Lecture Notes in Computer Science 11239

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

Editorial Board

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

Amos Beimel · Stefan Dziembowski (Eds.)

Theory of Cryptography

16th International Conference, TCC 2018
Panaji, India, November 11–14, 2018
Proceedings, Part I

Springer

Editors
Amos Beimel
Ben Gurion University
Beer Sheva, Israel

Stefan Dziembowski
University of Warsaw
Warsaw, Poland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-03806-9 ISBN 978-3-030-03807-6 (eBook)
https://doi.org/10.1007/978-3-030-03807-6

Library of Congress Control Number: 2018960441

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 16th Theory of Cryptography Conference (TCC 2018) was held during November 11–14, 2018, at the Cidade de Goa hotel, in Panaji, Goa, India. It was sponsored by the International Association for Cryptologic Research (IACR). The general chairs of the conference were Shweta Agrawal and Manoj Prabhakaran. We would like to thank them for their hard work in organizing the conference.

The conference received 168 submissions, of which the Program Committee (PC) selected 50 for presentation (with two pairs of papers sharing a single presentation slot per pair). Each submission was reviewed by at least three PC members, often more. The 30 PC members (including PC chairs), all top researchers in our field, were helped by 211 external reviewers, who were consulted when appropriate. These proceedings consist of the revised version of the 50 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. Based on the experience from previous years, we again made use of the interaction feature supported by the review software, where PC members may 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 was the fifth 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 2005: "Evaluating 2-DNF Formulas on Ciphertexts" by Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. This paper was selected for introducing compact two-operation homomorphic encryption and developing new bilinear map techniques that led to major improvements in the design of cryptographic schemes. The authors were also invited to deliver a talk at TCC 2018. A Best Student Paper Award was given to Tianren Liu for his paper "On Basing Search SIVP on NP-Hardness."

The conference also featured two other invited talks, by Moni Naor and by Daniel Wichs.

We are greatly indebted to many people who were involved in making TCC 2018 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 chairs, Shweta Agrawal and Manoj Prabhakaran. We appreciate

the sponsorship from the IACR, Microsoft Research, IBM, and Google. We also wish to thank IIT Madras and IIT Bombay for their support. Finally, we are thankful to the TCC Steering Committee as well as the entire thriving and vibrant TCC community.

November 2018

Amos Beimel
Stefan Dziembowski
TCC 2018 Program Chairs

TCC 2018

The 16th Theory of Cryptography Conference

Goa, India

November 11–14, 2018

Sponsored by the *International Association for Cryptologic Research*

General Chairs

Shweta Agrawal	Indian Institute of Technology, Madras, India
Manoj Prabhakaran	Indian Institute of Technology, Bombay, India

Program Committee

Masayuki Abe	NTT and Kyoto University, Japan
Divesh Aggarwal	National University of Singapore, Singapore
Shweta Agrawal	Indian Institute of Technology, Madras, India
Gilad Asharov	Cornell Tech, USA
Amos Beimel (Co-chair)	Ben-Gurion University, Israel
Andrej Bogdanov	The Chinese University of Hong Kong, SAR China
Zvika Brakerski	Weizmann Institute of Science, Israel
Nishanth Chandran	Microsoft Research, India
Stefan Dziembowski (Co-chair)	University of Warsaw, Poland
Sebastian Faust	TU Darmstadt, Germany
Marc Fischlin	TU Darmstadt, Germany
Iftach Haitner	Tel Aviv University, Israel
Martin Hirt	ETH Zurich, Switzerland
Pavel Hubáček	Charles University in Prague, Czech Republic
Aggelos Kiayias	University of Edinburgh, UK
Eyal Kushilevitz	Technion, Israel
Anna Lysyanskaya	Brown University, USA
Tal Malkin	Columbia University, USA
Eran Omri	Ariel University, Israel
Chris Peikert	University of Michigan – Ann Arbor, USA
Krzysztof Pietrzak	IST Austria, Austria
Antigoni Polychroniadou	Cornell University, USA
Alon Rosen	IDC Herzliya, Israel
Mike Rosulek	Oregon State University, USA
Vinod Vaikuntanathan	MIT, USA
Ivan Visconti	University of Salerno, Italy
Hoeteck Wee	CNRS and ENS, France

Mor Weiss	Northeastern University, USA
Stefan Wolf	University of Lugano, Switzerland
Vassilis Zikas	University of Edinburgh, UK

TCC Steering Committee

Ivan Damgård	Aarhus University, Denmark
Shai Halevi (Chair)	IBM Research, USA
Huijia (Rachel) Lin	UCSB, USA
Tal Malkin	Columbia University, USA
Ueli Maurer	ETH, Switzerland
Moni Naor	Weizmann Institute of Science, Israel
Manoj Prabhakaran	Indian Institute of Technology, Bombay, India

Additional Reviewers

Aydin Abadi
Shashank Agrawal
Adi Akavia
Navid Alamati
Ghada Almashaqbeh
Bar Alon
Joel Alwen
Prabhanjan Ananth
Megumi Ando
Benny Applebaum
Frederik Armknecht
Christian Badertscher
Saikrishna Badrinarayanan
Karim Baghery
Marshall Ball
Fabio Banfi
Laasya Bangalore
Carsten Baum
Aner Ben-Efraim
Fabrice Benhamouda
Nir Bitansky
Jonathan Bootle
Cecilia Boschini
Florian Bourse
Elette Boyle
Anne Broadbent
Brent Carmer
David Cash
Anrin Chakraborti
Yilei Chen
Ilaria Chillotti
Wutichai Chongchitmate
Michele Ciampi
Ran Cohen
Xavier Coiteux-Roy
Sandro Coretti
Geoffroy Couteau
Dana Dachman-Soled
Pratish Datta
Bernardo David
Jean Paul Degabriele
Akshay Degwekar
Apoorvaa Deshpande
Nico Döttling
Lisa Eckey
Naomi Ephraim
Omar Fawzi
Serge Fehr
Matthias Fitzi
Nils Fleischhacker
Georg Fuchsbauer
Eiichiro Fujisaki
Steven Galbreith
Chaya Ganesh
Adria Gascon
Romain Gay
Peter Gazi
Ran Gelles
Badih Ghazi
Satrajit Ghosh
Irene Giacomelli
Junqing Gong
Dov Gordon
Paul Grubbs
Cyprien de Saint Guilhem
Siyao Guo
Divya Gupta
Arne Hansen
Patrick Harasser
Prahladh Harsha
Julia Hesse
Minki Hhan
Ryo Hiromasa
Justin Holmgren
Kristina Hostakova
Yuval Ishai
Muhammad Ishaq
Zahra Jafargholi
Tibor Jager
Aayush Jain
Abhishek Jain
Daniel Jost
Bruce Kapron

Tomasz Kazana
Dakshita Khurana
Jiseung Kim
Sam Kim
Fuyuki Kitagawa
Susumu Kiyoshima
Karen Klein
Ilan Komargodski
Orestis Konstantinidis
Venkata Koppula
Lucas Kowalczyk
Daniel Kraschewski
Mukul Kulkarni
Ashutosh Kumar
Rajendra Kumar
Benjamin Kuykendall
Rio LaVinge
Changmin Lee
Moon Sung Lee
Nikos Leonardos
Xiao Liang
Jyun-Jie Liao
Chengyu Lin
Huijia (Rachel) Lin
Feng-Hao Liu
Qipeng Liu
Tianren Liu
Yi-Kai Liu
Chen-Da Liu Zhang
Alex Lombardi
Julian Loss
Steve Lu
Yun Lu
Vadim Lyubashevsky
Urmila Mahadev
Mohammad Mahmoody
Subhamoy Maitra
Nikolaos Makriyannis
Takahiro Matsuda
Christian Matt
Jeremias Mechler
Peihan Miao
Daniele Micciancio
Michele Minelli
Konstantinos Mitropoulos
Tarik Moataz
Fabrice Mouhartem
Tamer Mour
Pratyay Mukherjee
Priyanka Mukhopadhyay
Marta Mularczyk
Jörn Müller-Quade
Kartik Nayak
Tobias Nilges
Chinmay Nirkhe
Ryo Nishimaki
Sai Lakshmi Bhavana Obbattu
Maciej Obremski
Miyako Ohkubo
Georgios Panagiotakos
Omer Paneth
Anat Paskin-Cherniavsky
Valerio Pastro
Serdar Pehlivanoglu
Renen Perlman
Giuseppe Persiano
Thomas Peters
Christopher Portmann
Srinivasan Raghuraman
Govind Ramnarayan
Samuel Ranellucci
Michael Raskin
Michael Riabzev
João Ribeiro
Silas Richelson
Felix Rohrbach
Lior Rotem
Paul Rösler
Manuel Sabin
Katerina Samari
Alessandra Scafuro
Giannicola Scarpa
Peter Scholl
Adam Sealfon
Sruthi Sekar
Yannick Seurin
Sina Shiehian
Tom Shrimpton
Luisa Siniscalchi
Veronika Slivova
Pratik Soni
Nick Spooner
Akshayaram Srinivasan
Martjin Stam
John Steinberger
Noah Stephens-Davidowitz
Qiang Tang
Stefano Tessaro
Ni Trieu
Rotem Tsabary
Yiannis Tselekounis
Margarita Vald
Prashant Vasudevan
Muthuramakrishnan Venkitasubramaniam
Daniele Venturi
Satyanarayana Vusirikala
Hendrik Waldner
Petros Wallden
Michael Walter
Xiao Wang
Christopher Williamson
David Wu
Keita Xagawa
Yu Yu
Shota Yamada
Takashi Yamakawa
Kevin Yeo
Eylon Yogev
Thomas Zacharias
Mark Zhandry
Jiamin Zhu
Dionysis Zindros
Giorgos Zirdelis

Contents – Part I

Information-Theoretic Cryptography

Trapdoor Permutations and Signatures

Coin-Tossing and Fairness

Functional and Identity-Based Encryption

Contents – Part II