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

The 43rd Annual IEEE Symposium on Foundations of Computer Science

FOCS 2002

The 43rd 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

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

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

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
Amihood 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)

SESSION 1B

Chair: Yuval Rabani

SESSION 2A

Chair: Ronitt Rubinfeld

SESSION 2B

Chair: Bernard Chazelle

SESSION 3A

Chair: Ronitt Rubinfeld

SESSION 3B

Chair: Piotr Indyk

SESSION 4A

Chair: Dan Spielman

SESSION 4B

Chair: Edith Cohen

SESSION 1A

Chair: David Shmoys

SESSION 1B

Chair: Tal Rabin

SESSION 2A

Chair: Yuval Rabani

SESSION 2B

Chair: Omer Reingold

SESSION 3A

Chair: David Shmoys

SESSION 3B

Chair: Dorit Aharonov

SESSION 4A

Chair: Bernard Chazelle

SESSION 4B

Chair: Maria Bonet

SESSION 1A

Chair: Piotr Indyk

SESSION 1B

Chair: Anna Gal

SESSION 2A

Chair: Claire Kenyon

SESSION 2B

Chair: Anna Gal

SESSION 3

Chair: Claire Kenyon

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).

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.

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

Proceedings of the 43 rd Annual IEEE Symposium on Foundations of Computer Science (FOCS'02)
0272-5428/02 $17.00 © 2002 **IEEE**

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