

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

Alfred Kobsa

University of California, Irvine, CA, 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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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

© International Association for Cryptologic Research 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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.

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

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

Virtual Black-Box Obfuscation for All Circuits via Generic Graded Encoding	1
<i>Zvika Brakerski and Guy N. Rothblum</i>	
Obfuscation for Evasive Functions	26
<i>Boaz Barak, Nir Bitansky, Ran Canetti, Yael Tauman Kalai, Omer Paneth, and Amit Sahai</i>	
On Extractability Obfuscation	52
<i>Elette Boyle, Kai-Min Chung, and Rafael Pass</i>	

Applications of Obfuscation

Two-Round Secure MPC from Indistinguishability Obfuscation	74
<i>Sanjam Garg, Craig Gentry, Shai Halevi, and Mariana Raykova</i>	
Chosen Ciphertext Security via Point Obfuscation	95
<i>Takahiro Matsuda and Goichiro Hanaoka</i>	

Zero Knowledge

Probabilistically Checkable Proofs of Proximity with Zero-Knowledge...	121
<i>Yuval Ishai and Mor Weiss</i>	
Achieving Constant Round Leakage-Resilient Zero-Knowledge	146
<i>Omkant Pandey</i>	
Statistical Concurrent Non-malleable Zero Knowledge	167
<i>Claudio Orlandi, Rafail Ostrovsky, Vanishree Rao, Amit Sahai, and Ivan Visconti</i>	
4-Round Resetably-Sound Zero Knowledge	192
<i>Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkatasubramanian, and Ivan Visconti</i>	

Black-Box Separations

Can Optimally-Fair Coin Tossing Be Based on One-Way Functions?	217
<i>Dana Dachman-Soled, Mohammad Mahmoody, and Tal Malkin</i>	

On the Power of Public-Key Encryption in Secure Computation 240
Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran

On the Impossibility of Basing Public-Coin One-Way Permutations on
 Trapdoor Permutations 265
Takahiro Matsuda

Secure Computation

Towards Characterizing Complete Fairness in Secure Two-Party
 Computation 291
Gilad Asharov

On the Cryptographic Complexity of the Worst Functions 317
Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz

Constant-Round Black-Box Construction of Composable Multi-Party
 Computation Protocol 343
Susumu Kiyoshima, Yoshifumi Manabe, and Tatsuaki Okamoto

One-Sided Adaptively Secure Two-Party Computation 368
Carmit Hazay and Arpita Patra

Multi-linear Secret-Sharing Schemes 394
Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin

Broadcast Amplification 419
Martin Hirt, Ueli Maurer, and Pavel Raykov

Coding and Cryptographic Applications

Non-malleable Coding against Bit-Wise and Split-State Tampering 440
Mahdi Cheraghchi and Venkatesan Guruswami

Continuous Non-malleable Codes 465
*Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, and
 Daniele Venturi*

Locally Updatable and Locally Decodable Codes 489
Nishanth Chandran, Bhavana Kanukurthi, and Rafail Ostrovsky

Leakage

Leakage Resilient Fully Homomorphic Encryption 515
Alexandra Berkoff and Feng-Hao Liu

Securing Circuits and Protocols against $1/\text{poly}(k)$ Tampering Rate 540
Dana Dachman-Soled and Yael Tauman Kalai

How to Fake Auxiliary Input	566
<i>Dimitar Jetchev and Krzysztof Pietrzak</i>	

Encryption

Standard versus Selective Opening Security: Separation and Equivalence Results	591
<i>Dennis Hofheinz and Andy Rupp</i>	
Dual System Encryption via Predicate Encodings	616
<i>Hoeteck Wee</i>	

Hardware-Aided Secure Protocols

(Efficient) Universally Composable Oblivious Transfer Using a Minimal Number of Stateless Tokens	638
<i>Seung Geol Choi, Jonathan Katz, Dominique Schröder, Arkady Yerukhimovich, and Hong-Sheng Zhou</i>	
Lower Bounds in the Hardware Token Model	663
<i>Shashank Agrawal, Prabhanjan Ananth, Vipul Goyal, Manoj Prabhakaran, and Alon Rosen</i>	

Encryption and Signatures

Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures	688
<i>Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi</i>	
On the Impossibility of Structure-Preserving Deterministic Primitives	713
<i>Masayuki Abe, Jan Camenisch, Rafael Dowsley, and Maria Dubovitskaya</i>	

Author Index	739
---------------------------	-----