

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

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

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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com

© International Association for Cryptologic Research 2007
Printed in Germany

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’être* 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

Encryption I

Does Privacy Require True Randomness?	1
<i>Carl Bosley and Yevgeniy Dodis</i>	
Tackling Adaptive Corruptions in Multicast Encryption Protocols	21
<i>Saurabh Panjwani</i>	

Universally Composable Security

Long-Term Security and Universal Composability	41
<i>Jörn Müller-Quade and Dominique Unruh</i>	
Universally Composable Security with Global Setup	61
<i>Ran Canetti, Yevgeniy Dodis, Rafael Pass, and Shabsi Walfish</i>	

Arguments and Zero Knowledge

Parallel Repetition of Computationally Sound Protocols Revisited	86
<i>Krzysztof Pietrzak and Douglas Wikström</i>	
Lower Bounds for Non-interactive Zero-Knowledge	103
<i>Hoeteck Wee</i>	
Perfect NIZK with Adaptive Soundness	118
<i>Masayuki Abe and Serge Fehr</i>	

Notions of Security

Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries	137
<i>Yonatan Aumann and Yehuda Lindell</i>	
On the Necessity of Rewinding in Secure Multiparty Computation	157
<i>Michael Backes, Jörn Müller-Quade, and Dominique Unruh</i>	
On Expected Probabilistic Polynomial-Time Adversaries: A Suggestion for Restricted Definitions and Their Benefits	174
<i>Oded Goldreich</i>	

Obfuscation

On Best-Possible Obfuscation	194
<i>Shafi Goldwasser and Guy N. Rothblum</i>	

Obfuscation for Cryptographic Purposes	214
<i>Dennis Hofheinz, John Malone-Lee, and Martijn Stam</i>	

Securely Obfuscating Re-encryption	233
<i>Susan Hohenberger, Guy N. Rothblum, abhi shelat, and Vinod Vaikuntanathan</i>	

Secret Sharing and Multiparty Computation

Weakly-Private Secret Sharing Schemes	253
<i>Amos Beimel and Matthew Franklin</i>	

On Secret Sharing Schemes, Matroids and Polymatroids	273
<i>Jaume Martí-Farré and Carles Padró</i>	

Secure Linear Algebra Using Linearly Recurrent Sequences	291
<i>Eike Kiltz, Payman Mohassel, Enav Weinreb, and Matthew Franklin</i>	

Towards Optimal and Efficient Perfectly Secure Message Transmission	311
<i>Matthias Fitzi, Matthew Franklin, Juan Garay, and S. Harsha Vardhan</i>	

Signatures and Watermarking

Concurrently-Secure Blind Signatures Without Random Oracles or Setup Assumptions	323
<i>Carmit Hazay, Jonathan Katz, Chiu-Yuen Koo, and Yehuda Lindell</i>	

Designated Confirmer Signatures Revisited	342
<i>Douglas Wikström</i>	

From Weak to Strong Watermarking	362
<i>Nicholas Hopper, David Molnar, and David Wagner</i>	

Private Approximation and Black-Box Reductions

Private Approximation of Clustering and Vertex Cover	383
<i>Amos Beimel, Renen Hallak, and Kobbi Nissim</i>	

Robuster Combiners for Oblivious Transfer	404
<i>Remo Meier, Bartosz Przydatek, and Jürg Wullschleger</i>	

One-Way Permutations, Interactive Hashing and Statistically Hiding Commitments	419
<i>Hoeteck Wee</i>	

Towards a Separation of Semantic and CCA Security for Public Key Encryption	434
<i>Yael Gertner, Tal Malkin, and Steven Myers</i>	

Key Establishment

Unifying Classical and Quantum Key Distillation	456
<i>Matthias Christandl, Artur Ekert, Michał Horodecki, Paweł Horodecki, Jonathan Oppenheim, and Renato Renner</i>	
Intrusion-Resilient Key Exchange in the Bounded Retrieval Model	479
<i>David Cash, Yan Zong Ding, Yevgeniy Dodis, Wenke Lee, Richard Lipton, and Shabsi Walfish</i>	
(Password) Authenticated Key Establishment: From 2-Party to Group	499
<i>Michel Abdalla, Jens-Matthias Bohli, María Isabel González Vasco, and Rainer Steinwandt</i>	

Encryption II

Multi-authority Attribute Based Encryption	515
<i>Melissa Chase</i>	
Conjunctive, Subset, and Range Queries on Encrypted Data	535
<i>Dan Boneh and Brent Waters</i>	
How to Shuffle in Public	555
<i>Ben Adida and Douglas Wikström</i>	
Evaluating Branching Programs on Encrypted Data	575
<i>Yuval Ishai and Anat Paskin</i>	
Author Index	595