

---

# EXPLORING NEW FRONTIERS OF THEORETICAL INFORMATICS

## **IFIP – The International Federation for Information Processing**

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

*IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.*

IFIP is a non-profit making organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

# EXPLORING NEW FRONTIERS OF THEORETICAL INFORMATICS

*IFIP 18th World Computer Congress  
TC1 3rd International Conference on  
Theoretical Computer Science (TCS2004)  
22–27 August 2004  
Toulouse, France*

Edited by

**Jean-Jacques Levy**  
*INRIA, France*

**Ernst W. Mayr**  
*Technische Universität München, Germany*

**John C. Mitchell**  
*Stanford University, USA*

**KLUWER ACADEMIC PUBLISHERS**  
NEW YORK, BOSTON, DORDRECHT, LONDON, MOSCOW

eBook ISBN: 1-4020-8141-3  
Print ISBN: 1-4020-8140-5

©2004 Springer Science + Business Media, Inc.

Print ©2004 by International Federation for Information Processing.  
Boston

All rights reserved

No part of this eBook may be reproduced or transmitted in any form or by any means, electronic, mechanical, recording, or otherwise, without written consent from the Publisher

Created in the United States of America

Visit Springer's eBookstore at:  
and the Springer Global Website Online at:

<http://www.ebooks.kluweronline.com>  
<http://www.springeronline.com>

CONTENTS

Preface ..... xi  
Program Committee..... xiii

Invited talks

The tPI (tRNA Pairing Index), a Mathematical Measure of  
Repetition in a (Biological) Sequence  
*Gaston Gonnet* ..... 1

Stability of Approximation in Discrete Optimization  
*Juraj Hromkovič* ..... 3

Towards a Broader Theory of Mobile Processes  
*Robin Milner*..... 19

A Decidable Analysis of Security Protocols  
*Michael Rusinowitch* .....21

Track (1) on Algorithms, Complexity, and  
Models of Computation

Looking Inside AES and BES  
*Ilia Toli, Alberto Zanoni* .....23

Remove Key Escrow from The Identity-Based Encryption System  
*Zhaohui Cheng, Richard Comley, Luminita Vasiliu* .....37

A Randomised Algorithm for Checking the Normality of Cryptographic Boolean Functions <i>An Braeken, Christopher Wolf, Bart Preneel</i> .....	51
Reversible Circuit Realizations of Boolean Functions <i>Alex Brodsky</i> .....	67
Resource Bounded Immunity and Simplicity <i>Toshio Suzuki, Tomoyuki Yamakami</i> .....	81
Degree Bounds on Polynomials and Relativization Theory <i>Holger Spakowski, Rahul Tripathi</i> .....	97
The Firing Squad Synchronization Problem with Many Generals For One-Dimensional CA <i>Hubert Schmid, Thomas Worsch</i> .....	111
A Matrix $q$ -Analogue of the Parikh Map <i>Omer Egecioglu, Oscar Ibarra</i> .....	125
The Inherent Queuing Delay of Parallel Packet Switches <i>Hagit Attiya, David Hay</i> .....	139
Efficient Protocols for Computing the Optimal Swap Edges of a Shortest Path Tree <i>Paola Flocchini, Antonio Mesa Enriques, Linda Pagli, Giuseppe Prencipe, Nicola Santoro</i> .....	153
Truthful Mechanisms for Generalized Utilitarian Problems <i>Giovanna Melideo, Paolo Penna, Guido Proietti, Roger Wattenhofer, Peter Widmayer</i> .....	167
The Driving Philosophers <i>Sébastien Baehni, Roberto Baldoni, Rachid Guerraoui, Bastian Pochon</i> .....	181
Engineering an External Memory Minimum Spanning Tree Algorithm <i>Roman Dementiev, Peter Sanders, Dominik Schultes, Jop Sibeyn</i> .....	195

Scheduling with Release Times and Deadlines on a Minimum Number of Machines <i>Mark Cieliebak, Thomas Erlebach, Fabian Hennecke, Birgitta Weber, Peter Widmayer</i> .....	209
Approximation Algorithms for Mixed Fractional Packing and Covering Problems <i>Klaus Jansen</i> .....	223
On Weighted Rectangle Packing with Large Resources <i>Aleksei V. Fishkin, Olga Gerber, Klaus Jansen</i> .....	237
An $O(n \log^2 n)$ Algorithm for the Optimal Sink Location Problem in Dynamic Tree Networks <i>Satoko Mamada, Takeaki Uno, Kazuhisa Makino, Satoru Fujishige</i> .....	251
Efficient Algorithms for Handling Molecular Weighted Sequences <i>Costas S. Iliopoulos, Christos Makris, Yannis Panagis, Katerina Perdikuri, Evangelos Theodoridis, Athanasios Tsakalidis</i> .....	265
Imperfectness of Data for STS-Based Physical Mapping <i>Hiro Ito, Kazuo Iwama, Takeyuki Tamura</i> .....	279
Solving Packing Problem with Weaker Block Solvers <i>Hu Zhang</i> .....	293
Adaptive Sorting with AVL Trees <i>Amr A. Elmasry</i> .....	307
Precise Analysis of $\pi$ -Calculus in Cubic Time <i>Livio Colussi, Gilberto Filè, A. Griggio</i> .....	317
<b>Track (2) on Logic, Semantics, Specification, and Verification</b>	
Prototyping Proof Carrying Code <i>Martin Wildmoser, Tobias Nipkow, Gerwin Klein, Sebastian Nanz</i> .....	333
Contract Oriented Development of Component Software <i>Zhiming Liu, He Jifeng, Xiaoshan Li</i> .....	349

New Insights on Architectural Connectors <i>Roberto Bruni, José Luiz Fiadeiro, Ivan Lanese, Antónia Lopes, Ugo Montanari</i> .....	367
On Complexity of Model-Checking for the TQL Logic <i>Iovka Boneva, Jean-Marc Talbot</i> .....	381
A Generic Framework for Checking Semantic Equivalences between Pushdown Automata and Finite-State Automata <i>Antonín Kučera, Richard Mayr</i> .....	395
Tailoring Recursion to Characterize Non-Deterministic Complexity Classes over Arbitrary Structures <i>Olivier Bournez, Felipe Cucker, Paulin Jacobé de Naurois, Jean-Yves Marion</i> .....	409
A Calculus with Lazy Module Operators <i>Davide Ancona, Sonia Fagorzi, Elena Zucca</i> .....	423
Dynamic Typing with Dependent Types <i>Xinming Ou, Gang Tan, Yitzhak Mandelbaum, David Walker</i> .....	437
Subtyping-Inheritance Conflicts: The Mobile Mixin Case <i>Lorenzo Bettini, Viviana Bono, Betti Venneri</i> .....	451
Asymptotic Behaviors of Type-2 Algorithms and Induced Baire Topologies <i>Chung-Chih Li</i> .....	465
Effective Chemistry for Synchrony and Asynchrony <i>Deepak Garg, Akash Lal, Sanjiva Prasad</i> .....	479
Controller Synthesis for Probabilistic Systems <i>Christel Baier, Marcus Groesser, Martin Leucker, Benedikt Bollig, Frank Ciesinski</i> .....	493
Highly Undecidable Questions for Process Algebras <i>Petr Jančar, Jiří Srba</i> .....	507



New-HOPLA: A Higher-order Process Language with Name Generation <i>Glynn Winskel, Francesco Zappa Nardelli</i> .....	521
Behavioural Equivalences for Dynamic Web Data <i>Sergio Maffei, Philippa Gardner</i> .....	535
Behavioural Theory for Mobile Ambients <i>Massimo Merro, Francesco Zappa Nardelli</i> .....	549
Nested Commits for Mobile Calculi: Extending Join <i>Roberto Bruni, Hernán C. Melgratti, Ugo Montanari</i> .....	563
Dynamic and Local Typing for Mobile Ambients <i>Mario Coppo, Mariangiola Dezani-Ciancaglini, Elio Giovannetti, Rosario Pugliese</i> .....	577
PolyA: True Type Polymorphism for Mobile Ambients <i>Torben Amtoft, Henning Makholm, J. B. Wells</i> .....	591
Recovering Resources in the $\pi$ -calculus <i>David Teller</i> .....	605
Ensuring Termination by Typability <i>Yuxin Deng, Davide Sangiorgi</i> .....	619
The Simply-typed Pure Pattern Type System Ensures Strong Normalization <i>Benjamin Wack</i> .....	633
Termination in Modal Kleene Algebra <i>Jules Desharnais, Bernhard W. Möller, Georg Struth</i> .....	647
Regular Tree Language Recognition with Static Information <i>Alain Frisch</i> .....	661
Author Index .....	675

# PREFACE

IFIP TCS 2004 is the third international conference organized by IFIP TC1, whose activities cover the entire field of theoretical computer science. The major topics of the conference were chosen reflecting the current activities in theoretical computer science forming the two tracks:

Track (1) on Algorithms, Complexity, and Models of Computation,  
Track (2) on Logic, Semantics, Specification, and Verification.

The program of IFIP TCS 2004 included the presentations of twenty-two contributed papers in Track (1) and twenty-four contributed papers in Track (2). The Program Committees selected them from sixty-five submissions to Track (1) and eighty-two submissions to Track (2).

The four plenary invited speakers were chosen by the Steering Committee, the Chair and the PC Co-Chairs.

This volume constitutes the record of the technical program, consisting of the contributed papers and the invited talks. We had the pleasure of chairing the conference and the program committees of the third IFIP International Conference on Theoretical Computer Science. We are extremely grateful to Jean-Claude Laprie and his staff, who helped us in preparing and announcing the call for papers, the program, and the web pages, and in putting together the proceedings.

We would like to express our thanks to the other members of the Program Committees, who are listed below, for their help in reviewing all submissions and for selecting the papers.

Jean-Jacques Lévy  
Chair  
Ernst W. Mayr  
John C. Mitchell  
Co-Chairs

# **PROGRAM COMMITTEE**

## **Track (1) on Algorithms, Complexity, and Models of Computation**

Farid Ablayev (State University, Kazan)  
Hagit Attiya (The Technion, Haifa)  
Stefano Leonardi (Universita di Roma)  
Maurice Margenstern (Université de Metz)  
Ernst Mayr, Chair (Technische Universität München)  
Satoru Miyano (University of Tokyo)  
Jean-Eric Pin (LIAFA CNRS, Paris)  
Nicola Santoro (Carleton University)  
Thomas Schwentick (Philipps-Universität Marburg)  
Sandeep Sen (Indian Institute of Technology Delhi)  
Subhash Suri (University of California Santa Barbara)  
Osamu Watanabe (Tokyo Institute of Technology)

## **Track (2) on Logic, Semantics, Specification, and Verification**

Roberto Amadio (Université de Provence, Marseille)  
Luca Cardelli (Microsoft Research Cambridge)  
Giuseppe Castagna (École Normale Supérieure, Paris)  
Hubert Comon-Lundh (École Normale Supérieure de Cachan)  
Adriana Compagnoni (Stevens Institute of Technology)  
Drew Dean (SRI)  
Marcelo Fiore (University of Cambridge)  
Giorgio Ghelli (Università di Pisa)  
Martin Hofmann (Ludwig-Maximilians-Universität, München)  
Alan Jeffrey (DePaul University)  
Bruce Kapron (University of Victoria)  
Orna Kupferman (Hebrew University)  
John Mitchell, Chair (Stanford University)  
George Necula (University of California Berkeley)  
Catuscia Palamidessi (INRIA Futurs)  
Martin Rinard (MIT)  
Davide Sangiorgi (University of Bologna)

Vladimiro Sassone (University of Sussex)

Vitaly Shmatikov (SRI)

Martin Wirsing (Ludwig-Maximilians-Universität, München)