

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

Amit Sahai (Ed.)

Theory of Cryptography

10th Theory of Cryptography Conference, TCC 2013
Tokyo, Japan, March 3-6, 2013
Proceedings



Springer

Volume Editor

Amit Sahai
UCLA
3731E Boelter Hall
Los Angeles, CA 90095, USA
E-mail: sahai@cs.ucla.edu

ISSN 0302-9743
ISBN 978-3-642-36593-5
DOI 10.1007/978-3-642-36594-2
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-36594-2

Library of Congress Control Number: 2013931230

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 2013

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.

The use of general descriptive names, registered names, trademarks, 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.

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

These are the proceedings of TCC 2013, the 10th Theory of Cryptography Conference, held at the University of Tokyo, Japan, during March 3–6, 2013. The conference was sponsored by the International Association for Cryptologic Research (IACR). The General Chairs were Masayuki Abe and Tatsuaki Okamoto.

The Program Committee accepted 36 papers out of 98 submissions. The program included papers on a wide variety of topics, from secure computation to zero-knowledge PCPs, by authors from many different backgrounds: one paper, “On the Circular Security of Bit-Encryption,” is solely authored by a PhD student, Ron D. Rothblum; another paper, “Characterizing the Cryptographic Properties of Reactive 2-Party Functionalities,” is co-authored by R. Amzi Jeffs, who was a high-school student at the time the paper was written.

On behalf of the Program Committee (PC), I thank the authors of all submissions for contributing excellent manuscripts. These contributions are of course the lifeblood of TCC, providing the most essential ingredient for the conference. The high quality of the submissions made the PC’s job both rewarding and challenging. Conflicts of interest were taken seriously by the PC. In particular, no PC member (including the PC chair) played any role in deciding the fate of submissions by authors that were current students, postdoctoral researchers, or colleagues in the same institution. The program also included three invited talks: by Craig Gentry, titled “Encrypted Messages from the Heights of Cryptomania”; by Tal Malkin, titled “Secure Computation for Big Data”; and by Benny Applebaum, titled “Cryptographic Hardness of Random Local Functions – A Survey.” The conference featured a rump session for informal short presentations and announcements, chaired by abhi shelat.

There are many individuals to whom I am grateful in connection with this conference. But I begin by thanking Dan Boneh and Shai Halevi, who went above and beyond the call of duty in providing assistance to the success of the conference, despite having no official role in the organization of TCC 2013.

This year, to increase the quality of the reviewing process, I wanted to add an automated way for PC members to have ongoing anonymous interactive communication with authors throughout the review period: this would enable reviewers to obtain clarifications on any aspects of submissions in a timely manner – at the time when they are most engaged with any particular paper. (This is in contrast to a single response phase, where often the author responses arrive too late to help with crucial PC discussions.) However, no currently available software package for conference management supports such a feature, and communication via the PC Chair is too cumbersome to encourage such interactions. Dan Boneh volunteered to write a Web-based software system to enable such interactions, and was very responsive to my requests for additional features and changes. Shai Halevi generously agreed to incorporate Dan’s system into his existing confer-

ence management software, and provided me with very helpful assistance for using his software throughout the review process. The PC used this new system throughout the TCC review process, and it greatly helped in clarifying issues about submissions. Despite this being a new experimental process, the PC used the new system to engage in interactions with over a quarter of submitted papers. This would not have been possible without the generous contributions of time and effort by Dan Boneh and Shai Halevi, and I am deeply grateful to them for their work.

The PC, which consisted of 20 top researchers in our field, worked very hard and I thank them for their dedication and effort. Special thanks are in order to Allison Lewko, Thomas Holenstien, and Mohammad Mahmoody, who agreed to serve as shepherds for certain accepted papers. I also thank all the external reviewers (listed in the following pages) for providing thoughtful reviews of submissions. For running the conference itself, I am very grateful to the General Chairs Masayuki Abe and Tatsuaki Okamoto, and all the members of the local Organizing Committee for their hard work: Takeshi Chikazawa, Masami Hagiya (Organizing Committee Chair), Noboru Kunihiro, Hirofumi Muratani, Ryo Nishimaki, Miyako Ohkubo, Yuji Suga, Koutarou Suzuki, Keisuke Tanaka, Shigenori Uchiyama, and Saho Uchida. I also wish to thank the two volunteers who managed the conference website: Shinichiro Matsuo and Hirokazu Hiruma. All of these individuals gave their time on a voluntary basis and their work was essential to the organization of the conference.

Finally, I am indebted to Oded Goldreich, the Chair of the TCC Steering Committee, and all the members of the TCC Steering Committee, Mihir Bellare, Ivan Dămgard, Shafi Goldwasser, Shai Halevi, Russell Impagliazzo, Ueli Maurer, Silvio Micali, Moni Naor, and Tatsuaki Okamoto, for their advice and trust. I am also grateful to previous TCC Chairs Tal Rabin, Shai Halevi, Ran Canetti, Yuval Ishai, and Ronald Cramer for their generous advice.

January 2013

Amit Sahai

TCC 2013

The 10th Theory of Cryptography Conference

University of Tokyo, Tokyo, Japan
March 3–6, 2013

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

General Chairs

Masayuki Abe	NTT, Japan
Tatsuaki Okamoto	NTT, Japan

Program Chair

Amit Sahai	UCLA, USA
------------	-----------

Program Committee

Masayuki Abe	NTT, Japan
Boaz Barak	Microsoft Research New England, USA
Ivan Damgård	Aarhus University, Denmark
Rosario Gennaro	City University of New York, USA
Vipul Goyal	Microsoft Research, India
Thomas Holenstein	ETH Zurich, Switzerland
Yuval Ishai	Technion, Israel
Yael Kalai	Microsoft Research New England, USA
Allison Lewko	Microsoft Research New England, USA
Mohammad Mahmoody	Cornell University, USA
Hemanta Maji	UCLA, USA
Ilya Mironov	Microsoft Research Silicon Valley, USA
Steve Myers	Indiana University, USA
Krzysztof Pietrzak	IST Austria, Austria
Tal Rabin	IBM Research, USA
Alon Rosen	IDC Herzliya, Israel
Amit Sahai	UCLA, USA, Chair
abhi shelat	University of Virginia, USA
Stefano Tessaro	MIT, USA
Hoeteck Wee	George Washington University, USA

External Reviewers

Anonymous	Dennis Hofheinz	Mariana Raykova
Shashank Agrawal	Pavel Hubacek	Renato Renner
Shweta Agrawal	William E. Skeith III	Leonid Reyzin
Benny Applebaum	Abhishek Jain	Thomas Ristenpart
Gilad Asharov	Thomas Jakobsen	Mike Rosulek
Abhishek Banerjee	Shiva Kasiviswanathan	Yannis Rouselakis
Kfir Barhum	Jonathan Katz	Alessandra Scafuro
Mihir Bellare	Eike Kiltz	Christian Schaffner
Andrej Bogdanov	Hugo Krawczyk	Gil Segev
Dan Boneh	Stephan Krenn	Or Sheffet
Zvika Brakerski	A. Kumarasubramanian	Victor Shoup
David Cash	Ranjit Kumaresan	Thomas Shrimpton
Kai-Min Chung	Robin Künzler	Nigel Smart
Laszlo Csirmaz	Jooyoung Lee	John Steinberger
Morten Dahl	Benoit Libert	Björn Tackmann
Angelo De Carlo	Huijia Rachel Lin	Aris Tentes
Nico Döttling	Yehuda Lindell	Daniel Tschudi
Rafael Dowsley	Edward Lui	Yevgeniy Vahlis
Chandan Dubey	Takahiro Matsuda	Vinod Vaikuntanathan
Sebastian Faust	Sigurd Meldgaard	Daniele Venturi
Dario Fiore	Payman Mohassel	Akshay Wadia
Tore Frederiksen	Prattyay Mukherjee	Bogdan Warinschi
Eiichiro Fujisaki	Michael Naehrig	Brent Waters
Ariel Gabizon	Moni Naor	John Watrous
Sanjam Garg	Antonio Nicolosi	Daniel Wichs
Niv Gilboa	Jesper Buus Nielsen	Douglas Wikström
Sharon Goldberg	Ryo Nishimaki	Jürg Wullschleger
Sergey Gorbunov	Peter Nordholt	Keita Xagawa
Dov Gordon	Adam O'Neill	Kazuki Yoneyama
Jens Groth	Claudio Orlandi	Hongsheng Zhou
Siyao Guo	Valerio Pastro	Vassilis Zikas
Iftach Haitner	Christopher J Peikert	Angela Zottarel
Shai Halevi	Raluca Ada Popa	
Brett Hemenway	Pavel Raykov	

Table of Contents

Overcoming Weak Expectations	1
<i>Yevgeniy Dodis and Yu Yu</i>	
A Counterexample to the Chain Rule for Conditional HILL Entropy: And What Deniable Encryption Has to Do with It	23
<i>Stephan Krenn, Krzysztof Pietrzak, and Akshay Wadia</i>	
Hardness Preserving Reductions via Cuckoo Hashing	40
<i>Itay Berman, Iftach Haitner, Ilan Komargodski, and Moni Naor</i>	
Concurrent Zero Knowledge in the Bounded Player Model	60
<i>Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, and Ivan Visconti</i>	
Public-Coin Concurrent Zero-Knowledge in the Global Hash Model	80
<i>Ran Canetti, Huijia Lin, and Omer Paneth</i>	
Succinct Malleable NIZKs and an Application to Compact Shuffles	100
<i>Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn</i>	
Encrypted Messages from the Heights of Cryptomania	120
<i>Craig Gentry</i>	
Attribute-Based Functional Encryption on Lattices	122
<i>Xavier Boyen</i>	
When Homomorphism Becomes a Liability	143
<i>Zvika Brakerski</i>	
Garbling XOR Gates “For Free” in the Standard Model	162
<i>Benny Applebaum</i>	
Why “Fiat-Shamir for Proofs” Lacks a Proof	182
<i>Nir Bitansky, Dana Dachman-Soled, Sanjam Garg, Abhishek Jain, Yael Tauman Kalai, Adriana López-Alt, and Daniel Wichs</i>	
On the (In)security of Fischlin’s Paradigm	202
<i>Prabhanjan Ananth, Raghav Bhaskar, Vipul Goyal, and Vanishree Rao</i>	
Signatures of Correct Computation	222
<i>Charalampos Papamanthou, Elaine Shi, and Roberto Tamassia</i>	

A Full Characterization of Functions that Imply Fair Coin Tossing and Ramifications to Fairness	243
<i>Gilad Asharov, Yehuda Lindell, and Tal Rabin</i>	
Characterizing the Cryptographic Properties of Reactive 2-Party Functionalities	263
<i>R. Amzi Jeffs and Mike Rosulek</i>	
Feasibility and Completeness of Cryptographic Tasks in the Quantum World	281
<i>Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas</i>	
Languages with Efficient Zero-Knowledge PCPs are in SZK	297
<i>Mohammad Mahmoody and David Xiao</i>	
Succinct Non-interactive Arguments via Linear Interactive Proofs	315
<i>Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Omer Paneth, and Rafail Ostrovsky</i>	
Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments	334
<i>Rafael Pass</i>	
Secure Computation for Big Data	355
<i>Tal Malkin</i>	
Communication Locality in Secure Multi-party Computation: How to Run Sublinear Algorithms in a Distributed Setting	356
<i>Elette Boyle, Shafi Goldwasser, and Stefano Tessaro</i>	
Distributed Oblivious RAM for Secure Two-Party Computation	377
<i>Steve Lu and Rafail Ostrovsky</i>	
Black-Box Proof of Knowledge of Plaintext and Multiparty Computation with Low Communication Overhead	397
<i>Steven Myers, Mona Sergi, and abhi shelat</i>	
Testing the Lipschitz Property over Product Distributions with Applications to Data Privacy	418
<i>Kashyap Dixit, Madhav Jha, Sofya Raskhodnikova, and Abhradeep Thakurta</i>	
Limits on the Usefulness of Random Oracles	437
<i>Iftach Haitner, Eran Omri, and Hila Zarosim</i>	
Analyzing Graphs with Node Differential Privacy	457
<i>Shiva Prasad Kasiviswanathan, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith</i>	

Universally Composable Synchronous Computation	477
<i>Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas</i>	
Multi-Client Non-interactive Verifiable Computation	499
<i>Seung Geol Choi, Jonathan Katz, Ranjit Kumaresan, and Carlos Cid</i>	
On the Feasibility of Extending Oblivious Transfer	519
<i>Yehuda Lindell and Hila Zarosim</i>	
Computational Soundness of Coinductive Symbolic Security under Active Attacks	539
<i>Mohammad Hajiabadi and Bruce M. Kapron</i>	
Revisiting Lower and Upper Bounds for Selective Decommitments	559
<i>Rafail Ostrovsky, Vanishree Rao, Alessandra Scafuro, and Ivan Visconti</i>	
On the Circular Security of Bit-Encryption	579
<i>Ron D. Rothblum</i>	
Cryptographic Hardness of Random Local Functions – Survey	599
<i>Benny Applebaum</i>	
On the Power of Correlated Randomness in Secure Computation	600
<i>Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, Claudio Orlandi, and Anat Paskin-Cherniavsky</i>	
Constant-Overhead Secure Computation of Boolean Circuits using Preprocessing	621
<i>Ivan Damgård and Sarah Zakarias</i>	
Implementing Resettable UC-Functionalities with Untrusted Tamper-Proof Hardware-Tokens	642
<i>Nico Döttling, Thilo Mie, Jörn Müller-Quade, and Tobias Nilges</i>	
A Cookbook for Black-Box Separations and a Recipe for UOWHFs	662
<i>Kfir Barhum and Thomas Holenstein</i>	
Algebraic (Trapdoor) One-Way Functions and Their Applications	680
<i>Dario Catalano, Dario Fiore, Rosario Gennaro, and Konstantinos Vamvourellis</i>	
Randomness-Dependent Message Security	700
<i>Eleanor Birrell, Kai-Min Chung, Rafael Pass, and Sidharth Telang</i>	
Errata to <i>(Nearly) Round-Optimal Black-Box Constructions of Commitments Secure against Selective Opening Attacks</i>	721
<i>David Xiao</i>	
Author Index	723