Lecture Notes in Computer Science 12551

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

Rafael Pass · Krzysztof Pietrzak (Eds.)

Theory of Cryptography

18th International Conference, TCC 2020
Durham, NC, USA, November 16–19, 2020
Proceedings, Part II

Springer

Editors
Rafael Pass
Cornell Tech
New York, NY, USA

Krzysztof Pietrzak
Institute of Science and Technology Austria
Klosterneuburg, Austria

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-64377-5 ISBN 978-3-030-64378-2 (eBook)
https://doi.org/10.1007/978-3-030-64378-2

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 18th Theory of Cryptography Conference (TCC 2020) was held virtually during November 16–19, 2020. It was sponsored by the International Association for Cryptologic Research (IACR). The general chair of the conference was Alessandra Scafuro.

TCC 2020 was originally planned to be co-located with FOCS 2020 in Durham, North Carolina, USA. Due to the COVID-19 pandemic both events were converted into virtual events, and were held on the same day at the same time. The authors uploaded videos of roughly 20 minutes prior to the conference, and at the conference had a 10-minute window to present a summary of their work and answer questions. The virtual event would not have been possible without the generous help of Kevin and Kay McCurley, and we would like to thank them wholeheartedly.

The conference received 167 submissions, of which the Program Committee (PC) selected 71 for presentation. Each submission was reviewed by at least four PC members. The 39 PC members (including PC chairs), all top researchers in the field, were helped by 226 external reviewers, who were consulted when appropriate. These proceedings consist of the revised version of the 71 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.

This was the 7th 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: "Perfectly-Secure MPC with Linear Communication Complexity" by Zuzana Trubini and Martin Hirt. The Award Committee recognized this paper "for introducing hyper-invertible matrices to perfectly secure multiparty computation, thus enabling significant efficiency improvements and, eventually, constructions with minimal communication complexity."

We are greatly indebted to many people who were involved in making TCC 2020 a success. A big thanks to the authors who submitted their papers and to the PC members and external reviewers for their hard work, dedication, and diligence in reviewing the papers, verifying the correctness, and in-depth discussions. A special thanks goes to the general chair Alessandra Scafuro and the TCC Steering Committee.

October 2020

Rafael Pass
Krzysztof Pietrzak

Organization

General Chair

Alessandra Scafuro	North Carolina State University, USA

Program Chairs

Rafael Pass	Cornell Tech, USA
Krzysztof Pietrzak	IST Austria, Austria

Program Committee

Prabhanjan Ananth	University of California, Santa Barbara, USA
Marshall Ball	Columbia University, USA
Sonia Belaïd	CryptoExperts, France
Jeremiah Blocki	Purdue University, USA
Andrej Bogdanov	The Chinese University of Hong Kong, Hong Kong
Chris Brzuszka	Aalto University, Finland
Ignacio Cascudo	IMDEA Software Institute, Spain
Kai-Min Chung	Academia Sinica, Taiwan
Aloni Cohen	Boston University, USA
Ran Cohen	Northeastern University, USA
Nico Dottling	CISPA - Helmholtz Center for Information Security, Germany
Stefan Dziembowski	University of Warsaw, Poland
Oriol Farràs	Universitat Rovira i Virgili, Spain
Georg Fuchsbauer	TU Wien, Austria
Niv Gilboa	Ben-Gurion University of the Negev, Israel
Vipul Goyal	Carnegie Mellon University, USA
Mohammad Hajiabadi	University of California, Berkeley, USA
Justin Holmgren	NTT Research, USA
Zahra Jafargholi	Aarhus University, Denmark
Yael Tauman Kalai	Microsoft Research and MIT, USA
Seny Kamara	Brown University, USA
Dakshita Khurana	University of Illinois Urbana-Champaign, USA
Markulf Kohlweiss	The University of Edinburgh, UK
Ilan Komargodski	NTT Research, USA
Huijia Lin	University of Washington, USA
Mohammad Mahmoody	University of Virginia, USA
Jesper Buus Nielsen	Aarhus University, Denmark
Emmanuela Orsini	KU Leuven, Belgium
Sunoo Park	MIT and Harvard University, USA

Anat Paskin-Cherniavsky	Ariel University, Israel
Oxana Poburinnaya	Simons Institute for the Theory of Computing, USA
Silas Richelson	University of California, Riverside, USA
Alon Rosen	IDC Herzliya, Israel
Abhi Shelat	Northeastern University, USA
Nicholas Spooner	University of California, Berkeley, USA
Uri Stemmer	Ben-Gurion University of the Negev, Israel
Justin Thaler	Georgetown University, USA
Daniel Wichs	Northeastern University and NTT Research, USA
Eylon Yogev	Boston University, USA, and Tel Aviv University, Israel

External Reviewers

Hamza Abusalah
Amit Agarwal
Archita Agarwal
Divesh Aggarwal
Navid Alamati
Younes Talibi Alaoui
Bar Alon
Joel Alwen
Joël Alwen
Miguel Ambrona
Ghous Amjad
Christian Badertscher
Saikrishna Badrinarayanan
James Bartusek
Balthazar Bauer
Carsten Baum
Alex Block
Alexander Block
Jonathan Bootle
Adam Bouland
Elette Boyle
Zvika Brakerski
Pedro Branco
Benedikt Bünz
Alper Cakan
Matteo Campanelli
Wouter Castryck
Hubert Chan
Lijie Chen
Yanlin Chen
Yilei Chen
Ilaria Chillotti
Arka Rai Choudhuri
Hao Chung
Michele Ciampi
Katriel Cohn-Gordon
Sandro Coretti
Sandro Coretti-Drayton
Henry Corrigan-Gibbs
Geoffroy Couteau
Dana Dachman-Soled
Hila Dahari
Jost Daniel
Pratish Datta
Bernardo David
Bernardo Machado David
Gareth Davies
Akshay Degwekar
Jack Doerner
Rafael Dowsley
Betul Durak
Betül Durak
Naomi Ephraim
Daniel Escudero
Grzegorz Fabianski
Islam Faisal
Xiong Fan
Song Fang
Antonio Faonio
Prastudy Fauzi
Serge Fehr
Rex Fernando
Ben Fisch
Cody Freitag
Shiuan Fu
Tommaso Gagliardoni
Chaya Ganesh
Sanjam Garg
Romain Gay
Marilyn George
Marios Georgiou
Essam Ghadafi
Alexandru Gheorghiu
Satrajit Ghosh
Aarushi Goel
Sasha Golovnev
Junqing Gong
Rishab Goyal
Daniel Grier
Alex Grilo
Siyao Guo
Iftach Haitner
Britta Hale
Ariel Hamlin
Adam Blatchley Hansen
Alexander Hartl
Carmit Hazay
Javier Herranz
Kyle Hogan
Thibaut Horel
Yao-Ching Hsieh
James Hulett

Shih-Han Hung
Rawane Issa
Håkon Jacobsen
Aayush Jain
Abhishek Jain
Ruta Jawale
Zhengzhong Jin
Fatih Kaleoglu
Chethan Kamath
Simon Holmgaard Kamp
Pihla Karanko
Shuichi Katsumata
Tomasz Kazana
Thomas Kerber
Fuyuki Kitagawa
Susumu Kiyoshima
Michael Klooß
Dima Kogan
Dmitry Kogan
Lisa Kohl
Yash Kondi
Yashvanth Kondi
Venkata Koppula
Ashutosh Kumar
Po-Chun Kuo
Thijs Laarhoven
Fabien Laguillaumie
Kasper Green Larsen
Eysa Lee
Seunghoon Lee
Yi Lee
Tancrède Lepoint
Xiao Liang
Chengyu Lin
Wei-Kai Lin
Yao-Ting Lin
Quanquan Liu
Tianren Liu
Alex Lombardi
Sébastien Lord
Julian Loss
George Lu
Ji Luo
Fermi Ma
Yi-Hsin Ma
Urmila Mahadev
Saeed Mahloujifar
Christian Majenz
Nikolaos Makriyannis
Giulio Malavolta
Mary Maller
Easwar Mangipudi
Nathan Manohar
Jeremias Mechler
Pierre Meyer
Tarik Moataz
Tomoyuki Morimae
Tamer Mour
Marta Mularczyk
Jörn Müller-Quade
Ryo Nishimaki
Olga Nissenbaum
Adam O'Neill
Maciej Obremski
Michele Orrù
Elena Pagnin
Georgios Panagiotakos
Omer Paneth
Alain Passelègue
Sikhar Patranabis
Alice Pellet–Mary
Rafael Del Pino
Rolando La Placa
Antoine Plouviez
Antigoni Polychroniadou
Sihang Pu
Chen Qian
Luowen Qian
Willy Quach
Jordi Ribes-González
Thomas Ricosset
Schuyler Rosefield
Dragos Rotaru
Lior Rotem
Sylvain Ruhault
Alexander Russell
Paul Rösler
Pratik Sarkar
Or Sattath
Sarah Scheffler
Adam Sealfon
Gil Segev
Ido Shahaf
Sina Shiehian
Omri Shmueli
Jad Silbak
Mark Simkin
Luisa Siniscalchi
Marjan Skrobot
Fang Song
Pratik Soni
Akshayaram Srinivasan
Ron Steinfeld
Patrick Struck
Marika Swanberg
Akira Takahashi
Aravind Thyagarajan
Rotem Tsabary
Yiannis Tselekounis
Prashant Vasudevan
Muthuramakrishnan Venkitasubramaniam
Daniele Venturi
Mikhail Volkhov
Philip Wadler
Hendrik Waldner
Mingyuan Wang
Tianhao Wang
Rachit Garg and Brent Waters
Hoeteck Wee
Weiqiang Wen
Jeroen van Wier
David Wu
Sophia Yakoubov
Takashi Yamakawa
Lisa Yang
Kevin Yeo
Michal Zajac
Mark Zhandry
Bingsheng Zhang
Chen-Da Liu Zhang
Hong-Sheng Zhou
Jiadong Zhu
Vassilis Zikas
Georgios Zirdelis

Contents – Part II