

The 43^d Annual IEEE Symposium on Foundations of Computer Science

FOCS 2002

The 43^d Annual IEEE Symposium on Foundations of Computer Science

Proceedings

The 43rd Annual IEEE Symposium on
Foundations of Computer Science

Vancouver, BC, Canada
16-19 November 2002

Sponsored by

IEEE Computer Society Technical Committee on
Mathematical Foundations of Computing (TCMF)

In cooperation with

ACM/SIGACT



Los Alamitos, California

Washington • Brussels • Tokyo

Copyright © 2002 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number PR01822
ISBN 0-7695-1822-2
ISSN 0272-5428

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 714 821 8380
Fax: + 1 714 821 4641
[http://computer.org/
csbooks@computer.org](http://computer.org/csbooks@computer.org)

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
[http://shop.ieee.org/store/
customer-service@ieee.org](http://shop.ieee.org/store/customer-service@ieee.org)

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Editorial production by Danielle C. Martin

Cover art production by Alex Torres

Printed in the United States of America by The Printing House



Foreword

The papers in these proceedings were presented at the 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2002) sponsored by the IEEE Computer Society Technical Committee on Mathematical Foundations of Computing. The conference was held in Vancouver, Canada, November 16-19, 2002.

The program committee consisted of Dorit Aharonov (Hebrew U), Maria Luisa Bonet (UPC, Barcelona), Bernard Chazelle (Princeton & NEC Research), Edith Cohen (AT&T Labs), Lance Fortnow (NEC Research), Anna Gál (UT Austin), Venkatesan Guruswami (UC Berkeley & U Washington), Piotr Indyk (MIT), Ravi Kannan (Yale), Claire Kenyon (U Paris-Sud), Yuval Rabani (Technion), Tal Rabin (IBM Research), Omer Reingold (AT&T Labs), Ronitt Rubinfeld (NEC Research), David B. Shmoys (Cornell), Dan Spielman (MIT), Emo Welzl (ETH Zurich).

The program committee met on June 21-22, 2002 and selected 77 papers from 279 submitted. The submissions were reviewed as carefully as time permitted but they were not formally refereed. It is expected that many of them will appear in a more polished and complete form in scientific journals in the future. In addition to the regular program, we invited three speakers to give tutorial lectures, Oded Goldreich, Eva Tardos, and Salil Vadhan.

The committee selected three papers to receive the Best Paper Award. These were: "Constant-Round Coin-Tossing with a Man in the Middle or Realizing the Shared Random String Model," by Boaz Barak, "Minimizing Congestion in General Networks," by Harald Räcke, and "A Dichotomy Theorem for Constraints on a Three-Element Set," by Andrei A. Bulatov. In addition, the first two papers received the Machtey Award for best student-authored paper.

The committee wishes to thank all of those who submitted papers for consideration, as well as those external reviewers who helped evaluate the submissions. A list of reviewers appears under the heading "Reviewers." The program committee also wishes to thank Joe Kilian and Steve Tate for running the electronic submission server and Danielle Martin for the production of these proceedings.

Bernard Chazelle
Program Committee Chair

Program Committee

Chair of the IEEE Technical Committee on Mathematical Foundations of Computing
Prabhakar Raghavan, Verity

Local Arrangements and Finance Chair
Arvind Gupta, Simon Fraser University

Program Committee Chair
Bernard Chazelle, Princeton University and NEC Research

Program Committee Members

Dorit Aharonov
Maria Luisa Bonet
Bernard Chazelle
Edith Cohen
Lance Fortnow
Anna Gál
Venkatesan Guruswami
Piotr Indyk
Ravi Kannan
Claire Kenyon
Yuval Rabani
Tal Rabin
Omer Reingold
Ronitt Rubinfeld
David B. Shmoys
Dan Spielman
Emo Welzl

Awards

"Constant-Round Coin-Tossing with a Man in the Middle or
Realizing the Shared Random String Model"
Boaz Barak, *Best Paper Award & Machtey Award*

and

"Minimizing Congestion in General Networks"
Harald Räcke, *Best Paper Award & Machtey Award*

and

"A Dichotomy Theorem for Constraints on a Three-Element Set"
Andrei A. Bulatov, *Best Paper Award*

Reviewers

Scott Aaronson
Udo Adamy
Micah Adler
Pavan Aduri
Pankaj Agarwal
Bill Aiello
Eric Allender
Noga Alon
Andris Ambainis
Christoph Ambühl
Amihod Amir
David Applegate
Aaron Archer
Lars Arge
Sanjeev Arora
Albert Atserias
Hagit Attiya
Yossi Azar
Moshe Babaioff
Eric Bach
Jose Luis Balcazar
Amotz Bar-Noy
Yair Bartal
Eric Baum
Paul Beame
Richard Beigel
Amos Beimel
Alexander Below
Michael Ben-Or
Eli Ben-Sasson
Andras Benczur
Mark de Berg
Michel Berkovier
Johannes Blömer
Allan Borodin
Stéphane Boucheron
Gerth Brodal
Dan Brown
Adam Buchsbaum
Harry Buhrman
Sam Buss
Christian Calude
Ran Canetti
Michael Capalbo
Rafael Casas
Jorge Castro
Nicolo Cesa-Bianchi

Amit Chakrabarti
Timothy Chan
Moses Charikar
Chandra Chekuri
Ken Clarkson
Richard Cleve
Anne Condon
Don Coppersmith
Bruno Courcelle
Pilu Crescenzi
Janos Csirik
Petér Csorba
Victor Dalmau
Sanjoy Dasgupta
Ronald De Wolf
Luc Devroye
Volker Diekert
David DiVincenzo
Irit Dinur
Yevgeniy Dodis
Rod Downey
Michael Elkin
Robert Elsasser
Ioannis Emiris
Lars Engebretsen
Funda Ergun
Thomas Erlebach
Juan Luis Esteban
Ron Fagin
Martin Farach-Colton
Joan Feigenbaum
Wenceslas Fernandez de la Vega
Amos Fiat
Faith Fich
Eldar Fischer
Kaspar Fischer
Roger Fischlin
Philippe Flajolet
Tamas Fleiner
Lisa Fleischer
Sally Floyd
Steve Fortune
Pierre Fraigniaud
Ari Freund
Yoav Freund
Katalin Friedl

Alan Frieze
Peter Gacs
Nicola Galesi
Ricard Gavalda
Bill Gasarch
Rosario Gennaro
Joachim Giesen
Anna Gilbert
Marc Giusti
Wayne Goddard
Ashish Goel
Andrew Goldberg
Leslie Goldberg
Oded Goldreich
Daniel Gottesman
Sudipto Guha
Torben Hagerup
Shai Halevi
Joe Halperin
Sariel Har-Peled
Johan Håstad
Lisa Hellerstein
Christoph Helmberg
Maurice Herlihy
John Hitchcock
Michael Hoffmann
Peter Hoyer
Juraj Hromkovic
Mark Huber
Dominic Hughes
Sandy Irani
Yuval Ishai
Alon Itai
David Johnson
Sampath Kannan
Haim Kaplan
Bruce Kapron
Juhani Karhumäki
Howard Karloff
Gyula Karolyi
Richard Kenyon
Joe Kilian
Valerie King
Sanjeev Khanna
Subhash Khot
Phil Klein
Jon Kleinberg

Table of Contents

The 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2002)

Foreword	xiii
Program Committee	xiv
Reviewers	xv

TUTORIAL 1

Chair: Venkatesan Guruswami

Zero-Knowledge	3
<i>Oded Goldreich, Weizmann Institute of Science, Israel</i>	

TUTORIAL 2

Chair: Yuval Rabani

Approximation Algorithms	
<i>Eva Tardos, Cornell University</i>	

TUTORIAL 3

Chair: Omer Reingold

Randomness Extractors and Their Many Guises	9
<i>Salil P. Vadhan, Harvard University</i>	

SESSION 1A

Chair: Venkatesan Guruswami

Locally Testable Codes and PCPs of Almost-Linear Length	13
<i>O. Goldreich and M. Sudan</i>	
Hardness Results for Coloring 3-Colorable 3-Uniform Hypergraphs	23
<i>S. Khot</i>	
The Hardness of 3-Uniform Hypergraph Coloring	33
<i>I. Dinur, O. Regev, and C. Smyth</i>	

SESSION 1B

Chair: Yuval Rabani

Minimizing Congestion in General Networks.....	43
<i>H. Räcke</i>	
Small Induced-Universal Graphs and Compact Implicit Graph Representations.....	53
<i>S. Alstrup and T. Rauhe</i>	
Deterministic Broadcasting Time in Radio Networks of Unknown Topology	63
<i>D. Kowalski and A. Pelc</i>	
Explicit Unique-Neighbor Expanders.....	73
<i>N. Alon and M. Capalbo</i>	

SESSION 2A

Chair: Ronitt Rubinfeld

Abstract Combinatorial Programs and Efficient Property Testers	83
<i>A. Czumaj and C. Sohler</i>	
A Lower Bound for Testing 3-Colorability in Bounded-Degree Graphs	93
<i>A. Bogdanov, K. Obata, and L. Trevisan</i>	
Testing Juntas	103
<i>E. Fischer, G. Kindler, D. Ron, S. Safra, and A. Samorodnitsky</i>	
A Spectral Algorithm for Learning Mixtures of Distributions	113
<i>S. Vempala and G. Wang</i>	

SESSION 2B

Chair: Bernard Chazelle

Equivalence between Priority Queues and Sorting	125
<i>M. Thorup</i>	
Integer Sorting in $O(n\sqrt{\log \log n})$ Expected Time and Linear Space	135
<i>Y. Han and M. Thorup</i>	
Implicit B-Trees: New Results for the Dictionary Problem	145
<i>G. Franceschini, R. Grossi, J. Munro, and L. Pagli</i>	
An Inverse-Ackermann Style Lower Bound for the Online Minimum Spanning Tree Verification Problem	155
<i>S. Pettie</i>	

SESSION 3A

Chair: Ronitt Rubinfeld

PAC = PAExact and Other Equivalent Models in Learning.....	167
<i>N. Bshouty and D. Gavinsky</i>	
Learning Intersections and Thresholds of Halfspaces	177
<i>A. Klivans, R. O'Donnell, and R. Servedio</i>	
On-Line Confidence Machines Are Well-Calibrated.....	187
<i>V. Vovk</i>	
Learning a Hidden Matching.....	197
<i>N. Alon, R. Beigel, S. Kasif, S. Rudich, and B. Sudakov</i>	

SESSION 3B

Chair: Piotr Indyk

An Information Statistics Approach to Data Stream and Communication Complexity	209
<i>Z. Bar-Yossef, T. Jayram, R. Kumar, and D. Sivakumar</i>	
Static Optimality Theorem for External Memory String Access	219
<i>V. Ciriani, P. Ferragina, F. Luccio, and S. Muthukrishnan</i>	
A Simple Algorithmic Characterization of Uniform Solvability	228
<i>E. Gafni</i>	
Correlation Clustering	238
<i>N. Bansal, A. Blum, and S. Chawla</i>	

SESSION 4A

Chair: Dan Spielman

Decoding Turbo-Like Codes via Linear Programming.....	251
<i>J. Feldman and D. Karger</i>	
Breaking the $O(n^{1/(2k-1)})$ Barrier for Information-Theoretic Private Information Retrieval	261
<i>A. Beimel, Y. Ishai, E. Kushilevitz, and J.-F. Raymond</i>	
LT Codes	271
<i>M. Luby</i>	

SESSION 4B

Chair: Edith Cohen

Graphs with Tiny Vector Chromatic Numbers and Huge Chromatic Numbers	283
<i>U. Feige, M. Langberg, and G. Schechtman</i>	
Scheduling over a Time-Varying User-Dependent Channel with Applications to High Speed Wireless Data	293
<i>M. Andrews and L. Zhang</i>	
On-Line End-to-End Congestion Control	303
<i>N. Garg and N. Young</i>	

SESSION 1A

Chair: David Shmoys

Proving Integrality Gaps without Knowing the Linear Program	313
<i>S. Arora, B. Bollobás, and L. Lovász</i>	
Dependent Rounding in Bipartite Graphs	323
<i>R. Gandhi, S. Khuller, S. Parthasarathy, and A. Srinivasan</i>	
A Constant-Factor Approximation Algorithm for the Multicommodity Rent-or-Buy Problem	333
<i>A. Kumar, A. Gupta, and T. Roughgarden</i>	

SESSION 1B

Chair: Tal Rabin

Constant-Round Coin-Tossing with a Man in the Middle or Realizing the Shared Random String Model	345
<i>B. Barak</i>	
Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions from Worst-Case Complexity Assumptions	356
<i>D. Micciancio</i>	
Concurrent Zero Knowledge with Logarithmic Round-Complexity	366
<i>M. Prabhakaran, A. Rosen, and A. Sahai</i>	
On the (non)Universality of the One-Time Pad	376
<i>Y. Dodis and J. Spencer</i>	

SESSION 2A

Chair: Yuval Rabani

Market Equilibrium via a Primal-Dual-Type Algorithm.....	389
<i>N. Devanur, C. Papadimitriou, A. Saberi, and V. Vazirani</i>	
On the Hardness of Optimal Auctions	396
<i>A. Ronen and A. Saberi</i>	
Auctions with Severely Bounded Communication	406
<i>L. Blumrosen and N. Nisan</i>	
Nash Equilibria in Competitive Societies, with Applications to Facility Location, Traffic Routing and Auctions	416
<i>A. Vetta</i>	

SESSION 2B

Chair: Omer Reingold

Privacy and Interaction in Quantum Communication Complexity and a Theorem about the Relative Entropy of Quantum States.....	429
<i>R. Jain, J. Radhakrishnan, and P. Sen</i>	
Linear Diophantine Equations over Polynomials and Soft Decoding of Reed-Solomon Codes.....	439
<i>M. Alekhnovich</i>	
Authentication of Quantum Messages	449
<i>H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp</i>	
Limits on the Power of Quantum Statistical Zero-Knowledge.....	459
<i>J. Watrous</i>	

SESSION 3A

Chair: David Shmoys

Protocols and Impossibility Results for Gossip-Based Communication Mechanisms.....	471
<i>D. Kempe and J. Kleinberg</i>	
Covering Problems with Hard Capacities.....	481
<i>J. Chuzhoy and J. Naor</i>	
Packing 2-Dimensional Bins in Harmony.....	490
<i>A. Caprara</i>	

Fast Approximation Algorithms for Fractional Steiner Forest and Related Problems	500
<i>N. Garg and R. Khandekar</i>	

SESSION 3B

Chair: Dorit Aharonov

Quantum Lower Bounds for the Collision and the Element Distinctness Problems	513
<i>Y. Shi</i>	
Quantum Computation and Lattice Problems	520
<i>O. Regev</i>	
On the Decidability of Self-Assembly of Infinite Ribbons	530
<i>L. Adleman, J. Kari, L. Kari, and D. Reishus</i>	
The Parameterized Complexity of Counting Problems	538
<i>J. Flum and M. Grohe</i>	

SESSION 4A

Chair: Bernard Chazelle

Dimension Reduction in the ℓ_1 Norm	551
<i>M. Charikar and A. Sahai</i>	
On Approximating the Radii of Point Sets in High Dimensions.....	561
<i>K. Varadarajan, S. Venkatesh, and J. Zhang</i>	
Low-Dimensional Linear Programming with Violations	570
<i>T. Chan</i>	

SESSION 4B

Chair: Maria Bonet

Bounded-Depth Frege Lower Bounds for Weaker Pigeonhole Principles.....	583
<i>J. Buresh-Oppenheim, P. Beame, T. Pitassi, R. Raz, and A. Sabharwal</i>	
Satisfiability, Branch-Width and Tseitin Tautologies	593
<i>M. Alekhnovich and A. Razborov</i>	
A Switching Lemma for Small Restrictions and Lower Bounds for k -DNF Resolution	604
<i>N. Segerlind, S. Buss, and R. Impagliazzo</i>	

SESSION 1A

Chair: Piotr Indyk

Dynamic Planar Convex Hull.....	617
<i>G. Brodal and R. Jacob</i>	
Optimal System of Loops on an Orientable Surface.....	627
<i>É. Colin de Verdière and F. Lazarus</i>	
The Partition Technique for Overlays of Envelopes	637
<i>V. Koltun and M. Sharir</i>	

SESSION 1B

Chair: Anna Gal

A Dichotomy Theorem for Constraints on a Three-Element Set.....	649
<i>A. Bulatov</i>	
Lower Bounds on the Bounded Coefficient Complexity of Bilinear Maps	659
<i>P. Bürgisser and M. Lotz</i>	
Power from Random Strings	669
<i>E. Allender, H. Buhrman, M. Koucký, D. van Melkebeek, and D. Ronneburger</i>	
Improved Dynamic Reachability Algorithms for Directed Graphs	679
<i>L. Roditty and U. Zwick</i>	

SESSION 2A

Chair: Claire Kenyon

Conflict-Free Colorings of Simple Geometric Regions with Applications to Frequency Assignment in Cellular Networks.....	691
<i>G. Even, Z. Lotker, D. Ron, and S. Smorodinsky</i>	
Global Information from Local Observation	701
<i>I. Benjamini and L. Lovász</i>	
Rapidly Mixing Markov Chains for Sampling Contingency Tables with a Constant Number of Rows.....	711
<i>M. Cryan, M. Dyer, L. Goldberg, M. Jerrum, and R. Martin</i>	
Spectral Gap and log-Sobolev Constant for Balanced Matroids.....	721
<i>M. Jerrum and J.-B. Son</i>	

SESSION 2B**Chair: Anna Gal**

Random Lattices and a Conjectured 0 - 1 Law about Their Polynomial Time Computable Properties	733
<i>M. Ajtai</i>	
Graph Isomorphism is in SPP	743
<i>V. Arvind and P. Kurur</i>	
Kolmogorov's Structure Functions with an Application to the Foundations of Model Selection.....	751
<i>N. Vereshchagin and P. Vitányi</i>	
Forbidden Information	761
<i>L. Levin</i>	

SESSION 3**Chair: Claire Kenyon**

The 3-XORSAT Threshold.....	769
<i>O. Dubois and J. Mandler</i>	
The Asymptotic Order of the Random k -SAT Threshold.....	779
<i>D. Achlioptas and C. Moore</i>	
On Random Symmetric Travelling Salesman Problems	789
<i>A. Frieze</i>	
Load Balancing with Memory.....	799
<i>M. Mitzenmacher, B. Prabhakar, and D. Shah</i>	
Erratum to "Vickrey Pricing and Shortest Paths: What Is an Edge Worth?"	809
<i>J. Hershberger and S. Suri</i>	
Author Index	811

Zero-Knowledge: Abstract of a Tutorial*

Oded Goldreich

Department of Computer Science

Weizmann Institute of Science

Rehovot, ISRAEL.

Email: oded@wisdom.weizmann.ac.il

Zero-Knowledge proofs are fascinating and extremely useful constructs. Their fascinating nature is due to their seemingly contradictory definition; zero-knowledge proofs are both convincing and yet yield nothing beyond the validity of the assertion being proven. Their applicability in the domain of cryptography is vast; they are typically used to force malicious parties to behave according to a predetermined protocol. In addition to their direct applicability in Cryptography, zero-knowledge proofs serve as a good bench-mark for the study of various problems regarding cryptographic protocols (e.g., “secure composition of protocols” and the “use of of the adversary’s program within the proof of security”).

In this tutorial we will present the basic definitions and results regarding zero-knowledge as well as some recent developments regarding this notion.

The Basics. Loosely speaking, zero-knowledge proofs are proofs that yield nothing beyond the validity of the assertion. That is, a verifier obtaining such a proof only gains conviction in the validity of the assertion. This is formulated by saying that anything that is feasibly computable from a zero-knowledge proof is also feasibly computable from the (valid) assertion itself (by a so-called simulator). Variants on the basic definition include:

- Consideration of auxiliary inputs.
- Universal and black-box simulations.
- Restricting attention to honest verifiers.
- The level of similarity required of the simulation.

It is well-known that *zero-knowledge proofs exist for any NP-set*, provided that one-way functions exist. This result is a powerful tool in the design of cryptographic protocols, because it enables to force parties to behave according to a predetermined protocol (i.e., the protocol requires parties to provide zero-knowledge proofs of the correctness of their secret-based actions, without revealing these secrets).

*The full version of this tutorial is available from URL <http://www.wisdom.weizmann.ac.il/~oded/zk-tut02.html>

Advanced Topics. We focus on two basic problems regarding zero-knowledge, which actually arise also with respect to the security of other cryptographic primitives. The first question refers to the preservation of security (i.e., zero-knowledge in our case) under various types of composition operations. We survey the known results regarding sequential, parallel and concurrent execution of (arbitrary and/or specific) zero-knowledge protocols. The main facts are:

- Zero-knowledge (w.r.t auxiliary inputs) is closed under sequential composition.
- In general, zero-knowledge is not closed under parallel composition. Yet, some zero-knowledge proofs (for NP) preserve their security when many copies are executed in parallel. Furthermore, some of these protocol use a constant number of rounds.
- Some zero-knowledge proofs (for NP) preserve their security when many copies are executed concurrently, but such a result is not known for constant-round protocols.

The second basic question regarding zero-knowledge refers to the usage of the adversary’s program within the proof of security (i.e., demonstration of the zero-knowledge property). For 15 years, all known proofs of security used the adversary’s program as a black-box (i.e., a universal simulator was presented using the adversary’s program as an oracle). Furthermore, it was believed that there is no advantage in having access to the code of the adversary’s program. Consequently it was conjectured that negative results regarding black-box simulation represent an inherent limitation of zero-knowledge. This belief has been refuted recently by a zero-knowledge argument (for NP) that has important properties that are unachievable by black-box simulation.

Other topics treated in the full version of the tutorial (but not in its oral presentation) include proofs of knowledge, Non-Interactive Zero-Knowledge proofs, Statistical Zero-Knowledge, Knowledge Complexity, and the resettability of a party’s random-tape.

Johannes Kobler
 Robert Krauthgamer
 Amit Kumar
 Ravi Kumar
 Eyal Kushilevitz
 Hugo Krawczyk
 Sophie Laplante
 Ron Lavi
 Stefano Leonardi
 Leonid Levin
 Jordi Levy
 Moshe Lewenstein
 Ming Li
 Leonid Libkin
 Nati Linial
 Zsuzsanna Lipták
 Zvika Lotker
 Gabor Lugosi
 Alexey Lvov
 Frank McSherry
 Avner Magen
 Johann Makowsky
 Dalia Malkhi
 Tal Malkin
 Yishay Mansour
 Conrado Martinez
 Jirí Matoušek
 Marios Mavronikolas
 Elvira Mayordomo
 Daniele Micciancio
 Peter Bro Miltersen
 Joe Mitchell
 Michael Mitzenmacher
 Shlomo Moran
 Elchanan Mossel
 Ahuva Mualem
 Ian Munro
 Muthu Muthukrishnan
 Moni Naor
 Seffi Naor
 Ilan Newman
 Noam Nisan
 Kobbi Nissim
 Yoshio Okamoto
 Rafail Ostrovsky
 Joseph O'Rourke
 Christos Papadimitriou
 Michal Parnas
 Boaz Patt-Shamir
 David Pennock

Erez Petrank
 Ion Petre
 Steven Phillips
 Benny Pinkas
 Toniann Pitassi
 Pavel Pudlak
 Yuri Rabinovich
 Charlie Rackoff
 Ranjith Rajagopalan
 Dana Randall
 Satish Rao
 Ran Raz
 Alexander Razborov
 Oded Regev
 Leonid Reyzin
 Lajos Ronyai
 Alon Rosen
 Ronny Roth
 Tim Roughgarden
 Salvador Roura
 Gitit Ruchenstein
 Matthias Ruhl
 Alex Russell
 Joerg Sack
 Amit Sahai
 Cenk Sahinalp
 Mike Saks
 Louis Salvail
 Rahul Sami
 Alex Samorodnitsky
 Jeff Sanders
 V. Lokam Satyanarayana
 Rob Schapire
 Baruch Schieber
 Uwe Schöning
 Ilya Segal
 Luc Ségoufin
 Rocco Servedio
 Ronen Shaltiel
 Scott Shenker
 Peter Shor
 Dan Simon
 Mona Singh
 Ramesh Sitaraman
 Bob Sloan
 Adam Smith
 Warren Smith
 Clifford Smyth
 Greg Sorkin
 Bettina Speckmann

Aravind Srinivasan
 Divesh Srivastava
 Stamatis Stefanakos
 Cliff Stein
 Jim Storer
 Martin Strauss
 Benjamin Sudakov
 Madhu Sudan
 Maxim Sviridenko
 Tibor Szabó
 Mario Szegedy
 Roberto Tamassia
 Eva Tardos
 Gabor Tardos
 Amnon Ta-Shma
 Shang-Hua Teng
 Lothar Thiele
 Dimitrios Thilikos
 Jayram Thathachar
 Andrew Thomason
 Mikkel Thorup
 Jean-Pierre Tillich
 Jacobo Toran
 Csaba D. Tóth
 Luca Trevisan
 Vladimir Trifonov
 Falk Tschirschnitz
 Wen-Guey Tzeng
 Salil Vadhan
 Gabriel Valiente
 Pavel Valtr
 Dieter van Melkebeek
 Farrokh Vatan
 Suresh Venkatasubramanian
 Bernhard von Stengel
 Uli Wagner
 Tandy Warnow
 Roger Wattenhofer
 Avi Wigderson
 Thomas Wilke
 Dan Willard
 David Williamson
 Gerhard Woeginger
 Neal Young
 An Zhu
 Günter M. Ziegler
 David Zuckerman
 Uri Zwick