Lecture Notes in Computer Science 7785

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

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 e-ISSN 1611-3349
ISBN 978-3-642-36593-5 e-ISBN 978-3-642-36594-2
DOI 10.1007/978-3-642-36594-2
Springer Heidelberg Dordrecht London New York

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

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

Table of Contents