# Lecture Notes in Computer Science 8349

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Yehuda Lindell (Ed.)

# Theory of Cryptography

11th Theory of Cryptography Conference, TCC 2014
San Diego, CA, USA, February 24-26, 2014
Proceedings

Springer

Volume Editor

Yehuda Lindell
Bar-Ilan University
Department of Computer Science
Ramat Gan 52900, Israel
E-mail: lindell@biu.ac.il

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-54241-1 e-ISBN 978-3-642-54242-8
DOI 10.1007/978-3-642-54242-8
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014930318

CR Subject Classification (1998): E.3, D.4.6, K.6.5, F.1.1-2, C.2.0, F.2.1-2, G.2.2, I.1

LNCS Sublibrary: SL 4 – Security and Cryptology

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

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

TCC 2014 was held at the University of California San Diego in California, during February 24–26, 2014. TCC 2014 was sponsored by the International Association for Cryptologic Research (IACR). The general chairs of the conference were Mihir Bellare and Daniele Micciancio. I would like to thank them in the name of the TCC community in general, and in the name of all of the participants of TCC 2014 in particular, for their hard work in organizing the conference.

The conference received 90 submissions, of which the Program Committee selected 30 for presentation at the conference. These proceedings consist of the revised versions of the 30 papers. The revisions were not reviewed, and the authors bear full responsibility for the contents of their papers. In addition to the regular paper presentations, TCC 2014 featured a rump session where short presentations of recent results were given, and two invited talks. The invited speakers were Russell Impagliazzo and Silvio Micali, and the Program Committee is very grateful to them for accepting our invitation.

I am greatly indebted to many people who contributed to the success of TCC 2014. First and foremost, I would like to thank all those who submitted their papers to TCC. The success of TCC is due mainly to your work. In addition, I would like to thank the Program Committee for all of their hard work and diligence in reviewing the submissions and choosing the program. A lot of work is involved in this process, and your service to the community is greatly appreciated. I would also like to thank all of the external reviewers who participated in the process and provided in-depth reviews of the papers that they read. Finally, I owe deep thanks to Shai Halevi and Tal Rabin who provided me with valuable advice when I needed it. The TCC Program Committee also used Shai's excellent web-review software, and I thank Shai for writing it and for the support he provided when needed.

This was the 11th Theory of Cryptography Conference, and it was my honor and pleasure to act as the program chair of TCC as it entered its second decade. A quick look at the proceedings herein suffices to appreciate the vibrant and dynamic work being carried out by the TCC community. The proceedings include research on new and exciting topics like obfuscation, as well as basic foundational research on classic topics like zero-knowledge, secure computation, encryption, black-box separations, cryptographic coding theory and more. In addition to the fascinating research presented at TCC, the conference atmosphere is always warm and friendly and is essentially a meeting of friends who come together to study the fundamentals of our field. I thank the entire TCC community for creating this event and for maintaining its unique and special qualities.

February 2014 Yehuda Lindell

# TCC 2014
# The 11th Theory of Cryptography Conference

University of California San Diego, California, USA
February 24–26, 2014

Sponsored by the *International Association for Cryptologic Research (IACR)*

## General Chair

| | |
|---|---|
| Mihir Bellare | UCSD, USA |
| Daniele Micciancio | UCSD, USA |

## Program Chair

| | |
|---|---|
| Yehuda Lindell | Bar-Ilan University, Israel |

## Program Committee

| | |
|---|---|
| Amos Beimel | Ben-Gurion University, Israel |
| Alexandra Boldyreva | Georgia Tech, USA |
| Kai-Min Chung | Academia Sinica, Taiwan |
| Yevgeniy Dodis | New York University, USA |
| Nelly Fazio | City University of New York, USA |
| Marc Fischlin | Darmstadt University of Technology, Germany |
| Jens Groth | University College London, UK |
| Iftach Haitner | Tel-Aviv University, Israel |
| Martin Hirt | ETH Zurich, Switzerland |
| Dennis Hofheinz | Karlsruhe Institute of Technology, Germany |
| Susan Hohenberger Waters | Johns Hopkins University, USA |
| Eike Kiltz | Ruhr-Universität Bochum, Germany |
| Eyal Kushilevitz | Technion – Israel Institute of Technology, Israel |
| Mohammad Mahmoody | Cornell University, USA |
| Claudio Orlandi | Aarhus University, Denmark |
| Christopher J. Peikert | Georgia Tech, USA |
| Krzysztof Pietrzak | IST, Austria |
| Mike Rosulek | Oregon State University, USA |
| Adam Smith | Pennsylvania State University, USA |
| Salil Vadhan | Harvard University, USA |
| Vinod Vaikuntanathan | University of Toronto, Canada |

## External Reviewers

Divesh Aggarwal
Shashank Agrawal
Martin Albrecht
Jacob Alperin-Sheriff
Joel Alwen
Christian Badertscher
Paul Baecher
Abhishek Banerjee
Nir Bitansky
Olivier Blazy
Elette Boyle
Christina Brzuska
Nishanth Chandran
Melissa Chase
Cheng Chen
Alessandro Chiesa
Sherman Chow
Sandro Coretti
Özgür Dagdelen
Ivan Damgåard
Grégory Demay
Frederic Dupuis
Serge Fehr
Tore Frederiksen
Georg Fuchsbauer
Felix Günther
Tommaso Gagliardoni
Chaya Ganesh
Sanjam Garg
Peter Gazi
Rosario Gennaro
Sergey Gorbunov
Vipul Goyal
Shai Halevi
Kristiyan Haralambiev
Javier Herranz
Thomas Holenstein
Yuval Ishai
Tibor Jager
Abhishek Jain
Daniel Kraschewski
Sara Krehbiel
Guanfeng Liang
Huijia (Rachel) Lin
Feng-Hao Liu
Zhenming Liu
Adriana Lopez-Alt
Hemanta Maji
Giorgia Azzurra Marson
Daniel Masny
Eric Miles
Payman Mohassel
Antonio Nicolosi
Adam O'Neill
Cristina Onete
Jiaxin Pan
Omer Paneth
Milinda Perera
Manoj Prabhakaran
Carla Rafols
Ananth Raghunathan
Vanishree Rao
Pavel Raykov
Guy Rothblum
Christian Schaffner
Dominique Schröder
Karn Seth
Or Sheffet
Tom Shrimpton
Fang Song
Francois-Xavier Standaert
Uri Stemmer
Noah Stephens-Davidowitz
Björn Tackmann
Sidharth Telang
Aris Tentes
Stefano Tessaro
Roberto Trifiletti
Daniel Tschudi
Dominique Unruh
Yevgeniy Vahlis
Muthuramakrishnan Venkitasubramaniam
Dhinakaran Vinayagamurthy
Brent Waters
Daniel Wichs
Scott Yilek
Hong-Sheng Zhou

# Invited Talks

# Collusion and Privacy in Mechanism Design

Silvio Micali

Laboratory for Computer Science,
MIT, Cambridge, MA 02139
silvio@csail.mit.edu

**Abstract.** Mechanism design aims at engineering games that, rationally played, yield desired outcomes. In such games, multiple players interact very much as in a cryptographic protocol. But there are some fundamental differences. No player is "good", that is, always follows his prescribed instruction. No player is "malicious", that is, always acts so as to prevent the desired outcome from being achieved. Rather, every player is RATIONAL, that is, always acts so as to maximize HIS OWN utility.

Rational players too, however, have incentives to collude, and value privacy. Thus, privacy and collusion can disrupt the intended course of a game, and ultimately prevent the desired outcome from being achieved. Mechanism design has been only moderately successful in protecting against collusion, and has largely ignored privacy.

I believe that there is an opportunity for cryptographers and game theorists to join forces and produce new mechanisms that are resilient to collusion and privacy issues. I also believe that, to be successful, this effort requires a good deal of modeling and the development of new conceptual frameworks. In sum, there is the promise of a great deal of fun, challenge, and excitement, and I would like to recruit as much talent as possible towards this effort.

As a concrete example of what may be done in this area, I will describe a (quite) resilient mechanism, designed by Jing Chen and I, for achieving a (quite) alternative revenue benchmark in unrestricted combinatorial auctions. In such auctions there are multiple distinct goods for sale, each player privately attributes an arbitrary value to any possible subset of the goods, and the seller has no information about the players valuations. (Traditional mechanisms for unrestricted combinatorial auctions were uniquely "vulnerable" to collusion and privacy.)

# Specific versus General Assumptions in Cryptography

Russell Impagliazzo [*]

CSE Department, UCSD

**Abstract.** Modern cryptography began with the insight that computational difficulty could limit the ability of an attacker to break encryption or forge signatures. However, it was not for another few years that the required computational difficulty of specific problems on specific distributions for a cryptographic protocol to be secure was made explicit and quantitative. A further advantage of formalizing this connection is that it clarifies the exact properties, both in terms of which aspects should be computationally feasible and which related problems should be computationally intractable, were used to prove security of the protocol. This lays the foundation for proving possibility results in cryptography based on general assumptions, about the existence of types of cryptographically useful tools, rather than based on the difficulty of specific problems. A pattern emerged, where a new cryptographic goal is proposed, an "existence proof" given based on specific assumptions (sometimes untested) is given, then a variety of protocols are given based on different assumptions, and then these protocols are abstracted in terms of more general assumptions that suffice.

This talk will focus on the history of how this pattern emerged, the advantages that proofs of security based on general assumptions gives over protocol design based on specific assumptions, and on both progress and set-backs in basing cryptography on general assumptions.

[*] Work supported by the Simons Foundation and NSF grant CCF-121351.

# Table of Contents

## Obfuscation

## Applications of Obfuscation

## Zero Knowledge

## Black-Box Separations

## Secure Computation

## Coding and Cryptographic Applications

## Leakage

## Encryption

## Hardware-Aided Secure Protocols

## Encryption and Signatures