

Lecture Notes in Computer Science

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

2951

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

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media
springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

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

Notions of Reducibility between Cryptographic Primitives	1
<i>Omer Reingold, Luca Trevisan, Salil Vadhan</i>	
Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology	21
<i>Ueli Maurer, Renato Renner, Clemens Holenstein</i>	
On the Random-Oracle Methodology as Applied to Length-Restricted Signature Schemes	40
<i>Ran Canetti, Oded Goldreich, Shai Halevi</i>	
Universally Composable Commitments Using Random Oracles	58
<i>Dennis Hofheinz, Jörn Müller-Quade</i>	
Transformation of Digital Signature Schemes into Designated Confirmer Signature Schemes	77
<i>Shafi Goldwasser, Erez Waisbard</i>	
List-Decoding of Linear Functions and Analysis of a Two-Round Zero-Knowledge Argument	101
<i>Cynthia Dwork, Ronen Shaltiel, Adam Smith, Luca Trevisan</i>	
On the Possibility of One-Message Weak Zero-Knowledge	121
<i>Boaz Barak, Rafael Pass</i>	
Soundness of Formal Encryption in the Presence of Active Adversaries	133
<i>Daniele Micciancio, Bogdan Warinschi</i>	
Rerandomizable and Replayable Adaptive Chosen Ciphertext Attack Secure Cryptosystems	152
<i>Jens Groth</i>	
Alternatives to Non-malleability: Definitions, Constructions, and Applications	171
<i>Philip MacKenzie, Michael K. Reiter, Ke Yang</i>	
A Note on Constant-Round Zero-Knowledge Proofs for NP	191
<i>Alon Rosen</i>	
Lower Bounds for Concurrent Self Composition	203
<i>Yehuda Lindell</i>	

Secret-Key Zero-Knowledge and Non-interactive Verifiable Exponentiation	223
<i>Ronald Cramer, Ivan Damgård</i>	
A Quantitative Approach to Reductions in Secure Computation	238
<i>Amos Beimel, Tal Malkin</i>	
Algorithmic Tamper-Proof (ATP) Security: Theoretical Foundations for Security Against Hardware Tampering	258
<i>Rosario Gennaro, Anna Lysyanskaya, Tal Malkin, Silvio Micali, Tal Rabin</i>	
Physically Observable Cryptography	278
<i>Silvio Micali, Leonid Reyzin</i>	
Efficient and Universally Composable Committed Oblivious Transfer and Applications	297
<i>Juan A. Garay, Philip MacKenzie, Ke Yang</i>	
A Universally Composable Mix-Net	317
<i>Douglas Wikström</i>	
A General Composition Theorem for Secure Reactive Systems	336
<i>Michael Backes, Birgit Pfitzmann, Michael Waidner</i>	
Unfair Noisy Channels and Oblivious Transfer	355
<i>Ivan Damgård, Serge Fehr, Kirill Morozov, Louis Salvail</i>	
Computational Collapse of Quantum State with Application to Oblivious Transfer	374
<i>Claude Crépeau, Paul Dumais, Dominic Mayers, Louis Salvail</i>	
Implementing Oblivious Transfer Using Collection of Dense Trapdoor Permutations	394
<i>Iftach Haitner</i>	
Composition of Random Systems: When Two Weak Make One Strong ...	410
<i>Ueli Maurer, Krzysztof Pietrzak</i>	
Simpler Session-Key Generation from Short Random Passwords	428
<i>Minh-Huyen Nguyen, Salil Vadhan</i>	
Constant-Round Oblivious Transfer in the Bounded Storage Model	446
<i>Yan Zong Ding, Danny Harnik, Alon Rosen, Ronen Shaltiel</i>	
Hierarchical Threshold Secret Sharing	473
<i>Tamir Tassa</i>	
On Compressing Encrypted Data without the Encryption Key	491
<i>Mark Johnson, David Wagner, Kannan Ramchandran</i>	

On the Notion of Pseudo-Free Groups 505
 Ronald L. Rivest

Author Index 523