Lecture Notes in Computer Science 11892

More information about this series at http://www.springer.com/series/7410

Dennis Hofheinz · Alon Rosen (Eds.)

Theory of Cryptography

17th International Conference, TCC 2019
Nuremberg, Germany, December 1–5, 2019
Proceedings, Part II

Springer

Editors
Dennis Hofheinz
Karlsruhe Institute of Technology
Karlsruhe, Germany

Alon Rosen
IDC Herzliya
Herzliya, Israel

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-36032-0 ISBN 978-3-030-36033-7 (eBook)
https://doi.org/10.1007/978-3-030-36033-7

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 17th Theory of Cryptography Conference (TCC 2019) was held during December 1–5, 2019, at the DB Museum in Nuremberg, Germany. It was sponsored by the International Association for Cryptologic Research (IACR). The general chair of the conference was Dominique Schröder.

The conference received 147 submissions, of which the Program Committee (PC) selected 43 for presentation. Each submission was reviewed by at least three PC members, often more. The 35 PC members (including PC chairs), all top researchers in our field, were helped by 171 external reviewers, who were consulted when appropriate. These proceedings consist of the revised version of the 43 accepted papers. The revisions were not reviewed, and the authors bear full responsibility for the content of their papers.

As in previous years, we used Shai Halevi's excellent Web-review software, and are extremely grateful to him for writing it, and for providing fast and reliable technical support whenever we had any questions. We made extensive use of the interaction feature supported by the review software, where PC members could anonymously interact with authors. This was used to ask specific technical questions, such as suspected bugs. We felt this approach helped us prevent potential misunderstandings and improved the quality of the review process.

This year's TCC was extended from three to four days of talks, and the lengths of the presentations were accordingly extended from 20 to 25 minutes.

This was the sixth year that TCC presented the Test of Time Award to an outstanding paper that was published at TCC at least eight years ago, making a significant contribution to the theory of cryptography, preferably with influence also in other areas of cryptography, theory, and beyond. This year the Test of Time Award Committee selected the following paper, published at TCC 2008: "Incrementally Verifiable Computation or Proofs of Knowledge Imply Time/Space Efficiency" by Paul Valiant. This paper was selected for demonstrating the power of recursive composition of proofs of knowledge and enabling the development of efficiently verifiable proofs of correctness for complex computations. The authors were invited to deliver a talk at TCC 2019. The conference also featured two other invited talks, by Rachel Lin and by Omer Reingold.

A Best Young Researcher Paper Award was given to Henry Corrigan-Gibbs and Dmitry Kogan for their paper "The Function-Inversion Problem: Barriers and Opportunities."

We are greatly indebted to many people who were involved in making TCC 2019 a success. First of all, a big thanks to the most important contributors: all the authors who submitted papers to the conference. Next, we would like to thank the PC members for their hard work, dedication, and diligence in reviewing the papers, verifying the correctness, and in-depth discussion. We are also thankful to the external reviewers for their volunteered hard work and investment in reviewing papers and answering

questions, often under time pressure. For running the conference itself, we are very grateful to the general chair, Dominique Schröder. We appreciate the sponsorship from the IACR, Deloitte, Siemens, Syss, and HGS. We also wish to thank Friedrich-Alexander-Universität Erlangen-Nürnberg and Nuremberg Campus of Technology for their support. Finally, we are thankful to the TCC Steering Committee as well as the entire thriving and vibrant TCC community.

October 2019

Dennis Hofheinz
Alon Rosen

TCC 2019

The 17th Theory of Cryptography Conference

Nuremberg, Germany,
December 1–5, 2019

General Chair

Dominique Schröder	University of Erlangen-Nuremberg, Germany

Program Co-chairs

Dennis Hofheinz	Karlsruhe Institute of Technology
Alon Rosen	IDC Herzliya

Program Committee

Adi Akavia	Haifa University, Israel
Joël Alwen	Wickr, USA
Benny Applebaum	Tel Aviv University, Israel
Gilad Asharov	JP Morgan AI Research, USA
Nir Bitansky	Tel Aviv University, Israel
Chris Brzuska	Aalto University, Finland
Kai-Min Chung	Institute of Information Science, Academia Sinica, Taiwan
Ran Cohen	BU and Northeastern University, USA
Geoffroy Couteau	Karlsruhe Institute of Technology, Germany
Dana Dachman-Soled	University of Maryland, USA
Nico Döttling	CISPA, Saarbrücken, Germany
Marc Fischlin	Technische Universität Darmstadt, Germany
Siyao Guo	NYU Shanghai, China
Julia Hesse	Technische Universität Darmstadt, Germany
Pavel Hubáček	Charles University Prague, Czech Republic
Abhishek Jain	Johns Hopkins University, USA
Bhavana Kanukurthi	Indian Institute of Science, India
Eike Kiltz	Ruhr-Universität Bochum, Germany
Susumu Kiyoshima	NTT Secure Platform Laboratories, Japan
Venkata Koppula	Weizmann Institute of Science, Israel
Mohammad Mahmoody	University of Virginia, USA
Nikolaos Makriyannis	Technion, Israel
Pratyay Mukherjee	Visa Research, San Francisco, USA
Jörn Müller-Quade	Karlsruhe Institute of Technology, Germany

Ryo Nishimaki	NTT Secure Platform Laboratories, Japan
Omer Paneth	MIT, USA
Antigoni Polychroniadou	JP Morgan AI Research, USA
Mariana Raykova	Google, Inc., New York, USA
Ron Rothblum	IDC Herzliya, Israel
Noah Stephens-Davidowitz	MIT, USA
Prashant Vasudevan	UC Berkeley, USA
Muthuramakrishnan Venkitasubramaniam	University of Rochester, USA
Yu Yu	Shanghai Jiaotong University, China

External Reviewers

Masayuki Abe
Hamza Abusalah
Divesh Aggarwal
Shashank Agrawal
Thomas Agrikola
Prabhanjan Ananth
Daniel Apon
Benedikt Auerbach
Marshall Ball
Laasya Bangalore
Carsten Baum
Amos Beimel
Wasilij Beskorovajnov
Dan Boneh
Zvika Brakerski
Anne Broadbent
Brandon Broadnax
Ran Canetti
Ignacio Cascudo
David Cash
Leo de Castro
Hubert Chan
Nishanth Chandran
Xing Chaoping
Yilei Chen
Yu Chen
Wutichai Chongchitmate
Arka Rai Choudhuri
Hao Chung
Michele Ciampi
Deepesh Data
Akshay Degwekar
Frédéric Dupuis
Naomi Ephraim
Xiong (Leo) Fan
Pooya Farshim
Serge Fehr
Ariel Gabizon
Tommaso Gagliardoni
Chaya Ganesh
Romain Gay
Federico Giacon
Aarushi Goel
Huijing Gong
Rishab Goyal
Vipul Goyal
Alex Bredariol Grilo
Adam Groce
Josh Grochow
Roland Gröll
Chun Guo
Iftach Haitner
Mohammad Hajiabadi
Carmit Hazay
Kuan-Yi Ho
Thibaut Horel
Shih-Han Hung
Vincenzo Iovino
Aayush Jain
Stanislaw Jarecki
Zhengfeng Ji
Haodong Jiang
Zhengzhong Jin
Seny Kamara
Shuichi Katsumata
Sam Kim
Fuyuki Kitagawa
Michael Klooss
Alexander Koch
Konrad Kohbrok
Lisa Kohl
Ilan Komargodski
Yashvanth Kondi
Mukul Kulkarni
Ashutosh Kumar
Sai Lakshmi
Rio LaVigne
Eysa Lee
Yi Lee
Max Leibovich
Xin Li
Xiao Liang
Tai-Ning Liao
Wei-Kai Lin
Qipeng Liu
Tianren Liu
Yi-Kai Liu
Zhen Liu
Alex Lombardi
Julian Loss
Steve Lu
Fermi Ma
Sven Maier
Monosij Maitra
Giulio Malavolta
Yacov Manevich

Nathan Manohar
Daniel Masny
Noam Mazor
Jeremias Mechler
Nikolas Melissaris
Takaaki Mizuki
Ameer Mohammed
Tamer Mour
Marta Mularczyk
Matthias Nagel
Ariel Nof
Bhavana Obbattu
Maciej Obremski
Eran Omri
Michele Orru
Jiaxin Pan
Sikhar Patranabis
Udi Peled
Naty Peter
Oxana Poburinnaya
Sihang Pu
Erick Purwanto
Willy Quach
Samuel Ranellucci
Divya Ravi
Joao Ribeiro
Silas Richelson
Miruna Rosca
Paul Rösler
Pratik Sarkar
Santanu Sarkar
Peter Scholl
Rebecca Schwerdt
Sven Schäge
Adam Sealfon
Mahdi Sedaghat
Sruthi Sekar
Ido Shahaf
Devika Sharma
Sina Shiehian
Kazumasa Shinagawa
Omri Shmueli
Jad Silbak
Yifan Song
Nick Spooner
Akshayaram Srinivasan
Igors Stepanovs
Pierre-Yves Strub
Shi-Feng Sun
Siwei Sun
Xiaoming Sun
Björn Tackmann
Katsuyuki Takashima
Justin Thaler
Junichi Tomida
Rotem Tsabary
Dominique Unruh
Bogdan Ursu
Alexandre Wallet
Yuyu Wang
Mor Weiss
Daniel Wichs
David Wu
Keita Xagawa
Sophia Yakoubov
Shota Yamada
Takashi Yamakawa
Avishay Yanai
Kevin Yeo
Eylon Yogev
Fan Zhang
Jiapeng Zhang
Vassilis Zikas
Giorgos Zirdelis
Akin Ünal

Contents – Part II

Contents – Part I