Lecture Notes in Computer Science 2951

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Moni Naor (Ed.)

Theory of Cryptography

First Theory of Cryptography Conference, TCC 2004
Cambridge, MA, USA, February 19-21, 2004
Proceedings

Springer

Volume Editor

Moni Naor
Weizmann Institute of Science
Department of Computer Science and Applied Mathematics
Rehovot 76100, Israel
E-mail: moni.naor@weizmann.ac.il

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

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

ISSN 0302-9743
ISBN 3-540-21000-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10986196 06/3142 5 4 3 2 1 0

Preface

This volume contains the papers selected for presentation at the 1st Theory of Cryptography Conference (TCC) which was held at the Massachusetts Institute of Technology during February 19–21, 2004. The theory of cryptography deals with the paradigms, approaches and techniques used to conceptualize, define and provide solutions to natural cryptographic problems. The Theory of Cryptography Conference is a new venue dedicated to the dissemination of results in the area. The aim of the conference is to provide a meeting place for researchers and be instrumental in shaping the identity of the theory of cryptography community. A more detailed statement of purpose ('manifesto') is available on the TCC Web site (http://www-cse.ucsd.edu/users/mihir/tcc/).
The TCC 2004 program committee consisted of:

Ran Canetti	IBM T.J. Watson Research Center, USA
Ronald Cramer	Århus University, Denmark
Cynthia Dwork	Microsoft Research, USA
Yuval Ishai	Technion, Israel
Joe Kilian	NEC Research Labs, USA
Phil Mackenzie	Bell Labs, Lucent, USA
Daniele Micciancio	UCSD, USA
Moni Naor (PC Chair)	Weizmann Institute, Israel
Birgit Pfitzmann	IBM Research, Zurich, Switzerland
Omer Reingold	AT&T Research and IAS, USA
Salil Vadhan	Harvard University and Radcliffe Institute, USA

The program committee chose 29 papers out of the 70 submitted to the conference. Two sets of authors decided to merge, so the volume contains 28 papers altogether. In addition, given recent developments in the field, the committee decided to have a panel discussion on *Cryptography and Formal Methods*.

Acknowledgments : First and foremost I wish to thank all the people who submitted papers to the conference. Without them, of course, there would have been no conference. The hard task of reading, commenting on and selecting the papers to be accepted to the conference fell on the program committee members. Given that this is the first conference of its kind the mission was even trickier than usual. I am indebted to the committee members' collective knowledge, wisdom and effort. The committee also used external reviewers to extend the expertise and ease the burden. The names of these reviewers are listed on the pages that follow. My deepest gratitude to them as well.

I thank Joe Kilian for handling (and writing!) the server for submissions and reviews, as well as Omer Reingold and Edna Wigderson for helping out when Joe was away.

I thank Shafi Goldwasser for chairing this conference and making all the necessary arrangements at MIT. Shafi in turn is tremendously grateful to Joanne Talbot who coordinated the conference facilities, hotels, Web page, budgets, and the conference chair relentlessly and without a single complaint. Thank you Joanne. I thank Mihir Bellare for chairing the Steering Committee of TCC and the members of the committee (see the list in the pages that follow) for helping out with many issues concerning the conference, including the proceedings and the TCC Web-site. Finally a big thanks is due to Oded Goldreich who initiated this endeavor and pushed hard for it.

Rehovot, Israel
December 2003

Moni Naor
Program Chair
TCC 2004

External Referees

Masayuki Abe
Luis von Ahn
Michael Backes
Boaz Barak
Amos Beimel
Mihir Bellare
Alexandra Boldyreva
Harry Buhrman
Christian Cachin
Jan Camenisch
Claude Crépeau
Anand Desai
Yan Zong Ding
Yevgeniy Dodis
Marc Fischlin
Juan Garay
Rosario Gennaro
Daniel Gottesman
Jens Groth
Shai Halevi
Danny Harnik
Alejandro Hevia
Thomas Jakobsen
Markus Jakobsson
Ari Juels
Jonathan Katz
Hugo Krawczyk
Eyal Kushilevitz
Yehuda Lindell
Anna Lysyanskaya
Tal Malkin
David Meyer
Ashwin Nayak
Gregory Neven
Jesper Buus Nielsen
Adriana Palacio
Erez Petrank
Benny Pinkas
Tal Rabin
Oded Regev
Amit Sahai
Jean-Pierre Seifert
Adam Smith
Martijn Stam
Yael Tauman Kalai
Michael Waidner
John Watrous
Douglas Wikström
Bogdan Warinschi
Stephanie Wehner
Ke Yang

TCC Steering Committee

Mihir Bellare (Chair)	UCSD, USA
Ivan Damgård	Århus University, Denmark
Oded Goldreich	Weizmann Institute, Israel and Radcliffe Institute, USA
Shafi Goldwasser	MIT, USA and Weizmann Institute, Israel
Johan Håstad	Royal Institute of Technology, Sweden
Russell Impagliazzo	UCSD, USA
Ueli Maurer	ETH, Switzerland
Silvio Micali	MIT, USA
Moni Naor	Weizmann Institute, Israel
Tatsuaki Okamoto	NTT, Japan

Sponsoring Institutions

We acknowledge financial support from the following institutions:
CoreStreet Ltd.
IBM Corporation

Table of Contents