit Maximization with Production Costs</b> .....	77
<i>A. Blum, A. Gupta, Y. Mansour, A. Sharma</i>	
<b>Mechanism Design with Set-Theoretic Beliefs</b> .....	87
<i>J. Chen, S. Micali</i>	

## SESSION 2A

<b>Efficient Fully Homomorphic Encryption from (Standard) LWE</b> .....	97
<i>Z. Brakerski, V. Vaikuntanathan</i>	
<b>Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits</b> .....	107
<i>C. Gentry, S. Halevi</i>	
<b>Coin Flipping with Constant Bias Implies One-Way Functions</b> .....	117
<i>I. Haitner, E. Omri</i>	
<b>How to Garble Arithmetic Circuits</b> .....	127
<i>B. Applebaum, Y. Ishai, E. Kushilevitz</i>	

## SESSION 2B

<b>Sharp Mixing Time Bounds for Sampling Random Surfaces</b> .....	137
<i>P. Caputo, F. Martinelli, F. Toninelli</i>	
<b>Improved Mixing Condition on the Grid for Counting and Sampling Independent Sets</b> .....	147
<i>R. Resprtrepo, J. Shin, P. Tetali, E. Vigoda, L. Yang</i>	
<b>Solving Connectivity Problems Parameterized by Treewidth in Single Exponential Time</b> .....	157
<i>M. Cygan, M. Pilipczuk, J. Nederlof, J. Rooij, M. Pilipczuk, J. Wojtaszczyk</i>	
<b>The Minimum k-way Cut of Bounded Size is Fixed-Parameter Tractable</b> .....	167
<i>K. Kawarabayashi, M. Thorup</i>	

### SESSION 3A

<b>Multiple-Source Multiple-Sink Maximum Flow in Directed Planar Graphs in Near-Linear Time</b> .....	177
<i>G. Borradaile, P. Klein, S. Mozes, Y. Nussbaum, C. Wulff-Nilsen</i>	
<b>Minimum Weight Cycles and Triangles: Equivalences and Algorithms</b> .....	187
<i>L. Roditty, V. Williams</i>	
<b>Graph Connectivities, Network Coding, and Expander Graphs</b> .....	197
<i>H. Cheung, L. Lau, K. Leung</i>	
<b>Maximum Edge-Disjoint Paths in Planar Graphs with Congestion 2</b> .....	207
<i>L. Seguin-Charbonneau, F. Shepherd</i>	
<b>Online Node-Weighted Steiner Tree and Related Problems</b> .....	217
<i>J. Naor, D. Panigrahi, M. Singh</i>	

### SESSION 3B

<b>Extractors for Circuit Sources</b> .....	227
<i>E. Viola</i>	
<b>Randomness Buys Depth for Approximate Counting</b> .....	237
<i>E. Viola</i>	
<b>Pseudorandomness for Read-Once Formulas</b> .....	247
<i>A. Bogdanov, P. Papakonstantinou, A. Wan</i>	
<b>Dispersers for Affine Sources with Sub-polynomial Entropy</b> .....	254
<i>R. Shaltiel</i>	
<b>A Small PRG for Polynomial Threshold Functions of Gaussians</b> .....	264
<i>D. Kane</i>	

### SESSION 4

<b>A Polylogarithmic-Competitive Algorithm for the k-Server Problem</b> .....	274
<i>N. Bansal, N. Buchbinder, A. Madry, J. Naor</i>	
<b>3-SAT Faster and Simpler - Unique-SAT Bounds for PPSZ Hold in General</b> .....	284
<i>T. Hertli</i>	

### SESSION 5A

<b>On the Power of Adaptivity in Sparse Recovery</b> .....	292
<i>P. Indyk, E. Price, D. Woodruff</i>	
<b>(1 + <math>\epsilon</math>)-Approximate Sparse Recovery</b> .....	302
<i>E. Price, D. Woodruff</i>	
<b>Near-Optimal Column-Based Matrix Reconstruction</b> .....	312
<i>C. Boutsidis, P. Drineas, M. Magdon-Ismail</i>	
<b>Near Linear Lower Bound for Dimension Reduction in <math>L_1</math></b> .....	322
<i>A. Andoni, M. Charikar, O. Neiman, H. Nguyen</i>	

### SESSION 5B

<b>The 1D Area Law and the Complexity of Quantum States: A Combinatorial Approach</b> .....	331
<i>D. Aharonov, Z. Landau, U. Vazirani, I. Arad</i>	
<b>On the Complexity of Commuting Local Hamiltonians, and Tight Conditions for Topological Order in Such Systems</b> .....	341
<i>D. Aharonov, L. Eldar</i>	
<b>Quantum Query Complexity of State Conversion</b> .....	351
<i>T. Lee, R. Mittal, B. Reichardt, R. Spalek, M. Szegedy</i>	
<b>Optimal Bounds for Quantum Bit Commitment</b> .....	361
<i>A. Chailloux, I. Kerenidis</i>	

## **SESSION 6A**

<b>Streaming Algorithms via Precision Sampling</b> .....	370
<i>A. Andoni, R. Krauthgamer, K. Onak</i>	
<b>Steiner Shallow-Light Trees are Exponentially Lighter than Spanning Ones</b> .....	380
<i>M. Elkin, S. Solomon</i>	
<b>Fully Dynamic Maximal Matching in <math>O(\log n)</math> Update Time</b> .....	390
<i>S. Baswana, M. Gupta, S. Sen</i>	
<b>Which Networks are Least Susceptible to Cascading Failures?</b> .....	400
<i>L. Blume, D. Easley, J. Kleinberg, R. Kleinberg, E. Tardos</i>	

## **SESSION 6B**

<b>The Power of Linear Estimators</b> .....	410
<i>G. Valiant, P. Valiant</i>	
<b>An Algebraic Proof of a Robust Social Choice Impossibility Theorem</b> .....	420
<i>D. Falik, E. Friedgut</i>	
<b>Planar Graphs: Random Walks and Bipartiteness Testing</b> .....	430
<i>A. Czumaj, K. Onak, M. Monemizadeh, C. Sohler</i>	
<b>Testing and Reconstruction of Lipschitz Functions with Applications to Data Privacy</b> .....	440
<i>M. Jha, S. Raskhodnikova</i>	

## **SESSION 7A**

<b>How to Play Unique Games Against a Semi-random Adversary: Study of Semi-random Models of Unique Games</b> .....	450
<i>A. Kolla, K. Makarychev, Y. Makarychev</i>	
<b>The Grothendieck Constant is Strictly Smaller than Krivine's Bound</b> .....	460
<i>M. Braverman, K. Makarychev, Y. Makarychev, A. Naor</i>	
<b>A Parallel Approximation Algorithm for Positive Semidefinite Programming</b> .....	470
<i>R. Jain, P. Yao</i>	
<b>Rounding Semidefinite Programming Hierarchies via Global Correlation</b> .....	479
<i>B. Barak, P. Raghavendra, D. Steurer</i>	
<b>Lasserre Hierarchy, Higher Eigenvalues, and Approximation Schemes for Graph Partitioning and Quadratic Integer Programming with PSD Objectives</b> .....	489
<i>V. Guruswami, A. Sinop</i>	

## **SESSION 7B**

<b>Markov Layout</b> .....	499
<i>F. Chierichetti, R. Kumar, P. Raghavan</i>	
<b>Limitations of Randomized Mechanisms for Combinatorial Auctions</b> .....	509
<i>S. Dughmi, J. Vondrak</i>	
<b>Bayesian Combinatorial Auctions: Expanding Single Buyer Mechanisms to Many Buyers</b> .....	519
<i>S. Alaei</i>	
<b>Extreme-Value Theorems for Optimal Multidimensional Pricing</b> .....	529
<i>Y. Cai, C. Daskalakis</i>	
<b>Efficient Computation of Approximate Pure Nash Equilibria in Congestion Games</b> .....	539
<i>I. Caragiannis, A. Fanelli, N. Gravin, A. Skopalik</i>	

## **SESSION 8**

<b>On Range Searching in the Group Model and Combinatorial Discrepancy</b> .....	549
<i>K. Larsen</i>	
<b>A Randomized Rounding Approach to the Traveling Salesman Problem</b> .....	557
<i>S. Gharan, A. Saberi, M. Singh</i>	
<b>Approximating Graphic TSP by Matchings</b> .....	567
<i>T. Momke, O. Svensson</i>	

## **SESSION 9A**

<b>A Unified Continuous Greedy Algorithm for Submodular Maximization</b> .....	577
<i>M. Feldman, J. Naor, R. Schwartz</i>	
<b>Enumerative Lattice Algorithms in any Norm Via M-ellipsoid Coverings</b> .....	587
<i>D. Dadush, C. Peikert, S. Vempala</i>	
<b>A Nearly-m Log N Time Solver for SDD Linear Systems</b> .....	597
<i>I. Koutis, G. Miller, R. Peng</i>	
<b>Balls and Bins: Smaller Hash Families and Faster Evaluation</b> .....	606
<i>L. Celis, O. Reingold, G. Segev, U. Wieder</i>	

## **SESSION 9B**

<b>Lexicographic Products and the Power of Non-linear Network Coding</b> .....	616
<i>A. Blasiak, R. Kleinberg, E. Lubetzky</i>	
<b>Quadratic Goldreich-Levin Theorems</b> .....	626
<i>M. Tulsiani, J. Wolf</i>	
<b>Optimal Testing of Multivariate Polynomials over Small Prime Fields</b> .....	636
<i>E. Haramaty, A. Shpilka, M. Sudan</i>	
<b>Tight Lower Bounds for 2-query LCCs over Finite Fields</b> .....	645
<i>A. Bhattacharyya, A. Shpilka, Z. Dvir, S. Saraf</i>	

## **SESSION 10A**

<b>A Two Prover One Round Game with Strong Soundness</b> .....	655
<i>S. Khot, M. Safra</i>	
<b>The Randomness Complexity of Parallel Repetition</b> .....	665
<i>K. Chung, R. Pass</i>	
<b>Privacy Amplification and Non-malleable Extractors via Character Sums</b> .....	675
<i>Y. Dodis, X. Li, T. Wooley, D. Zuckerman</i>	
<b>Stateless Cryptographic Protocols</b> .....	685
<i>V. Goyal, H. Maji</i>	
<b>Storing Secrets on Continually Leaky Devices</b> .....	695
<i>Y. Dodis, A. Lewko, B. Waters, D. Wichs</i>	

## **SESSION 10B**

<b>Medium Access Using Queues</b> .....	705
<i>D. Shah, J. Shin, P. Tetali</i>	
<b>Local Distributed Decision</b> .....	715
<i>P. Fraigniaud, A. Korman, D. Peleg</i>	
<b>The Complexity of Renaming</b> .....	725
<i>D. Alistarh, J. Aspnes, S. Gilbert, R. Guerraoui</i>	
<b>Mutual Exclusion with <math>O(\log^2 \log n)</math> Amortized Work</b> .....	735
<i>M. Bender, S. Gilbert</i>	
<b>Algorithms for the Generalized Sorting Problem</b> .....	745
<i>Z. Huang, S. Kannan, S. Khanna</i>	

## **SESSION 11A**

<b>Information Equals Amortized Communication</b> .....	755
<i>M. Braverman, A. Rao</i>	
<b>Delays and the Capacity of Continuous-Time Channels</b> .....	765
<i>S. Khanna, M. Sudan</i>	
<b>Efficient and Explicit Coding for Interactive Communication</b> .....	775
<i>R. Gelles, A. Moitra, A. Sahai</i>	
<b>Efficient Reconstruction of Random Multilinear Formulas</b> .....	785
<i>A. Gupta, N. Kayal, S. Lokam</i>	

<b>New Extension of the Weil Bound for Character Sums with Applications to Coding .....</b>	<b>795</b>
<i>T. Kaufman, S. Lovett</i>	

**SESSION 11B**

<b>Maximizing Expected Utility for Stochastic Combinatorial Optimization Problems .....</b>	<b>804</b>
<i>J. Li, A. Deshpande</i>	
<b>Approximation Algorithms for Submodular Multiway Partition.....</b>	<b>814</b>
<i>C. Chekuri, A. Ene</i>	
<b>An FPTAS for #Knapsack and Related Counting Problems .....</b>	<b>824</b>
<i>P. Gopalan, A. Klivans, R. Meka, D. Stefankovic, S. Vempala, E. Vigoda</i>	
<b>Approximation Algorithms for Correlated Knapsacks and Non-martingale Bandits .....</b>	<b>834</b>
<i>A. Gupta, R. Krishnaswamy, M. Molinaro, R. Ravi</i>	
<b>Evolution with Recombination .....</b>	<b>844</b>
<i>V. Kanade</i>	
<b>Author Index</b>	