# Lecture Notes in Computer Science 3378

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

Springer is a part of Springer Science+Business Media

springeronline.com

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 hatters 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

## Graphs and Groups

## Simulation and Secure Computation

## Security of Encryption

## Steganography and Zero Knowledge

## Secure Computation I

## Secure Computation II

## Quantum Cryptography and Universal Composability

## Cryptographic Primitives and Security

## Encryption and Signatures

## Information Theoretic Cryptography