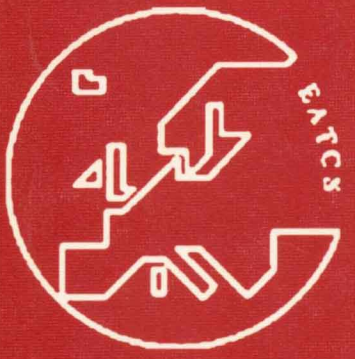
Luís Caires
Giuseppe F. Italiano
Luís Monteiro
Catuscia Palamidessi
Moti Yung (Eds.)

LNCS 3580

# Automata, Languages and Programming

32nd International Colloquium, ICALP 2005
Lisbon, Portugal, July 2005
Proceedings




Springer

Luís Caires Giuseppe F. Italiano
Luís Monteiro Catuscia Palamidessi
Moti Yung (Eds.)

# Automata, Languages and Programming

32nd International Colloquium, ICALP 2005
Lisbon, Portugal, July 11-15, 2005
Proceedings

Springer

Volume Editors

Luís Caires
Universidade Nova de Lisboa, Departamento de Informatica
2829-516 Caparica, Portugal
E-mail: Luis.Caires@di.fct.unl.pt

Giuseppe F. Italiano
Universitá di Roma "Tor Vergata"
Dipartimento di Informatica, Sistemi e Produzione
Via del Politecnico 1, 00133 Roma, Italy
E-mail: italiano@disp.uniroma2.it

Luís Monteiro
Universidade Nova de Lisboa, Departamento de Informatica
2829-516 Caparica, Portugal
E-mail: lm@di.fct.unl.pt

Catuscia Palamidessi
INRIA Futurs and LIX, École Polytechnique
rue de Saclay, 91128 Palaiseau, France
E-mail: catuscia@lix.polytechnique.fr

Moti Yung
RSA Laboratories and Columbia University
Computer Science Department
1214 Amsterdam Av., New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2005928673

CR Subject Classification (1998): F, D, C.2-3, G.1-2, I.3, E.1-2

ISSN 0302-9743
ISBN-10 3-540-27580-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-27580-0 Springer Berlin Heidelberg New York



Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11523468 06/3142 5 4 3 2 1 0

# Preface

The 32nd International Colloquium on Automata, Languages and Programming (ICALP 2005) was held in Lisbon, Portugal from July 11 to July 15, 2005. These proceedings contain all contributed papers presented at ICALP 2005, together with the papers by the invited speakers Giuseppe Castagna (ENS), Leonid Libkin (Toronto), John C. Mitchell (Stanford), Burkhard Monien (Paderborn), and Leslie Valiant (Harvard). The program had an additional invited lecture by Adi Shamir (Weizmann Institute) which does not appear in these proceedings.

ICALP is a series of annual conferences of the European Association for Theoretical Computer Science (EATCS). The first ICALP took place in 1972. This year, the ICALP program consisted of the established track A (focusing on algorithms, automata, complexity and games) and track B (focusing on logic, semantics and theory of programming), and innovated on the structure of its traditional scientific program with the inauguration of a new track C (focusing on security and cryptography foundation).

In response to a call for papers, the Program Committee received 407 submissions, 258 for track A, 75 for track B and 74 for track C. This is the highest number of submitted papers in the history of the ICALP conferences. The Program Committees selected 113 papers for inclusion in the scientific program. In particular, the Program Committee for track A selected 65 papers, the Program Committee for track B selected 24 papers, and the Program Committee for track C selected 24 papers. All the work of the Program Committees was done electronically.

ICALP 2005 was held in conjunction with the Annual ACM International Symposium on Principles and Practice of Declarative Programming (PPDP 2005). Additionally, the following workshops were held as satellite events of ICALP 2005: the 2nd Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA), the 1st International Workshop on Verification of COncurrent Systems with dynaMIC Allocated Heaps (COSMICAH), the 1st International Workshop on New Developments in Computational Models (DCM), the 4th International Workshop on Parallel and Distributed Methods in Verification (PDMC), the 4th International Workshop on Proof Theory, Computation, Complexity (PCC), the Workshop on Structures and Deduction — The Quest for the Essence of Proofs (DS), the 2nd Workshop on Structural Operational Semantics (SOS), and the Workshop on Semigroups and Automata (WSA).

We wish to thank all authors who submitted papers for consideration, the Program Committees for their hard work, as well as the external reviewers who assisted the Program Committees in the evaluation process.

We thank the sponsors and the Gulbenkian Foundation of Lisbon for hosting ICALP 2005. We are also grateful to the Department of Informatics of the

Faculty of Sciences and Technology, New University of Lisbon, in particular the administrative office and the technical support service.

Last but not least, we would like to thank Andrei Voronkov for providing the conference management software EasyChair. It was of great help in handling the submissions and the electronic PC meeting.

Luís Caires
Giuseppe F. Italiano
Luís Monteiro
Catuscia Palamidessi
Moti Yung

# Organization

## Program Committee

### Track A

Lars Arge, Duke University, USA
Giorgio Ausiello, University of Rome "La Sapienza", Italy
Surender Baswana, Max-Planck-Institut für Informatik, Saarbrücken, Germany
Hans Bodlaender, University of Utrecht, The Netherlands
Véronique Bruyère, University of Mons-Hainaut, Belgium
Adam Buchsbaum, AT&T Labs Research, USA
Josep Diaz, Universitat Politècnica de Catalunya, Spain
David Eppstein, University of Irvine, USA
Andrew Goldberg, Microsoft, USA
Monika Henzinger, Google and ETH Lausanne, Switzerland
Giuseppe F. Italiano, University of Rome "Tor Vergata", Italy (Chair)
Marios Mavronicolas, University of Cyprus, Cyprus
Peter Bro Miltersen, University of Aarhus, Denmark
Mike Paterson, University of Warwick, UK
Dominique Perrin, Université de Marne la Vallée, France
Seth Pettie, Max-Planck-Institut für Informatik, Saarbrücken, Germany
Yuval Rabani, Technion, Israel
Antonio Restivo, University of Palermo, Italy
José Rolim, University of Geneva, Switzerland
Dorothea Wagner, University of Karlsruhe, Germany
Tandy Warnow, University of Texas at Austin, USA
Christos Zaroliagis, CTI and University of Patras, Greece

### Track B

Kenichi Asai, Ochanomizu University, Japan
Jos Baeten, Eindhoven University of Technology, The Netherlands
Peter Buneman, University of Edinburgh, UK
Zoltan Esik, University of Szeged, Hungary and Rovira University, Spain
Javier Esparza, University of Stuttgart, Germany
Marcelo Fiore, Christ's College and University of Cambridge, UK
Manuel Hermenegildo, Universidad Politècnica de Madrid, Spain
Delia Kesner, Université Paris VII, France
Kim Guldstrand Larsen, University of Aalborg, Denmark
Gopalan Nadathur, University of Minnesota, USA

Uwe Nestmann, EPFL, Switzerland
Catuscia Palamidessi, INRIA, France (Chair)
Amr Sabry, University of Indiana, USA
Davide Sangiorgi, Università di Bologna, Italy
Roberto Segala, Università di Verona, Italy
Harald Søndergaard, University of Melbourne, Australia

## Track C

David Basin, ETH Zurich, Switzerland
Christian Cachin, IBM Research, Switzerland
Alfredo De Santis, Università di Salerno, Italy
Cynthia Dwork, Microsoft Research, USA
Matt Franklin, U.C. Davis, USA
Michael Goodrich, U.C. Irvine, USA
Andrew D. Gordon, Microsoft Research, UK
Roberto Gorrieri, Università di Bologna, Italy
Yuval Ishai, Technion, Israel
Phil MacKenzie, DoCoMo Labs, USA
Tatsuaki Okamoto, NTT Labs, Japan
David Pointcheval, ENS Paris, France
Tal Rabin, IBM Research, USA
Omer Reingold, Weizmann Institute, Israel
Adi Rosen, Technion, Israel
Amit Sahai, UCLA, USA
Andre Scedrov, University of Pennsylvania, USA
Igor Shparlinski, Macquarie University, Australia
Nigel Smart, University of Bristol, UK
Moti Yung, Columbia University and RSA Laboratories, USA (Chair)

## Organizing Committee

Luís Caires, Conference Co-chair
Luís Monteiro, Conference Co-chair
António Ravara, Workshops Co-chair
Vasco Vasconcelos, Workshops Co-chair
Margarida Mamede
João Costa Seco
José Pacheco

# List of External Referees

## Track A

Karen Aardal
Scott Aaronson
Saurabh Aggarwal
Marjan van den Akker
Cyril Allauzen
Jean-Paul Allouche
Luca Allulli
Carme Alvarez
Andris Ambainis
Marcella Anselmo
Sanjeev Arora
Albert Atserias
Vincenzo Auletta
Jose Balcazar
Jeremy Barbay
Amotz Bar-Noy
Tugkan Batu
Michael Baur
Marie-Pierre Béal
Luca Becchetti
Philip Bille
Yvonne Bleischwitz
Maria J. Blesa
Avrim Blum
Luc Boasson
Vincenzo Bonifaci
Paola Bonizzoni
Vasco Brattka
Gerth Stølting Brodal
Peter Buergisser
Harry Buhrman
Luciana S. Buriol
Costas Busch
Cristian S. Calude
Massimiliano Caramia
Jean Cardinal
Olivier Carton
Patrick Cegielski
Julien Cervelle
J.-M. Champarnaud
Sunil Chandran
Moses Charikar
Hubie Chen
Joseph Cheriyan
Janka Chlebikova
Bogdan Chlebus
Christian Choffrut
George Christodoulou
Serafino Cicerone
Julien Clément
Andrea Clementi
Eric de La Clergerie
Bruno Codenotti
Edith Cohen
Anne Condon
Pier Francesco Cortese
Stefano Crespi-Reghizzi
Peter Damaschke
Fabrizio d'Amore
Camil Demetrescu
Kedar Dhamdhere
Christoph Dorr
Petros Drineas
Christoph Durr
Stephan Eidenbenz
Amr Elmasry
Thomas Erlebach
Alex Fabrikant
Rolf Fagerberg
Jacques Farré
Lene Favrholdt
Rainer Feldmann
Stephen A. Fenner
Antonio Fernandez
Henning Fernau
Paolo Ferragina
Jiri Fiala
Irene Finocchi
Fedor Fomin
Lance Fortnow
Dimitris Fotakis
Paolo G. Franciosa
Gudmund Frandsen
Alan Frieze
Andrea Frosini
Marco Gaertler
Martin Gairing
Emden Gansner
Naveen Garg
William Ian Gasarch
Leszek Gasieniec
Georgiadis Georgios
Kostis Georgiou
Arkadeb Ghosal
Dora Giammarresi
Raffaele Giancarlo
Aristides Gionis
Ashish Goel
Paul Golberg
Robert Görke
Fabrizio Grandoni
Serge Grigorieff
Alexander Grigoriev
Joachim Gudmundsson
Rachid Guerraoui
Dan Gusfield
Gus Gutoski
M. Hajiaghayi
Magnus M. Halldorsson
Kristoffer Hansen
Sariel Har-Peled
Ramesh Hariharan
Herman Haverkort
Illya V. Hicks
Mika Hirvensalo
John Hitchcock
Martin Holzer
Han Hoogeveen
Peter Hoyer
Juraj Hromkovic
Cor Hurkens
Lucian Ilie
Costas Iliopoulos

Piotr Indyk
Garud Iyengar
Kamal Jain
Petr Jančar
Klaus Jansen
Mark Jerrum
David Johnson
Adrian Johnstone
Marcin Jurdzinski
Erich Kaltofen
Juhani Karhumäki
Anna Karlin
Marek Karpinski
Claire Kenyon
Richard Kenyon
Iordanis Kerenidis
Leonid Khachiyan
Rohit Khandekar
Pekka Kilpelainen
Lefteris Kirousis
Ralf Klasing
Rolf Klein
Bettina Klinz
Adam Klivans
Pascal Koiran
Jochen Konemann
Spyros Kontogiannis
Guy Kortsarz
Arie Koster
Manolis Koubarakis
Elias Koutsoupias
Daniel Kral
Evangelos Kranakis
Dieter Kratsch
Michael Krivelevich
Ravi Kumar
Viraj Kumar
Dietrich Kuske
Shay Kutten
Gregory Lafitte
Jens Lagergren
Sophie Laplante
Michel Latteux
Luigi Laura
Van Bang Le
Thierry Lecroq
Stefano Leonardi
Pierre Leone
Xiang-Yang Li
Paolo Liberatore
Christian Liebchen
Michael Loizos
Thomas Luecking
George Lueker
Alejandro Maas
Marina Madonia
Malik Magdon-Ismail
Frederic Magniez
Mohammad Mahdian
Christos Makris
Sebastian Maneth
Alberto Spaccamela
Maurice Margenstern
Vangelis Markakis
Chip Martel
Giancarlo Mauri
Jacques Mazoyer
Pierre McKenzie
Frank McSherry
Steffen Mecke
Dieter van Melkebeek
Carlo Mereghetti
Wolfgang Merkle
Ramgopal Mettu
Ulrich Meyer
Dimitrios Michail
Christian Michaux
Filippo Mignosi
Vahab Mirrokni
Michael Mitzenmacher
Shuichi Miyazaki
Kousha MoaveniNejad
Mehryar Mohri
Burkhard Monien
Cris Moore
Shlomo Moran
Burkhard Morgenstern
Kenichi Morita
Gabriel Moruz
Thomas Moscibroda
Philippe Moser
Anca Muscholl
Umberto Nanni
Konstantinos Nedas
Mark-Jan Nederhof
Jaroslav Nesetril
Frank Neven
Sotiris Nikoletseas
John Noga
Rasmus Pagh
Jakob Illeborg Pagter
Rina Panigrahy
Anindya Patthak
Christian N.S. Pedersen
David Peleg
Sriram Pemmaraju
Giovanni Pighizzini
Jean-Eric Pin
Giuseppe Pirillo
Nadia Pisanti
Andrzej Proskurowski
J. Radhakrishnan
Harald Raecke
Mathieu Raffinot
Srinivasa Rao
David Rappaport
Jean-François Raskin
S.S. Ravi
John Reif
Jan Reimann
Omer Reingold
Eric Rémila
Christophe Reutenauer
Michel Rigo
Adi Rosen
Martin Rotteler
Tim Roughgarden
Gilles Roussel
Alexander Russell
Jacques Sakarovitch
Peter Sanders
Pierluigi San Pietro
Miklos Santha
Martin Sauerhoff
Guido Schaefer

Thomas Schank
Christian Schindelhauer
Torsten Schlieder
Anita Schöbel
Sylvain Schmitz
Étienne Schramm
Frank Schulz
Elizabeth Scott
Luc Segoufin
Helmut Seidl
Pranab Sen
Géraud Sénizergues
Maria Serna
Rocco Servedio
Jeffrey Shallit
Micha Sharir
Peter Shor
Riccardo Silvestri
Alistair Sinclair
Spiros Skiadopoulos
Martin Skutella
Roberto Solis-Oba
Robert Spalek
Klaus Ambos Spies
Paul Spirakis
Venkatesh Srinivasan
Ludwig Staiger
Yannis Stamatiou
Cliff Stein
David Steurer
Leen Stougie
Howard Straubing
Martin Strauss
K.S. Sudeep
Peng Sun
Maxim Sviridenko
Mario Szegedy
Claude Tadonki
Kunal Talwar
Gerard Tel
Dimitrios Thilikos
Wolfgang Thomas
Karsten Tiemann
Luca Trevisan
Panayiotis Tsaparas
Kostas Tsichlas
Marc Uetz
Ugo Vaccaro
Kasturi Varadarajan
Vijay V. Vazirani
S. Venkatasubramanian
Adrian Vetta
Eric Vigoda
Emanuele Viola
Rakesh V. Vohra
Heribert Vollmer
Nicolai Vorbjov
Osamu Watanabe
Pascal Weil
Klaus Wich
Peter Widmayer
Jef Wijsen
Gerhard Woeginger
Alexander Wolff
Deng Xiaotie
Hiroaki Yamamoto
Mihalis Yannakakis
Norbert Zeh
Li Zhang
Wieslaw Zielonka
Uri Zwick

**Track B**

Elvira Albert
Thorsten Altenkirch
Rajeev Alur
Sergio Antoy
André Arnold
Benjamin Aziz
Brian Babcock
James Bailey
Vincent Balat
José Balcázar
Michael Baldamus
Jiri Barnat
Gerd Behrmann
Martin Berger
Jan Bergstra
Luca Bianco
Lars Birkedal
Frédéric Blanqui
Benedikt Bollig
Johannes Borgström
Dragan Bošnački
Debora Botturi
Ahmed Bouajjani
Patricia Bouyer
Julian Bradfield
Mario Bravetti
Franck van Breugel
Sébastien Briais
Geoffrey Brown
Glenn Bruns
Antonio Bucciarelli
Francisco Bueno
Nadia Busi
Luís Caires
Cristiano Calcagno
Manuel Campagnolo
Manuel Carro
D. Caucal
Witold Charatonik
Krishnendu Chatterjee
Chiyan Chen
James Cheney
Tom Chothia
Horatiu Cirstea
Rance Cleaveland
John Cochran
Thomas Colcombet
Andrea Corradini
Flavio Corradini
Alin Deutsch
Silvano Dal-Zilio
Vincent Danos
Alexandre David
Anuj Dawar

Soeren Debois
Yuxin Deng
M. Dezani-Ciancaglini
Volker Diekert
Rachid Echahed
Norm Ferns
Thomas Hildebrandt
Matthew Flatt
Cédric Fournet
Michael Franssen
Fabio Gadducci
Jacques Garrigue
Floris Geerts
Blaise Genest
Dan R. Ghica
Rob van Glabbeek
Patrice Godefroid
Jan Friso Groote
Sudipto Guha
Vesa Halava
James Harland
Russ Harmer
Tobias Heindel
Holger Hermanns
Thomas Hildebrandt
Kees Huizing
Hans Hüttel
Atsushi Igarashi
Jacob Illum Rasmussen
Anna Ingólfsdóttir
Radha Jagadeesan
Achim Jung
Marcin Jurdziński
Yukiyoshi Kameyama
Deepak Kapur
Claude Kirchner
Christoph Koch
Simon Kramer
Antonín Kučera
Werner Kuich
Ruurd Kuiper
K. Narayan Kumar
Orna Kupferman
Marcos Kurban
Martin Kutrib

Barbara König
Salvatore La Torre
Daniel Leivant
Stéphane Lengrand
Michael Leuschel
Leonid Libkin
Didier Lime
Jim Lipton
Kamal Lodaya
Markus Lohrey
Pedro López
Etienne Lozes
Michael Luttenberger
Bas Luttik
Angelika Mader
A. Maggiolo Schettini
Istvan Majzik
Luc Maranget
Julio Mariño
Hidehiko Masuhara
Sjouke Mauw
Guy McCusker
Paul-André Melliès
Michael Mendler
Massimo Merro
Dale Miller
Kevin Millikin
Alexandre Miquel
Alberto Momigliano
Madhavan Mukund
Anca Muscholl
Anders Møller
Francesco Zappa Nardelli
Damian Niwinski
Dirk Nowotka
Jan Obdržálek
Martin Otto
Matthew Parkinson
Justin Pearson
Simon Peyton Jones
Frank Pfenning
Iain Phillips
Sophie Pinchinat
G. Michele Pinna
François Pottier

Marc Pouzet
John Power
Germán Puebla
Jean-François Raskin
Anders Ravn
Henrik Reif Andersen
Didier Rémy
Eike Ritter
Francesca Rossi
Wojciech Rytter
Jean-Paul Sansonnet
Vijay Saraswat
Stefan Schwoon
Géraud Senizergues
Natalia Sidorova
Petr Sosik
Jeremy Sproston
Jiri Srba
Graham Steel
Martin Steffen
Colin Stirling
Oldřich Stražovský
Martin Strecker
Thomas Streicher
Martin Sulzmann
Stephanie Swerich
Paulo Tabuada
Vanessa Teague
P.S. Thiagarajan
Hayo Thielecke
Marc Tommasi
Lorenzo Tortora de Falco
Frank D. Valencia
Dirk Van Gucht
Daniele Varacca
Helmut Veith
Bob Veroff
Alicia Villanueva
Erik de Vink
Walter Vogler
Marc Voorhoeve
Jérôme Vouillon
Roel de Vrijer
David S. Warren
Hiroshi Watanabe

Stephanie Weirich
Joe Wells
J. Winkowski
Anthony Wirth
James Worrell
Eric Van Wyk
Hongwei Xi
Alexander Yakhnis
Mihalis Yannakakis
Dachuan Yu
Hans Zantema
Marc Zeitoun
Wieslaw Zielonka
Pascal Zimmer

**Track C**

Martín Abadi
Michel Abdalla
Alessandro Acquisti
Saurabh Agarwal
Alessandro Aldini
Giuseppe Ateniese
Michael Backes
Zuzana Beerliova
Kamel Bentahar
Carlo Blundo
Marcello Bonsangue
Xavier Boyen
Marzia Buscemi
Jan Camenisch
Marco Carbone
Dario Catalano
Qi Cheng
Jung Hee Cheon
Mika Cohen
Hubert Comon-Lundh
Scott Contini
Nicolas Courtois
Silvia Crafa
Paolo D'Arco
Stephanie Delaune
Giovanni Di Crescenzo
Pierpaolo Degano
Christophe Doche
Seiji Doi
Paul Hankes Drielsma
Claudiu Duma
Orr Dunkelman
Antonio Durante
Sandro Etalle
Pooya Farshim
Serge Fehr
Sebastian Fischmeister
Riccardo Focardi
Pierre-Alain Fouque
Cédric Fournet
Jessica Fridrich
Martin Gagne
Steven Galbraith
Pierrick Gaudry
Rosario Gennaro
Craig Gentry
Rob Granger
Claudio Guidi
Shai Halevi
Amir Herzberg
Omer Horvitz
Markus Jakobsson
Marc Joye
Bruce Kapron
Hartmut Klauck
Ralf Kuesters
Sebastien Kunz-Jacques
Eyal Kushilevitz
Peeter Laud
Kristin Lauter
Peter Leadbitter
Shiyong Lu
Ben Lynn
Anna Lysyanskaya
Matteo Maffei
Toshiaki Makita
John Malone-Lee
Heiko Mantel
Barbara Masucci
Alexander May
Willi Meier
Phong Nguyen
Jesper Buus Nielsen
Kobbi Nissim
Dan Page
Enes Pasalic
Rafael Pass
Kenny Paterson
Manas Patra
Erez Petrank
Duong Hieu Phan
Krzysztof Pietrzak
Benny Pinkas
Alexander Pretschner
Zulfikar Ramzan
Oded Regev
Leonid Reyzin
Mike Roe
Alon Rosen
Sabina Rossi
Michael Scott
Andrei Serjantov
Ronen Shaltiel
Vitaly Shmatikov
Christoph Sprenger
Martijn Stam
Pante Stanica
Ron Steinfeld
Jacques Stern
Koutarou Suzuki
Tamir Tassa
Yael Tauman-Kalai
Luca Trevisan
A. Troina
Luca Vigano
Ivan Visconti
Bogdan Warinschi
Brent Waters
Diego Zamboni

## Sponsors

Fundação para a Ciência e Tecnologia, Ministério da Ciência e Ensino Superior
Centro de Informática e Tecnologias da Informação/FCT/UNL
Centro de Lógica e Computação/IST/UTL

# Table of Contents

## Invited Lectures

Holographic Circuits
*Leslie G. Valiant* ..... 1

Probabilistic Polynomial-Time Semantics for a Protocol Security Logic
*Anupam Datta, Ante Derek, John C. Mitchell, Vitaly Shmatikov, Mathieu Turuani* ..... 16

A Gentle Introduction to Semantic Subtyping
*Giuseppe Castagna, Alain Frisch* ..... 30

Logics for Unranked Trees: An Overview
*Leonid Libkin* ..... 35

Nash Equilibria, the Price of Anarchy and the Fully Mixed Nash Equilibrium Conjecture
*Martin Gairing, Thomas Lücking, Burkhard Monien, Karsten Tiemann* ..... 51

## Data Structures I

The Tree Inclusion Problem: In Optimal Space and Faster
*Philip Bille, Inge Li Gørtz* ..... 66

Union-Find with Constant Time Deletions
*Stephen Alstrup, Inge Li Gørtz, Theis Rauhe, Mikkel Thorup, Uri Zwick* ..... 78

Optimal In-place Sorting of Vectors and Records
*Gianni Franceschini, Roberto Grossi* ..... 90

Towards Optimal Multiple Selection
*Kanela Kaligosi, Kurt Mehlhorn, J. Ian Munro, Peter Sanders* ..... 103

## Cryptography and Complexity

Simple Extractors via Constructions of Cryptographic Pseudo-random Generators
*Marius Zimand* ..... 115

Bounds on the Efficiency of "Black-Box" Commitment Schemes
*Omer Horvitz, Jonathan Katz* ..... 128

On Round-Efficient Argument Systems
*Hoeteck Wee* ..... 140

Computational Bounds on Hierarchical Data Processing with Applications to Information Security
*Roberto Tamassia, Nikos Triandopoulos* ..... 153

## Data Structures II

Balanced Allocation and Dictionaries with Tightly Packed Constant Size Bins
*Martin Dietzfelbinger, Christoph Weidling* ..... 166

Worst Case Optimal Union-Intersection Expression Evaluation
*Ehsan Chiniforooshan, Arash Farzan, Mehdi Mirzazadeh* ..... 179

Measure and Conquer: Domination – A Case Study
*Fedor V. Fomin, Fabrizio Grandoni, Dieter Kratsch* ..... 191

## Cryptography and Distributed Systems

Optimistic Asynchronous Atomic Broadcast
*Klaus Kursawe, Victor Shoup* ..... 204

Asynchronous Perfectly Secure Communication over One-Time Pads
*Giovanni Di Crescenzo, Aggelos Kiayias* ..... 216

Single-Prover Concurrent Zero Knowledge in Almost Constant Rounds
*Giuseppe Persiano, Ivan Visconti* ..... 228

## Graph Algorithms I

LCA Queries in Directed Acyclic Graphs
*Miroslaw Kowaluk, Andrzej Lingas* ..... 241

Replacement Paths and $k$ Simple Shortest Paths in Unweighted Directed Graphs
*Liam Roditty, Uri Zwick* ..... 249

Deterministic Constructions of Approximate Distance Oracles and Spanners
*Liam Roditty, Mikkel Thorup, Uri Zwick* ..... 261

An $\tilde{O}(m^2n)$ Randomized Algorithm to Compute a Minimum Cycle Basis of a Directed Graph
*Telikepalli Kavitha* ..... 273

## Security Mechanisms

Basing Cryptographic Protocols on Tamper-Evident Seals
*Tal Moran, Moni Naor* ..... 285

Hybrid Trapdoor Commitments and Their Applications
*Dario Catalano, Ivan Visconti* ..... 298

On Steganographic Chosen Covertext Security
*Nicholas Hopper* ..... 311

Classification of Boolean Functions of 6 Variables or Less with Respect to Some Cryptographic Properties
*An Braeken, Yuri Borissov, Svetla Nikova, Bart Preneel* ..... 324

## Graph Algorithms II

Label-Guided Graph Exploration by a Finite Automaton
*Reuven Cohen, Pierre Fraigniaud, David Ilcinkas, Amos Korman, David Peleg* ..... 335

On the Wake-Up Problem in Radio Networks
*Bogdan S. Chlebus, Leszek Gąsieniec, Dariusz R. Kowalski, Tomasz Radzik* ..... 347

Distance Constrained Labelings of Graphs of Bounded Treewidth
*Jiří Fiala, Petr A. Golovach, Jan Kratochvíl* ..... 360

Optimal Branch-Decomposition of Planar Graphs in $O(n^3)$ Time
*Qian-Ping Gu, Hisao Tamaki* ..... 373

## Automata and Formal Languages I

NFAs With and Without $\varepsilon$-Transitions
*Juraj Hromkovič, Georg Schnitger* ..... 385

On the Equivalence of $\mathbb{Z}$-Automata
*Marie-Pierre Béal, Sylvain Lombardy, Jacques Sakarovitch* ..... 397

A Tight Linear Bound on the Neighborhood of Inverse Cellular Automata
*Eugen Czeizler, Jarkko Kari* ..... 410

Groupoids That Recognize Only Regular Languages
*Martin Beaudry, François Lemieux, Denis Thérien* ..... 421

## Signature and Message Authentication

Append-Only Signatures
*Eike Kiltz, Anton Mityagin, Saurabh Panjwani, Barath Raghavan* .... 434

Hierarchical Group Signatures
*Mårten Trolin, Douglas Wikström* ..... 446

Designated Verifier Signature Schemes: Attacks, New Security Notions and a New Construction
*Helger Lipmaa, Guilin Wang, Feng Bao* ..... 459

Single-Key AIL-MACs from Any FIL-MAC
*Ueli Maurer, Johan Sjödin* ..... 472

## Algorithmic Game Theory

The Efficiency and Fairness of a Fixed Budget Resource Allocation Game
*Li Zhang* ..... 485

Braess's Paradox, Fibonacci Numbers, and Exponential Inapproximability
*Henry Lin, Tim Roughgarden, Éva Tardos, Asher Walkover* ..... 497

## Automata and Logic

Weighted Automata and Weighted Logics
*Manfred Droste, Paul Gastin* ..... 513

Restricted Two-Variable FO + MOD Sentences, Circuits and Communication Complexity
*Pascal Tesson, Denis Thérien* ..... 526