Lecture Notes in Computer Science 4392

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

Salil P. Vadhan (Ed.)

Theory of Cryptography

4th Theory of Cryptography Conference, TCC 2007
Amsterdam, The Netherlands, February 21-24, 2007
Proceedings

Volume Editor

Salil P. Vadhan
Harvard University
Division of Engineering & Applied Sciences (DEAS)
33 Oxford Street, Cambridge, MA 02138, USA
E-mail: salil@eecs.harvard.edu

Library of Congress Control Number: 2007920469

CR Subject Classification (1998): E.3, F.2.1-2, C.2.0, G, D.4.6, K.4.1, K.4.3, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-70935-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-70935-0 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12021475 06/3142 5 4 3 2 1 0

Preface

TCC 2007, the Fourth Theory of Cryptography Conference, was held in Amsterdam, The Netherlands, from February 21 to 24, 2007, at Trippenhuis, the headquarters of the Royal Dutch Academy of Arts and Sciences (KNAW). TCC 2007 was sponsored by the International Association for Cryptologic Research (IACR) and was organized in cooperation with the Cryptology and Information Security Group at CWI, Amsterdam; the Mathematical Institute, Leiden University; and DIAMANT, the Dutch national mathematics cluster for discrete interactive and algorithmic algebra and number theory. The General Chair of the conference was Ronald Cramer.

The conference received 118 submissions, of which the Program Committee selected 31 for presentation at the conference. These proceedings consist of revised versions of those 31 papers. The revisions were not reviewed, and the authors bear full responsibility for the contents of their papers. The Best Student Paper Award was given to Saurabh Panjwani for his paper "Tackling Adaptive Corruptions in Multicast Encryption Protocols."

The conference program also included a tutorial on "Quantum Cryptography", given by Renato Renner, and a special event on "The Assumptions for Cryptography", consisting of a few short talks and a panel discussion. In addition, the Program Committee decided to augment the traditional rump session to include short informal presentations of not only new results, but also open problems and future research directions.

One of the things that has made my job as Program Chair a pleasure is the wonderful dedication our community has to the success of TCC. I am grateful to the many people who have contributed to the organization and content of the conference. First and foremost, this includes the authors of all submitted papers, whose research efforts are the raison d'etre for TCC. I am also indebted to my extremely dedicated Program Committee. They were faced with a larger than expected workload due to a jump in the number of submissions, yet they carried out the review process with extraordinary thoroughness and care for the high standards and integrity of TCC. I also thank the many external reviewers who assisted the Program Committee in its work.

I thank the Steering Committee of TCC for entrusting me with this responsibility, and its Chair, Oded Goldreich, for being available as a source of wisdom throughout the process. I also benefited from the experience and advice of the past TCC chairs, Moni Naor, Joe Kilian, Tal Rabin, and Shai Halevi. I am especially indebted to Shai, who wrote a wonderful software package that I used for handling the submissions, the PC discussions, and these proceedings and provided rapid-response customization and technical support throughout.

I am very grateful to Ronald Cramer, TCC 2007 General Chair; his Co-chairs, Serge Fehr, Dennis Hofheinz, and Eike Kiltz; and Wilmy van Ojik, the CWI

Conference Organizer, for all the work they have put into hosting the conference and managing its logistics. Thanks also to Microsoft for a generous donation that supported the conference in various ways, including stipends to help students attend.

My work as Program Chair was supported in part by grants from the National Science Foundation (CNS-0430336) and office of Naval Research (N00014-04-1-0478).

I appreciate the assistance provided by the Springer LNCS editorial staff, including Alfred Hofmann, Frank Holzwarth, and Anna Kramer, in assembling these proceedings. Finally, I thank Carol Harlow for the administrative help she provided here at Harvard.

TCC 2007 would not have been possible without the efforts of all the people I have mentioned here, as well as the many that I have surely forgotten (to whom I apologize).

December 2006 Salil Vadhan

TCC 2007

The 4th Theory of Cryptography Conference

KNAW Trippenhuis, Amsterdam, The Netherlands
February 21–24, 2007

Sponsored by *The International Association for Cryptologic Research*
Organized in cooperation with *Centrum voor Wiskunde en Informatica (CWI)* and *Mathematisch Instituut, Universiteit Leiden*
With financial support from *Microsoft Corporation*

General Chair

Ronald Cramer, CWI Amsterdam and Leiden University

Program Committee

Mihir Bellare	University of California, San Diego
Ran Canetti	IBM T.J. Watson Research Center
Ivan Damgård	University of Aarhus
Cynthia Dwork	Microsoft Research
Serge Fehr	CWI Amsterdam
Yuval Ishai	The Technion
Jonathan Katz	University of Maryland
Rafael Pass	MIT and Cornell University
Oded Regev	Tel Aviv University
Omer Reingold	Weizmann Institute of Science
Ronen Shaltiel	University of Haifa
Victor Shoup	New York University
Yael Tauman Kalai	MIT and Weizmann Institute of Science
Salil Vadhan (Chair)	Harvard University
Bogdan Warinschi	INRIA-Lorraine

TCC Steering Committee

Mihir Bellare	University of California, San Diego
Ivan Damgård	University of Aarhus
Oded Goldreich (Chair)	Weizmann Institute of Science
Shafi Goldwasser	MIT and Weizmann Institute of Science
Johan Håstad	Royal Institute of Technology
Russell Impagliazzo	University of California, San Diego
Ueli Maurer	ETH Zürich
Silvio Micali	Massachusetts Institute of Technology
Moni Naor	Weizmann Institute of Science
Tatsuaki Okamoto	NTT Laboratories

External Reviewers

Michel Abdalla
Benny Applebaum
Michael Backes
Boaz Barak
Adam Barth
Amos Beimel
Avraham Ben-Aroya
Michael Ben-Or
Eli Ben-Sasson
Bruno Blanchet
Alexandra Boldyreva
Jan Camenisch
Claude Carlet
Dario Catalano
Rafi Chen
Martin Cochran
Anupam Datta
Giovanni Di Crescenzo
Yan Zong Ding
Yevgeniy Dodis
Orr Dunkelman
Stefan Dziembowsky
Nelly Fazio
Marc Fischlin
Matthias Fitzi
Jun Furikawa
Ariel Gabizon
Rosario Gennaro
Craig Gentry
Jens Groth
Dan Gutfreund
Joshua Guttman
Robbert de Haan
Stuart Haber
Iftach Haitner
Shai Halevi
Goichiro Hanaoka
Danny Harnik
Prahladh Harsha
Avinatan Hassidim
Johan Håstad
Ishay Haviv
Alex Healy
Jonathan Herzog
Dennis Hofheinz
Susan Hohenberger
Nicholas J. Hopper
Nick Howgrave-Graham
Antoine Joux
Nathan Keller
Eike Kiltz
Chiu-Yuen Koo
Eyal Kushilevitz
Yehuda Lindell
Anna Lysyanskaya
Frank McSherry
Ilya Mironov
David Molnar
Tal Moran
Gregory Neven
Jesper Buus Nielsen
Adam O'Neill
Shien Jin Ong
Ivan Osipkov
Rafail Ostrovsky
Saurabh Panjwani
Kenny Paterson
Chris Peikert
Benny Pinkas
Manoj Prabhakaran
Tal Rabin
Zulfikar Ramzan
Leo Reyzin
Andrei Romashchenko
Alon Rosen
Guy Rothblum
Amit Sahai
Kazue Sako
Louis Salvail
Christian Schaffner
Gil Segev
Hovav Shacham
abhi shelat
Vladimir Shpilrain
Tomas Toft
Marten Trolin
Eran Tromer
Boaz Tsaban
Vinod Vaikuntanathan
Ivan Visconti
Shabsi Walfish
Brent Waters
John Watrous
Hoeteck Wee
Enav Weinreb
Douglas Wikström
Andreas Winter
David P. Woodruff

Table of Contents

Secret Sharing and Multiparty Computation

Signatures and Watermarking

Private Approximation and Black-Box Reductions

Key Establishment

Encryption II