

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

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 III

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 978-3-030-64380-5 ISBN 978-3-030-64381-2 (eBook)
<https://doi.org/10.1007/978-3-030-64381-2>

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2020

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

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

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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 Brzuska

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 Döttling

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 Jafarholi

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 Yogeve	Boston University, USA, and Tel Aviv University, Israel

External Reviewers

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

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

Contents – Part III

Universal Composition with Global Subroutines: Capturing Global Setup Within Plain UC	1
<i>Christian Badertscher, Ran Canetti, Julia Hesse, Björn Tackmann, and Vassilis Zikas</i>	
Security Analysis of SPAKE2 +	31
<i>Victor Shoup</i>	
Schrödinger’s Pirate: How to Trace a Quantum Decoder	61
<i>Mark Zhandry</i>	
Quantum Encryption with Certified Deletion	92
<i>Anne Broadbent and Rabib Islam</i>	
Secure Quantum Extraction Protocols	123
<i>Prabhanjan Ananth and Rolando L. La Placa</i>	
Non-interactive Classical Verification of Quantum Computation	153
<i>Gorjan Alagic, Andrew M. Childs, Alex B. Grilo, and Shih-Han Hung</i>	
Classical Verification of Quantum Computations with Efficient Verifier.	181
<i>Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa</i>	
Coupling of Random Systems.	207
<i>David Lanzenberger and Ueli Maurer</i>	
Towards Defeating Backdoored Random Oracles: Indifferentiability with Bounded Adaptivity	241
<i>Yevgeniy Dodis, Pooya Farshim, Sogol Mazaheri, and Stefano Tessaro</i>	
Zero-Communication Reductions.	274
<i>Varun Narayanan, Manoj Prabhakaran, and Vinod M. Prabhakaran</i>	
Lower Bounds on the Time/Memory Tradeoff of Function Inversion.	305
<i>Dror Chawin, Itzhak Haitner, and Noam Mazon</i>	
Super-Linear Time-Memory Trade-Offs for Symmetric Encryption	335
<i>Wei Dai, Stefano Tessaro, and Xihu Zhang</i>	
Algebraic Distinguishers: From Discrete Logarithms to Decisional Uber Assumptions.	366
<i>Lior Rotem and Gil Segev</i>	

On the Security of Time-Lock Puzzles and Timed Commitments	390
<i>Jonathan Katz, Julian Loss, and Jiayu Xu</i>	
Expected-Time Cryptography: Generic Techniques and Applications to Concrete Soundness.	414
<i>Joseph Jaeger and Stefano Tessaro</i>	
On the Complexity of Arithmetic Secret Sharing.	444
<i>Ronald Cramer, Chaoping Xing, and Chen Yuan</i>	
Robust Secret Sharing with Almost Optimal Share Size and Security Against Rushing Adversaries	470
<i>Serge Fehr and Chen Yuan</i>	
The Share Size of Secret-Sharing Schemes for Almost All Access Structures and Graphs	499
<i>Amos Beimel and Oriol Farràs</i>	
Transparent Error Correcting in a Computationally Bounded World.	530
<i>Ofer Grossman, Justin Holmgren, and Eylon Yogev</i>	
New Techniques in Replica Encodings with Client Setup.	550
<i>Rachit Garg, George Lu, and Brent Waters</i>	
Non-malleable Codes, Extractors and Secret Sharing for Interleaved Tampering and Composition of Tampering.	584
<i>Eshan Chattopadhyay and Xin Li</i>	
On Average-Case Hardness in TFNP from One-Way Functions	614
<i>Pavel Hubáček, Chethan Kamath, Karel Král, and Veronika Slívová</i>	
On Pseudorandom Encodings	639
<i>Thomas Agrikola, Geoffroy Couteau, Yuval Ishai, Stanisław Jarecki, and Amit Sahai</i>	
Author Index	671