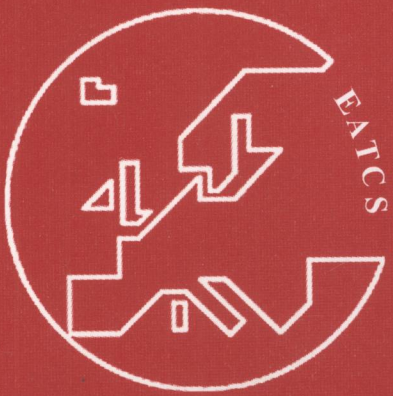
Michele Bugliesi
Bart Preneel
Vladimiro Sassone
Ingo Wegener (Eds.)

LNCS 4052

Automata, Languages and Programming

33rd International Colloquium, ICALP 2006
Venice, Italy, July 2006
Proceedings, Part II

2 Part II



Springer

Michele Bugliesi Bart Preneel
Vladimiro Sassone Ingo Wegener (Eds.)

Automata, Languages and Programming

33rd International Colloquium, ICALP 2006
Venice, Italy, July 10-14, 2006
Proceedings, Part II

Springer

Volume Editors

Michele Bugliesi
Università Ca'Foscari
Dipartimento di Informatica
Via Torino 155, 30172 Venezia-Mestre, Italy
E-mail: bugliesi@dsi.unive.it

Bart Preneel
Katholieke Universiteit Leuven
Department of Electrical Engineering-ESAT/COSIC
Kasteelpark Arenberg 10, 3001 Leuven-Heverlee, Belgium
E-mail: Bart.Preneel@esat.kuleuven.be

Vladimiro Sassone
University of Southampton
School of Electronics and Computer Science
SO17 1BJ, UK
E-mail: vs@ecs.soton.ac.uk

Ingo Wegener
Universität Dortmund
FB Informatik, LS2
Otto-Hahn-Str. 14, 44221 Dortmund, Germany
E-mail: ingo.wegener@uni-dortmund.de

Library of Congress Control Number: 2006928089

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

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-35907-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-35907-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11787006 06/3142 5 4 3 2 1 0

Preface

ICALP 2006, the 33rd edition of the International Colloquium on Automata, Languages and Programming, was held in Venice, Italy, July 10–14, 2006. ICALP is a series of annual conferences of the European Association for Theoretical Computer Science (EATCS) which first 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 of the recently introduced track C (focusing on security and cryptography foundation).

In response to the call for papers, the Program Committee received 407 submissions, 230 for track A, 96 for track B and 81 for track C. Out of these, 109 papers were selected for inclusion in the scientific program: 61 papers for Track A, 24 for Track B and 24 for Track C. The selection was made by the Program Committee based on originality, quality, and relevance to theoretical computer science. The quality of the manuscripts was very high indeed, and several deserving papers had to be rejected.

ICALP 2006 consisted of four invited lectures and the contributed papers. This volume of the proceedings contains all contributed papers presented at the conference in Track A, together with the paper by the invited speaker Noga Alon (Tel Aviv University, Israel). A companion volume contains all contributed papers presented in Track B and Track C together with the papers by the invited speakers Cynthia Dwork (Microsoft Research, USA) and Prakash Panangaden (Mc Gill University, Canada). The program had an additional invited lecture by Simon Peyton Jones (Microsoft Research, UK), which does not appear in the proceedings.

ICALP 2006 was held in conjunction with the Annual ACM International Symposium on Principles and Practice of Declarative Programming (PPDP 2006) and with the Annual Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 2006). Additionally, the following workshops were held as satellite events of ICALP 2006: ALGOSENSORS 2006 - International Workshop on Algorithmic Aspects of Wireless Sensor Networks; CHR 2006 - Third Workshop on Constraint Handling Rules; CL&C 2006 - Classical Logic and Computation; DCM 2006 - 2nd International Workshop on Developments in Computational Models; FCC 2006 - Formal and Computational Cryptography; iETA 2006 - Improving Exponential-Time Algorithms: Strategies and Limitations; MeCBIC 2006 - Membrane Computing and Biologically Inspired Process Calculi; SecReT 2006 - 1st Int. Workshop on Security and Rewriting Techniques; WCAN 2006 - 2nd Workshop on Cryptography for Ad Hoc Networks.

We wish to thank all authors who submitted extended abstracts for consideration, the Program Committee for their scholarly effort, and all referees who assisted the Program Committees in the evaluation process.

Thanks to the sponsors for their support, to the Venice International University and to the Province of Venice for hosting ICALP 2006 in beautiful S. Servolo. We are also grateful to all members of the Organizing Committee in the Department of Computer Science and to the Center for Technical Support Services and Telecommunications (CSITA) of the University of Venice. Thanks to Andrei Voronkov for his support with the conference management software EasyChair. It was great in handling the submissions and the electronic PC meeting, as well as in assisting in the assembly of the proceedings.

April 2006

Michele Bugliesi
Bart Preneel
Vladimiro Sassone
Ingo Wegener

Organization

Program Committee

Track A

Harry Buhrman, University of Amsterdam, The Netherlands
Mark de Berg, TU Eindhoven, The Netherlands
Uriel Feige, Weizmann Institute, Isreal
Anna Gal, University of Texas at Austin, USA
Johan Hastad, KTH Stockholm, Sweden
Edith Hemaspaandra, Rochester Institute of Technology, USA
Kazuo Iwama, Kyoto University, Japan
Mark Jerrum, University of Edinburgh, UK
Stefano Leonardi, Università di Roma, Italy
Friedhelm Meyer auf der Heide, Universität Paderborn, Germany
Ian Munro, University of Waterloo, Canada
Sotiris Nikoletseas, Patras University, Greece
Rasmus Pagh, IT Univerisy of Copenhagen, Denmark
Tim Roughgarden, Stanford University, USA
Jacques Sakarovitch, CRNS Paris, France
Jiri Sgall, Academy of Sciences, Prague, Czech Republic
Hans Ulrich Simon, Ruhr-Universität Bochum, Germany
Alistair Sinclair, University of Berkeley, USA
Angelika Steger, ETH Zürich, Switzerland
Denis Thérien, McGill University, Canada
Ingo Wegener, Universität Dortmund, Germany (Chair)
Emo Welzl, ETH Zurich, Switzerland

Track B

Roberto Amadio, Université Paris 7, France
Lars Birkedal, IT University of Copenhagen, Denmark
Roberto Bruni, Università di Pisa, Italy
Mariangiola Dezani-Ciancaglini, Università di Torino, Italy
Volker Diekert, University of Stuttgart, Germany
Abbas Edalat, Imperial College, UK
Jan Friso Groote, Eindhoven University of Technology, The Nederlands
Tom Henzinger, EPFL, Switzerland
Madhavan Mukund, Chennai Mathematical Institute, India
Jean-Éric Pin, LIAFA, France
Julian Rathke, University of Sussex, UK
Jakob Rehof, Microsoft Research, Redmont, USA

Vladimiro Sassone, University of Southampton, UK (Chair)
Don Sannella, University of Edinburgh, UK
Nicole Schweikardt, Humboldt-Universität zu Berlin, Germany
Helmut Seidl, Technische Universität München, Germany
Peter Selinger, Dalhousie University, Canada
Jerzy Tiuryn, Warsaw University, Poland
Victor Vianu, U. C. San Diego, USA
David Walker, Princeton University, USA
Igor Walukiewicz, Labri, Université Bordeaux, France

Track C

Martín Abadi, University of California at Santa Cruz, USA
Christian Cachin, IBM Research, Switzerland
Ronald Cramer, CWI and Leiden University, The Netherlands
Ivan Damgrd, University of Aarhus, Denmark
Giovanni Di Crescenzo, Telcordia, USA
Marc Fischlin, ETH Zürich, Switzerland
Dieter Gollmann, University of Hamburg-Harburg, Germany
Andrew D. Gordon, Microsoft Research, UK
Aggelos Kiayias, University of Connecticut, USA
Joe Kilian, Rutgers University, USA
Cathy Meadows, Naval Research Laboratory, USA
John Mitchell, Stanford University, USA
Mats Näslund, Ericsson, Sweden
Tatsuaki Okamoto, Kyoto University, Japan
Rafael Ostrovksy, University of California at Los Angeles, USA
Pascal Paillier, Gemplus, France
Giuseppe Persiano, University of Salerno, Italy
Benny Pinkas, HP Labs, Israel
Bart Preneel, Katholieke Universiteit Leuven, Belgium (Chair)
Vitaly Shmatikov, University of Texas at Austin, USA
Victor Shoup, New York University, USA
Jessica Staddon, PARC, USA
Frederik Vercauteren, Katholieke Universiteit Leuven, Belgium

Organizing Committee

Michele Bugliesi, University of Venice (Conference Chair)
Andrea Pietracaprina, University of Padova (Workshop Co-chair)
Francesco Ranzato, University of Padova (Workshop Co-chair)
Sabina Rossi, University of Venice (Workshop Co-chair)
Annalisa Bossi, University of Venice
Damiano Macedonio, University of Venice

Referees

Martín Abadi
Masayuki Abe
Zoe Abrams
Gagan Aggarwal
Mustaq Ahmed
Cagri Aksay
Tatsuya Akutsu
Susanne Albers
Eric Allender
Jean-Paul Allouche
Jesus Almansa
Helmut Alt
Joel Alwen
Andris Ambainis
Elena Andreeva
Spyros Angelopoulos
Elliot Anshelevich
Lars Arge
Stefan Arnborg
Sanjeev Arora
Vincenzo Auletta
Per Austrin
David Avis
Moshe Babaioff
Michael Backes
Evripides Bampis
Nikhil Bansal
Jeremy Barbay
Paulo Baretto
David Barrington
Roman Bartak
Adam Barth
Paul Beame
Luca Becchetti
Amos Beimel
Elizabeth Berg
Robert Berke
Piotr Berman
Thorsten Bernholt
Ivona Bezakova
Laurent Bienvenu
Mathieu Blanchette
Yvonne Bleischwitz
Isabelle Bloch
Avrim Blum
Liad Blumrosen
Alexander Bockmayr
Alexandra Boldyreva
Beate Bollig
Giuseppe Battista
Nicolas Bonichon
Vincenzo Bonifaci
Joan Boyar
An Braeken
Justin Brickell
Patrick Briest
Gerth Brodal
Gerth Stlting Brodal
Gerth S. Brodal
Peter Buergisser
Jonathan Buss
Gruia Calinescu
Christophe De Cannire
Flavio d'Alessandro
Alberto Caprara
Iliano Cervesato
Timothy M. Chan
Pandu Rangan Chandrasekaran
Krishnendu Chatterjee
Arkadev Chattopadhyay
Avik Chaudhuri
Kamalika Chaudhuri
Chandra Chekuri
Zhi-Zhong Chen
Joseph Cheriyan
Benoit Chevallier-Mames
Markus Chimani
Christian Choffrut
Marek Chrobak
Fabian Chudak
David Clarke
Andrea Clementi
Bruno Codenotti
Richard Cole
Scott Contini
Ricardo Corin
Graham Cormode
Jose Correa
Veronique Cortier
Stefano Crespi
Maxime Crochemore
Mary Cryan
Felipe Cucker
Artur Czumaj
Sanjoy Dasgupta
Ccile Delerable
Xiaotie Deng
Jonathan Derryberry
Jean-Louis Dessalles
Nikhil Devanur
Luc Devroye
Florian Diedrich
Martin Dietzfelbinger
Jintai Ding
Irit Dinur
Benjamin Doerr
Eleni Drinea
Petros Drineas
Stefan Droste
Laszlo Egri
Friedrich Eisenbrand
Michael Elkin
Leah Epstein
Kimmo Eriksson
Thomas Erlebach
Peter Gacs
Rolf Fagerberg
Ulrich Faigle
Piotr Faliszewski
Pooya Farshim
Arash Farzan
Serge Fehr
Sandor Fekete
Rainer Feldmann
Stefan Felsner
Coby Fernadess
Paolo Ferragina
Jiri Fiala

Faith Fich
Matthias Fitzi
Abraham Flaxman
Lisa K. Fleischer
Rudolf Fleischer
Fedor Fomin
Lance Fortnow
Pierre Fraignaud
Paolo Franciosa
Matt Franklin
Eiichiro Fujisaki
Satoshi Fujita
Toshihiro Fujito
Stanley Fung
Martin Furer
Jun Furukawa
Martin Frer
Bernd Gaertner
Martin Gairing
Steven Galbraith
Clemente Galdi
G. Ganapathy
Juan Garay
Naveen Garg
Ricard Gavalda
Dmitry Gavinsky
Joachim Gehweiler
Stefanie Gerke
Abhrajit Ghosh
Oliver Giel
Reza Dorri Giv
Andreas Goerdt
Eu-Jin Goh
Leslie Goldberg
Mikael Goldmann
Aline Gouget
Navin Goyal
Gregor Gramlich
Robert Granger
Alexander Grigoriev
Martin Grohe
Andre Gronemeier
Jiong Guo
Ankur Gupta
Anupam Gupta
Venkatesan Guruswami
Inge Li Grtz
Robbert de Haan
Torben Hagerup
Mohammad Taghi Hajiaghayi
Michael Hallett
Dan Halperin
Christophe Hancart
Goichiro Hanaoka
Dan Witzner Hansen
Sariel Har-Peled
Thomas Hayes
Meng He
Lane Hemaspaandra
Javier Herranz
Jan van den Heuvel
Martin Hirt
Michael Hoffmann
Dennis Hofheinz
Thomas Hofmeister
Christopher M. Homan
Hendrik Jan Hoogeboom
Juraj Hromkovic
Shunsuke Inenaga
Piotr Indyk
Yuval Ishai
Toshimasa Ishii
Hiro Ito
Toshiya Itoh
Gabor Ivanyos
Riko Jacob
Jens Jaegerskuepper
Sanjay Jain
Kamal Jain
Klaus Jansen
Thomas Jansen
Jesper Jansson
Stanislaw Jarecki
Wojciech Jawor
David Johnson
Tibor Jordan
Philippe Jorrand
Jan Juerjens
Valentine Kabanets
Jesse Kamp
Sampath Kannan
Haim Kaplan
Sarah Kappes
Bruce Kapron
Juha Karkkainen
Julia Kempe
Johan Karlander
Howard Karloff
Jonahtan Katz
Akinori Kawachi
Claire Kenion
Krishnaram Kenthapadi
Rohit Khandekar
Subhash A. Khot
Samir Khuller
Eike Kiltz
Guy Kindler
Valerie King
Lefteris Kirousis
Daniel Kirsten
Bobby Kleinberg
Adam Klivans
Johannes Koebler
Jochen Koenemann
Petr Kolman
Guy Kortsarz
Michal Koucky
Elias Koutsoupias
Dexter Kozen
Darek Kowalski
Matthias Krause
Hugo Krawczyk
Klaus Kriegel
Alexander Kroeller
Piotr Krysta
Ludek Kucera
Noboru Kunihiro
Eyal Kushilevitz
Minseok Kwon
Shankar Ram Lakshminarayanan
Joseph Lano
Sophie Laplante
Christian Lavault

Ron Lavi
Thierry Lecroq
Troy Lee
Hanno Lefmann
Francois Lemieux
Asaf Levin
Benoit Libert
Christian Liebchen
Andrzej Lingas
Helger Lipmaa
Sylvain Lombardy
Alex Lopez-Ortiz
Zvi Lotker
Laci Lovasz
Chris Luhrs
Rune Bang Lyngs
Peter Mahlmann
John Malone-Lee
Heikki Mannila
Alberto Marchetti-Spaccamela
Martin Marciniszyn
Gitta Marchand
Stuart Margolis
Martin Mares
Russell Martin
Toshimitsu Masuzawa
Jiri Matousek
Giancarlo Mauri
Alexander May
Elvira Mayordomo
Pierre McKenzie
Kurt Mehlhorn
Aranyak Mehta
Nele Mentens
Mark Mercer
Ron van der Meyden
Ulrich Meyer
Peter Bro Miltersen
Dieter Mitsche
Shuichi Miyazaki
Burkhard Monien
Cris Moore
Thomas Moscibroda
Mitsuo Motoki
Ahuva Mu'alem Kamesh Munagala
Ian Munro
Kazuo Murota
Petra Mutzel
Hiroshi Nagamochi
Shin-ichi Nakano
Seffi Naor
Gonzalo Navarro
Frank Neumann
Antonio Nicolosi
Rolf Niedermeier
Jesper Buus Nielsen
Svetla Nikova
Karl Norrman
Dirk Nowotka
Robin Nunkesser
Regina O'Dell
Hirotaka ONO
Mitsunori Ogihara
Kazuo Ohta
Chihiro Ohyama
Yusuke Okada
Yoshio Okamoto
Christopher Okasaki
Ole Østerby
Janos Pach
Anna stlin Pagh
Anna Palbom
Konstantinos Panagiotou
Leon Peeters
Derek Phillips
Toniann Pitassi
Giovanni Pighizzini
Wolf Polak
Pawel Pralat
Pavel Pudlak
Prashant Puniya
Yuri Rabinovich
Jaikumar Radhakrishnan
Stanislaw Radziszowski
Harald Raecke
Prabhakar Ragde
Zia Rahman
S. Raj Rajagopalan
V. Ramachandran
Dana Randall
S. Srinivasa Rao
Ran Raz
Alexander Razborov
Andreas Razen
Ken Regan
Ben Reichardt
Christophe Reutenauer
Eleanor Rieffel
Romeo Rizzi
Martin Roetteler
Phillip Rogaway
Amir Ronen
Dominique Rossin
Peter Rossmanith
Joerg Rothe
Arnab Roy
Leo Ruest
Milan Ruzic
Kunihiko Sadakane
Cenk Sahinalp
Kai Salomaa
Louis Salvail
Peter Sanders
Mark Sandler
Rahul Santhanam
Palash Sarkar
Martin Sauerhoff
Daniel Sawitzki
Nicolas Schabanel
Christian Schaffner
Michael Schapira
Dominik Scheder
Christian Scheideler
Christian Schindelhauer
Katja Schmidt-Samoa
Georg Schnitger
Henning Schnoor
Uwe Schoening
Gunnar Schomaker
Eva Schuberth
Andreas Schulz

Nathan Segerlind
Meinolf Sellmann
Pranab Sen
Hadas Shachnai
Ronen Shaltiel
Abhi Shelat
Bruce Sheppard
Oleg M. Sheyner
David Shmoys
Detlef Sieling
Jiri Sima
Mohit Singh
Naveen Sivadasan
Matthew Skala
Steve Skiena
Michiel Smid
Adam Smith
Shakhar Smorodinsky
Christian Sohler
Alexander Souza
Paul Spirakis
Michael Spriggs
Reto Sphel
Rob van Stee
Stamatis Stefanakos
Daniel Stefankovic
Cliff Stein
Bernhard von Stengel
Tobias Storch
Madhu Sudan
Dirk Sudholt
Mukund Sundararajan
Koutarou Suzuki
Maxim Sviridenko
Tibor Szabo
Zoltan Szigeti
Troels Bjerre Sørensen
Asano Takao
Hisao Tamaki
Akihisa Tamura
Eva Tardos
Sebastiaan Terwijn
Pascal Tesson
Prasad Tetali
Ralf Thoele
Karsten Tiemann
Yuuki Tokunaga
Takeshi Tokuyama
Eric Torng
Patrick Traxler
Luca Trevisan
Tatsuie Tsukiji
Gyorgy Turan
Pim Tuyls
Ryuhei Uehara
Chris Umans
Falk Unger
Takeaki Uno
Pavel Valtr
Sergei Vassilvitskii
Ingrid Verbauwhede
Kolia Vereshchagin
Damien Vergnaud
Adrian Vetta
Ivan Visconti
Berthold Voecking
Heribert Vollmer
Sergey Vorobyov
Sven de Vries
Stephan Waack
Uli Wagner
Michael Waidner
Bogdan Warinschi
Osamu Watanabe
Brent Waters
Kevin Wayne
Stephanie Wehner
Ralf-Philipp Weinmann
Andreas Weissl
Tom Wexler
Erik Winfree
Peter Winkler
Kai Wirt
Carsten Witt
Ronald de Wolf
Stefan Wolf
David Woodruff
Mutsunori Yagiura
Hiroaki Yamamoto
Go Yamamoto
Shigeru Yamashita
Takenaga Yasuhiko
Yiqun Lisa Yin
Filip Zagorski
Guochuan Zhang
Yuliang Zheng
Ming Zhong
Hong-Sheng Zhou
Xiao Zhou
Wieslaw Zielonka
Eckart Zitzler
David Zuckerman
Philipp Zumstein
Uri Zwick

Sponsoring Institutions

IBM Italy
Venis S.P.A - Venezia Informatica e Sistemi
Dipartimento di Informatica, Università Ca' Foscari
CVR - Consorzio Venezia Ricerche

Lecture Notes in Computer Science 4052

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Lecture Notes in Computer Science

For information about Vols. 1–3972

please contact your bookseller or Springer

Vol. 4067: D. Thomas (Ed.), ECOOP 2006 – Object-Oriented Programming. XIV, 527 pages. 2006.

Vol. 4063: I. Gorton, G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C.A. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 394 pages. 2006.

Vol. 4060: K. Futatsugi, J.-P. Jouannaud, J. Meseguer (Eds.), Algebra, Meaning and Computation. XXXVIII, 643 pages. 2006.

Vol. 4059: L. Arge, R. Freivalds (Eds.), Algorithm Theory – SWAT 2006. XII, 436 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4057: J.P. W. Pluim, B. Likar, F.A. Gerritsen (Eds.), Biomedical Image Registration. XII, 324 pages. 2006.

Vol. 4056: P. Flocchini, L. Gąsieniec (Eds.), Structural Information and Communication Complexity. X, 357 pages. 2006.

Vol. 4055: J. Lee, J. Shim, S.-g. Lee, C. Bussler, S. Shim (Eds.), Data Engineering Issues in E-Commerce and Services. IX, 290 pages. 2006.

Vol. 4054: A. Horváth, M. Telek (Eds.), Formal Methods and Stochastic Models for Performance Evaluation. VIII, 239 pages. 2006.

Vol. 4053: M. Ikeda, K.D. Ashley, T.-W. Chan (Eds.), Intelligent Tutoring Systems. XXVI, 821 pages. 2006.

Vol. 4052: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Part II. XXIV, 603 pages. 2006.

Vol. 4048: L. Goble, J.-J.C.. Meyer (Eds.), Deontic Logic and Artificial Normative Systems. X, 273 pages. 2006. (Sublibrary LNAI).

Vol. 4046: S.M. Astley, M. Brady, C. Rose, R. Zwiggelaar (Eds.), Digital Mammography. XVI, 654 pages. 2006.

Vol. 4045: D. Barker-Plummer, R. Cox, N. Swoboda (Eds.), Diagrammatic Representation and Inference. XII, 301 pages. 2006. (Sublibrary LNAI).

Vol. 4044: P. Abrahamsson, M. Marchesi, G. Succi (Eds.), Extreme Programming and Agile Processes in Software Engineering. XII, 230 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4041: S.-W. Cheng, C.K. Poon (Eds.), Algorithmic Aspects in Information and Management. XI, 395 pages. 2006.

Vol. 4040: R. Reulke, U. Eckardt, B. Flach, U. Knauer, K. Polthier (Eds.), Combinatorial Image Analysis. XII, 482 pages. 2006.

Vol. 4039: M. Morisio (Ed.), Reuse of Off-the-Shelf Components. XIII, 444 pages. 2006.

Vol. 4038: P. Ciancarini, H. Wiklicky (Eds.), Coordination Models and Languages. VIII, 299 pages. 2006.

Vol. 4037: R. Gorrieri, H. Wehrheim (Eds.), Formal Methods for Open Object-Based Distributed Systems. XVII, 474 pages. 2006.

Vol. 4036: O. H. Ibarra, Z. Dang (Eds.), Developments in Language Theory. XII, 456 pages. 2006.

Vol. 4035: H.-P. Seidel, T. Nishita, Q. Peng (Eds.), Advances in Computer Graphics. XX, 771 pages. 2006.

Vol. 4034: J. Münch, M. Vierimaa (Eds.), Product-Focused Software Process Improvement. XVII, 474 pages. 2006.

Vol. 4033: B. Stiller, P. Reichl, B. Tuffin (Eds.), Performability Has its Price. X, 103 pages. 2006.

Vol. 4032: O. Etzion, T. Kuflik, A. Motro (Eds.), Next Generation Information Technologies and Systems. XIII, 365 pages. 2006.

Vol. 4031: M. Ali, R. Dapoigny (Eds.), Innovations in Applied Artificial Intelligence. XXIII, 1353 pages. 2006. (Sublibrary LNAI).

Vol. 4029: L. Rutkowski, R. Tadeusiewicz, L.A. Zadeh, J. Zurada (Eds.), Artificial Intelligence and Soft Computing – ICAISC 2006. XXI, 1235 pages. 2006. (Sublibrary LNAI).

Vol. 4027: H.L. Larsen, G. Pasi, D. Ortiz-Arroyo, T. Andreasen, H. Christiansen (Eds.), Flexible Query Answering Systems. XVIII, 714 pages. 2006. (Sublibrary LNAI).

Vol. 4026: P.B. Gibbons, T. Abdelzaher, J. Aspnes, R. Rao (Eds.), Distributed Computing in Sensor Systems. XIV, 566 pages. 2006.

Vol. 4025: F. Eliassen, A. Montresor (Eds.), Distributed Applications and Interoperable Systems. XI, 355 pages. 2006.

Vol. 4024: S. Donatelli, P. S. Thiagarajan (Eds.), Petri Nets and Other Models of Concurrency - ICATPN 2006. XI, 441 pages. 2006.

Vol. 4021: E. André, L. Dybkjær, W. Minker, H. Neumann, M. Weber (Eds.), Perception and Interactive Technologies. XI, 217 pages. 2006. (Sublibrary LNAI).

Vol. 4020: A. Bredenfeld, A. Jacoff, I. Noda, Y. Takahashi (Eds.), RoboCup 2005: Robot Soccer World Cup IX. XVII, 727 pages. 2006. (Sublibrary LNAI).

Vol. 4019: M. Johnson, V. Vene (Eds.), Algebraic Methodology and Software Technology. XI, 389 pages. 2006.

Vol. 4018: V. Wade, H. Ashman, B. Smyth (Eds.), Adaptive Hypermedia and Adaptive Web-Based Systems. XVI, 474 pages. 2006.

Vol. 4016: J.X. Yu, M. Kitsuregawa, H.V. Leong (Eds.), Advances in Web-Age Information Management. XVII, 606 pages. 2006.

Vol. 4014: T. Uustalu (Ed.), Mathematics of Program Construction. X, 455 pages. 2006.

Vol. 4013: L. Lamontagne, M. Marchand (Eds.), Advances in Artificial Intelligence. XIII, 564 pages. 2006. (Sublibrary LNAI).

Vol. 4012: T. Washio, A. Sakurai, K. Nakajima, H. Takeda, S. Tojo, M. Yokoo (Eds.), New Frontiers in Artificial Intelligence. XIII, 484 pages. 2006. (Sublibrary LNAI).

Vol. 4011: Y. Sure, J. Domingue (Eds.), The Semantic Web: Research and Applications. XIX, 726 pages. 2006.

Vol. 4010: S. Dunne, B. Stoddart (Eds.), Unifying Theories of Programming. VIII, 257 pages. 2006.

Vol. 4009: M. Lewenstein, G. Valiente (Eds.), Combinatorial Pattern Matching. XII, 414 pages. 2006.

Vol. 4007: C. Àlvarez, M. Serna (Eds.), Experimental Algorithms. XI, 329 pages. 2006.

Vol. 4006: L.M. Pinho, M. González Harbour (Eds.), Reliable Software Technologies – Ada-Europe 2006. XII, 241 pages. 2006.

Vol. 4005: G. Lugosi, H.U. Simon (Eds.), Learning Theory. XI, 656 pages. 2006. (Sublibrary LNAI).

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 4003: Y. Koucheryavy, J. Harju, V.B. Iversen (Eds.), Next Generation Teletraffic and Wired/Wireless Advanced Networking. XVI, 582 pages. 2006.

Vol. 4001: E. Dubois, K. Pohl (Eds.), Advanced Information Systems Engineering. XVI, 560 pages. 2006.

Vol. 3999: C. Kop, G. Fliedl, H.C. Mayr, E. Métais (Eds.), Natural Language Processing and Information Systems. XIII, 227 pages. 2006.

Vol. 3998: T. Calamoneri, I. Finocchi, G.F. Italiano (Eds.), Algorithms and Complexity. XII, 394 pages. 2006.

Vol. 3997: W. Grieskamp, C. Weise (Eds.), Formal Approaches to Software Testing. XII, 219 pages. 2006.

Vol. 3996: A. Keller, J.-P. Martin-Flatin (Eds.), Self-Managed Networks, Systems, and Services. X, 185 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3994: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part IV. XXXV, 1096 pages. 2006.

Vol. 3993: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part III. XXXVI, 1136 pages. 2006.

Vol. 3992: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part II. XXXV, 1122 pages. 2006.

Vol. 3991: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), Computational Science – ICCS 2006, Part I. LXXXI, 1096 pages. 2006.

Vol. 3990: J. C. Beck, B.M. Smith (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. X, 301 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao, Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3988: A. Beckmann, U. Berger, B. Löwe, J.V. Tucker (Eds.), Logical Approaches to Computational Barriers. XV, 608 pages. 2006.

Vol. 3987: M. Hazas, J. Krumm, T. Strang (Eds.), Location- and Context-Awareness. X, 289 pages. 2006.

Vol. 3986: K. Stølen, W.H. Winsborough, F. Martinelli, F. Massacci (Eds.), Trust Management. XIV, 474 pages. 2006.

Vol. 3984: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part V. XXV, 1045 pages. 2006.

Vol. 3983: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part IV. XXVI, 1191 pages. 2006.

Vol. 3982: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part III. XXV, 1243 pages. 2006.

Vol. 3981: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part II. XXVI, 1255 pages. 2006.

Vol. 3980: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), Computational Science and Its Applications - ICCSA 2006, Part I. LXXV, 1199 pages. 2006.

Vol. 3979: T.S. Huang, N. Sebe, M.S. Lew, V. Pavlović, M. Kölsch, A. Galata, B. Kisačanin (Eds.), Computer Vision in Human-Computer Interaction. XII, 121 pages. 2006.

Vol. 3978: B. Hnich, M. Carlsson, F. Fages, F. Rossi (Eds.), Recent Advances in Constraints. VIII, 179 pages. 2006. (Sublibrary LNAI).

Vol. 3977: N. Fuhr, M. Lalmas, S. Malik, G. Kazai (Eds.), Advances in XML Information Retrieval and Evaluation. XII, 556 pages. 2006.

Vol. 3976: F. Boavida, T. Plagemann, B. Stiller, C. Westphal, E. Monteiro (Eds.), NETWORKING 2006. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems. XXVI, 1276 pages. 2006.

Vol. 3975: S. Mehrotra, D.D. Zeng, H. Chen, B. Thuraisingham, F.-Y. Wang (Eds.), Intelligence and Security Informatics. XXII, 772 pages. 2006.

Vol. 3973: J. Wang, Z. Yi, J. Zurada, B.-L. Lu, H. Yin (Eds.), Advances in Neural Networks - ISNN 2006, Part III. XXIX, 1402 pages. 2006.

fashion. Our first finding is an equivalence relation between two security notions for these protocols—we show that for a large class of such protocols, in which encryption is not nested (that is, each ciphertext is of the form $E_{K_1^*}(K_2)$) security against multiple corrupt receivers is equivalent to security against a single corrupt receiver. This equivalence holds both in the symbolic (Dolev-Yao) model (that is, symbolic security against single corruptions implies symbolic security against multiple corruptions), and, subject to some mild syntactic conditions (e.g., absence of encryption cycles), also in the computational model. The equivalence in the computational setting is, in fact, of a very strong flavor: if one can prove a protocol (within the said class) computationally secure against single corruptions for *some* implementation of the cryptographic primitives, then it is collusion-resistant for *every* implementation of the primitives satisfying standard security properties (semantic security against chosen plaintext attacks for the former and computational indistinguishability for the latter).

We exemplify the significance of this equivalence result by applying it to the security analysis of various existing protocols. (See Table 1 in Sect. 4.) Most protocols (11 out of 13) surveyed by us don't make use of nested encryption and, as such, a proof of security against single corruptions for such protocols automatically implies collusion-resistance. As a part of our analysis, we uncover security weaknesses in 7 of the surveyed protocols, and provide simple fixes that result in protocols that are provably secure against arbitrary (polynomial-time) computational attacks.

Our techniques to prove this equivalence result don't generalize to capture protocols that use nested encryption (that is, transmit ciphertexts created by iterative encryption of a key using *multiple* other keys), and, in fact, they cannot do so. We demonstrate this by constructing a protocol that uses nesting (in fact, at most two iterations of E per ciphertext suffice), is secure against single corruptions but is totally broken by malicious coalitions (of size as small as two). As with the equivalence result, our separation holds both in the symbolic and computational models of security.

Protocols like the one used in our separation result have already been known to exist [5, 7]. (We remark that both these protocols require stateful receivers while ours does not.) Such protocols have a significant advantage over collusion-resistant protocols in terms of communication efficiency (constant versus logarithmic) and, in fact, they *beat* known lower bounds on the communication cost of GKD protocols [12]. Our results provide a precise explanation for this anomaly: although the bound of [12] applies to nested-encryption protocols, it holds only when collusion-resistance is satisfied. In fact, from our equivalence theorem (and the result of [12]), it follows that the efficiency of [5, 7] is unachievable using single encryption alone; it is precisely the use of nesting (and relaxation of the security requirements) that provide the efficiency gain.

Our Approach. Our equivalence and separation results for GKD protocols are obtained using a modular two-stage approach. We first prove the results in the Dolev-Yao model (Sect. 2), treating encryption and PRGs as abstract

Table of Contents – Part II

Invited Papers

Zero-Knowledge and Signatures

Cryptographic Protocols

Secrecy and Protocol Analysis

Cryptographic Primitives

Bounded Storage and Quantum Models

Foundations