

*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

*New York University, NY, 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*

Joe Kilian (Ed.)

# Theory of Cryptography

Second Theory of Cryptography Conference, TCC 2005  
Cambridge, MA, USA, February 10-12, 2005  
Proceedings



Springer

Volume Editor

Joe Kilian

Yianilos Labs

707 State Rd., Rt. 206, Suite 212, Princeton, NJ 08540, USA

E-mail: joe@pnylab.com

Library of Congress Control Number: 2005920136

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 3-540-24573-1 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

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 11390305 06/3142 5 4 3 2 1 0

# Preface

TCC 2005, the 2nd Annual Theory of Cryptography Conference, was held in Cambridge, Massachusetts, on February 10–12, 2005. The conference received 84 submissions, of which the program committee selected 32 for presentation. These proceedings contain the revised versions of the submissions that were presented at the conference. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers.

The conference program also included a panel discussion on the future of theoretical cryptography and its relationship to the real world (whatever that is). It also included the traditional “rump session,” featuring short, informal talks on late-breaking research news.

Much as haters of old faced mercury-induced neurological damage as an occupational hazard, computer scientists will on rare occasion be afflicted with egocentrism, probably due to prolonged CRT exposure. Thus, you must view with pity and not contempt my unalloyed elation at having my name on the front cover of this LNCS volume, and my deep-seated conviction that I fully deserve the fame and riches that will surely come of it. However, having in recent years switched over to an LCD monitor, I would like to acknowledge some of the many who contributed to this conference.

First thanks are due to the many researchers from all over the world who submitted their work to this conference. Lacking shrimp and chocolate-covered strawberries, TCC has to work hard to be a good conference. As a community, I think we have.

Shafi Goldwasser, the general chair, and Joanne Talbot Hanley, her administrative assistant, went far beyond the call of duty in their support for this conference. It is a matter of debate whether temporary insanity is a prerequisite for volunteering to be general chair, or a consequence. But, certainly, volunteering twice consecutively qualifies one for academic sainthood, if not martyr status. I wish them both several months of well-deserved peace and quiet.

Evaluating submissions requires deep knowledge of the literature, razor-sharp analytical skills, impeccable taste, wisdom and common sense. For my part, I have some pretty good Python scripts. The rest was filled in by my committee. I picked twelve people, and every last one of them did a great job. That just doesn’t happen any more, not even in the movies. They supported me far more than I led them.

Like everyone else these days, we outsourced. Our deliberations benefited greatly from the expertise of the many outside reviewers who assisted us in our deliberations. My thanks to all those listed in the following pages, and my thanks and apologies to any I have missed.

I have had the pleasure of working with our publisher, Springer, and in particular with Alfred Hofmann, Ursula Barth, and Erika Siebert-Cole. Although this was my second time working with Springer, I am sure I have not lost my

amateur status. It is wrong to prejudge based on nationality, so forgive me, but I did sleep easier knowing that in Germany people spell “Kilian” correctly.

I am grateful to Mihir Bellare, the steering committee chair, and the steering committee in general for making this conference possible.

The time I spent on this project was graciously donated by my places of employment and by my family. I thank NEC and Peter Yianilos for their support and understanding. I thank Dina, Gersh and Pearl for their support, understanding and love.

Finally, I wish to acknowledge the lives and careers of Shimon Even and Larry Stockmeyer, who left us much too soon. Looking at my own work, I can point to specific papers and research directions where their influence is direct. On a deeper level, both shaped their fields by their work and by their interactions with others. Many are their heirs without knowing it. Thank you.

December 2004

Joe Kilian  
Program Chair  
TCC 2005

# TCC 2005

February 10–12, 2005, Cambridge, Massachusetts, USA

## General Chair

Shafi Goldwasser, Massachusetts Institute of Technology, USA  
Weizmann Institute, Israel  
Administrative Assistant: Joanne Talbot Hanley

## Program Committee

Boaz Barak . . . . . IAS and Princeton University, USA  
Amos Beimel . . . . . Ben-Gurion University, Israel  
Rosario Gennaro . . . . . IBM, USA  
Joe Kilian (Chair) . . . . . Yianilos Labs, USA  
Anna Lysyanskaya . . . . . Brown University, USA  
Tal Malkin . . . . . Columbia University, USA  
Rafail Ostrovsky . . . . . UCLA, USA  
Erez Petrank . . . . . Technion Institute, Israel  
Tal Rabin . . . . . IBM, USA  
Leonid Reyzin . . . . . Boston University, USA  
Alon Rosen . . . . . MIT, USA  
Amit Sahai . . . . . UCLA, USA  
Louis Salvail . . . . . Aarhus University, Denmark

## Steering Committee

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

# Table of Contents

## Hardness Amplification and Error Correction

Optimal Error Correction Against Computationally Bounded Noise <i>Silvio Micali, Chris Peikert, Madhu Sudan, David A. Wilson</i> .....	1
Hardness Amplification of Weakly Verifiable Puzzles <i>Ran Canetti, Shai Halevi, Michael Steiner</i> .....	17
On Hardness Amplification of One-Way Functions <i>Henry Lin, Luca Trevisan, Hoeteck Wee</i> .....	34

## Graphs and Groups

Cryptography in Subgroups of $\mathbb{Z}_n$ <i>Jens Groth</i> .....	50
Efficiently Constructible Huge Graphs That Preserve First Order Properties of Random Graphs <i>Moni Naor, Asaf Nussboim, Eran Tromer</i> .....	66

## Simulation and Secure Computation

Comparing Two Notions of Simulatability <i>Dennis Hofheinz, Dominique Unruh</i> .....	86
Relaxing Environmental Security: Monitored Functionalities and Client-Server Computation <i>Manoj Prabhakaran, Amit Sahai</i> .....	104
Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs <i>Jonathan Katz, Yehuda Lindell</i> .....	128

## Security of Encryption

Adaptively Secure Non-interactive Public-Key Encryption <i>Ran Canetti, Shai Halevi, Jonathan Katz</i> .....	150
---	-----

Adaptive Security of Symbolic Encryption <i>Daniele Micciancio, Saurabh Panjwani</i> .....	169
---	-----

Chosen-Ciphertext Security of Multiple Encryption <i>Yevgeniy Dodis, Jonathan Katz</i> .....	188
---	-----

## Steganography and Zero Knowledge

Public-Key Steganography with Active Attacks <i>Michael Backes, Christian Cachin</i> .....	210
---	-----

Upper and Lower Bounds on Black-Box Steganography <i>Nenad Dedić, Gene Itkis, Leonid Reyzin, Scott Russell</i> .....	227
---	-----

Fair-Zero Knowledge <i>Matt Lepinski, Silvio Micali, Abhi Shelat</i> .....	245
---	-----

## Secure Computation I

How to Securely Outsource Cryptographic Computations <i>Susan Hohenberger, Anna Lysyanskaya</i> .....	264
--	-----

Secure Computation of the Mean and Related Statistics <i>Eike Kiltz, Gregor Leander, John Malone-Lee</i> .....	283
---	-----

Keyword Search and Oblivious Pseudorandom Functions <i>Michael J. Freedman, Yuval Ishai, Benny Pinkas, Omer Reingold</i> .....	303
---	-----

## Secure Computation II

Evaluating 2-DNF Formulas on Ciphertexts <i>Dan Boneh, Eu-Jin Goh, Kobbi Nissim</i> .....	325
--	-----

Share Conversion, Pseudorandom Secret-Sharing and Applications to Secure Distributed Computing <i>Ronald Cramer, Ivan Damgård, Yuval Ishai</i> .....	342
--	-----

Toward Privacy in Public Databases <i>Shuchi Chawla, Cynthia Dwork, Frank McSherry, Adam Smith, Hoeteck Wee</i> .....	363
--	-----



## Quantum Cryptography and Universal Composability

The Universal Composable Security of Quantum Key Distribution <i>Michael Ben-Or, Michał Horodecki, Debbie W. Leung, Dominic Mayers, Jonathan Oppenheim</i> .....	386
Universally Composable Privacy Amplification Against Quantum Adversaries <i>Renato Renner, Robert König</i> .....	407
A Universally Composable Secure Channel Based on the KEM-DEM Framework <i>Waka Nagao, Yoshifumi Manabe, Tatsuaki Okamoto</i> .....	426

## Cryptographic Primitives and Security

Sufficient Conditions for Collision-Resistant Hashing <i>Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky</i> .....	445
The Relationship Between Password-Authenticated Key Exchange and Other Cryptographic Primitives <i>Minh-Huyen Nguyen</i> .....	457
On the Relationships Between Notions of Simulation-Based Security <i>Anupam Datta, Ralf Küsters, John C. Mitchell, Ajith Ramanathan</i> ...	476

## Encryption and Signatures

A New Cramer-Shoup Like Methodology for Group Based Provably Secure Encryption Schemes <i>María Isabel González Vasco, Consuelo Martínez, Rainer Steinwandt, Jorge L. Villar</i> .....	495
Further Simplifications in Proactive RSA Signature <i>Stanisław Jarecki, Nitesh Saxena</i> .....	510
Proof of Plaintext Knowledge for the Ajtai-Dwork Cryptosystem <i>Shafi Goldwasser, Dmitriy Kharchenko</i> .....	529

## Information Theoretic Cryptography

Entropic Security and the Encryption of High-Entropy Messages <i>Yevgeniy Dodis, Adam Smith</i> .....	556
--	-----

Error Correction in the Bounded Storage Model  
    *Yan Zong Ding* ..... 578

Characterizing Ideal Weighted Threshold Secret Sharing  
    *Amos Beimel, Tamir Tassa, Eran Weinreb* ..... 600

**Author Index** ..... 621