# Lecture Notes in Computer Science 12550


## 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 I

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 978-3-030-64374-4 ISBN 978-3-030-64375-1 (eBook)
https://doi.org/10.1007/978-3-030-64375-1

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 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 | 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 Badrinarayanan | Jost Daniel | Satrajit Ghosh |
| | 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 Bouland | 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
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 I


Lossiness and Entropic Hardness for Ring-LWE . . . . . 1
*Zvika Brakerski and Nico Döttling*

Multi-key Fully-Homomorphic Encryption in the Plain Model . . . . . 28
*Prabhanjan Ananth, Abhishek Jain, Zhengzhong Jin, and Giulio Malavolta*

Constant Ciphertext-Rate Non-committing Encryption from Standard Assumptions . . . . . 58
*Zvika Brakerski, Pedro Branco, Nico Döttling, Sanjam Garg, and Giulio Malavolta*

Efficient Range-Trapdoor Functions and Applications: Rate-1 OT and More . . . . . 88
*Sanjam Garg, Mohammad Hajiabadi, and Rafail Ostrovsky*

CP-ABE for Circuits (and More) in the Symmetric Key Setting . . . . . 117
*Shweta Agrawal and Shota Yamada*

Optimal Broadcast Encryption from LWE and Pairings in the Standard Model . . . . . 149
*Shweta Agrawal, Daniel Wichs, and Shota Yamada*

Equipping Public-Key Cryptographic Primitives with Watermarking (or: A Hole Is to Watermark) . . . . . 179
*Ryo Nishimaki*

Functional Encryption for Quadratic Functions from $k$-Lin, Revisited . . . . . 210
*Hoeteck Wee*

On Perfect Correctness in (Lockable) Obfuscation . . . . . 229
*Rishab Goyal, Venkata Koppula, Satyanarayana Vusirikala, and Brent Waters*

Can a Public Blockchain Keep a Secret? . . . . . 260
*Fabrice Benhamouda, Craig Gentry, Sergey Gorbunov, Shai Halevi, Hugo Krawczyk, Chengyu Lin, Tal Rabin, and Leonid Reyzin*

Blockchains from Non-idealized Hash Functions . . . . . 291
*Juan A. Garay, Aggelos Kiayias, and Giorgos Panagiotakos*

Ledger Combiners for Fast Settlement . . . . . 322
*Matthias Fitzi, Peter Gaži, Aggelos Kiayias, and Alexander Russell*

Asynchronous Byzantine Agreement with Subquadratic Communication . . . . 353
*Erica Blum, Jonathan Katz, Chen-Da Liu-Zhang, and Julian Loss*

Expected Constant Round Byzantine Broadcast Under Dishonest Majority . . . 381
*Jun Wan, Hanshen Xiao, Elaine Shi, and Srinivas Devadas*

Round-Efficient Byzantine Broadcast Under Strongly Adaptive and Majority Corruptions . . . . . 412
*Jun Wan, Hanshen Xiao, Srinivas Devadas, and Elaine Shi*

A Lower Bound for One-Round Oblivious RAM . . . . . 457
*David Cash, Andrew Drucker, and Alexander Hoover*

Lower Bounds for Multi-server Oblivious RAMs . . . . . 486
*Kasper Green Larsen, Mark Simkin, and Kevin Yeo*

On Computational Shortcuts for Information-Theoretic PIR . . . . . 504
*Matthew M. Hong, Yuval Ishai, Victor I. Kolobov, and Russell W. F. Lai*

Characterizing Deterministic-Prover Zero Knowledge . . . . . 535
*Nir Bitansky and Arka Rai Choudhuri*

NIZK from SNARG . . . . . 567
*Fuyuki Kitagawa, Takahiro Matsuda, and Takashi Yamakawa*

Weakly Extractable One-Way Functions . . . . . 596
*Nir Bitansky, Noa Eizenstadt, and Omer Paneth*

Towards Non-interactive Witness Hiding . . . . . 627
*Benjamin Kuykendall and Mark Zhandry*

FHE-Based Bootstrapping of Designated-Prover NIZK . . . . . 657
*Zvika Brakerski, Sanjam Garg, and Rotem Tsabary*

Perfect Zero Knowledge: New Upperbounds and Relativized Separations . . . . 684
*Peter Dixon, Sutanu Gayen, A. Pavan, and N. V. Vinodchandran*

**Author Index** . . . . . 705

# Contents – Part II

Recursive Proof Composition from Accumulation Schemes . . . . . 1
*Benedikt Bünz, Alessandro Chiesa, Pratyush Mishra, and Nicholas Spooner*

Linear-Time Arguments with Sublinear Verification from Tensor Codes . . . . 19
*Jonathan Bootle, Alessandro Chiesa, and Jens Groth*

Barriers for Succinct Arguments in the Random Oracle Model . . . . . 47
*Alessandro Chiesa and Eylon Yogev*

Accumulators in (and Beyond) Generic Groups: Non-trivial Batch Verification Requires Interaction . . . . . 77
*Gili Schul-Ganz and Gil Segev*

Batch Verification and Proofs of Proximity with Polylog Overhead . . . . . 108
*Guy N. Rothblum and Ron D. Rothblum*

Batch Verification for Statistical Zero Knowledge Proofs . . . . . 139
*Inbar Kaslasi, Guy N. Rothblum, Ron D. Rothblum, Adam Sealfon, and Prashant Nalini Vasudevan*

Public-Coin Zero-Knowledge Arguments with (almost) Minimal Time and Space Overheads . . . . . 168
*Alexander R. Block, Justin Holmgren, Alon Rosen, Ron D. Rothblum, and Pratik Soni*

On the Price of Concurrency in Group Ratcheting Protocols . . . . . 198
*Alexander Bienstock, Yevgeniy Dodis, and Paul Rösler*

Stronger Security and Constructions of Multi-designated Verifier Signatures . . . . . 229
*Ivan Damgård, Helene Haagh, Rebekah Mercer, Anca Nitulescu, Claudio Orlandi, and Sophia Yakoubov*

Continuous Group Key Agreement with Active Security . . . . . 261
*Joël Alwen, Sandro Coretti, Daniel Jost, and Marta Mularczyk*

Round Optimal Secure Multiparty Computation from Minimal Assumptions . . . . . 291
*Arka Rai Choudhuri, Michele Ciampi, Vipul Goyal, Abhishek Jain, and Rafail Ostrovsky*

Reusable Two-Round MPC from DDH . . . . . 320
*James Bartusek, Sanjam Garg, Daniel Masny, and Pratyay Mukherjee*

Mr NISC: Multiparty Reusable Non-Interactive Secure Computation . . . . . 349
*Fabrice Benhamouda and Huijia Lin*

Secure Massively Parallel Computation for Dishonest Majority . . . . . 379
*Rex Fernando, Ilan Komargodski, Yanyi Liu, and Elaine Shi*

Towards Multiparty Computation Withstanding Coercion of All Parties . . . . . 410
*Ran Canetti and Oxana Poburinnaya*

Synchronous Constructive Cryptography . . . . . 439
*Chen-Da Liu-Zhang and Ueli Maurer*

Topology-Hiding Communication from Minimal Assumptions . . . . . 473
*Marshall Ball, Elette Boyle, Ran Cohen, Lisa Kohl, Tal Malkin, Pierre Meyer, and Tal Moran*

Information-Theoretic 2-Round MPC Without Round Collapsing: Adaptive Security, and More . . . . . 502
*Huijia Lin, Tianren Liu, and Hoeteck Wee*

On Statistical Security in Two-Party Computation . . . . . 532
*Dakshita Khurana and Muhammad Haris Mughees*

The Resiliency of MPC with Low Interaction: The Benefit of Making Errors (Extended Abstract) . . . . . 562
*Benny Applebaum, Eliran Kachlon, and Arpita Patra*

Revisiting Fairness in MPC: Polynomial Number of Parties and General Adversarial Structures . . . . . 595
*Dana Dachman-Soled*

On the Power of an Honest Majority in Three-Party Computation Without Broadcast . . . . . 621
*Bar Alon, Ran Cohen, Eran Omri, and Tom Suad*

A Secret-Sharing Based MPC Protocol for Boolean Circuits with Good Amortized Complexity . . . . . 652
*Ignacio Cascudo and Jaron Skovsted Gundersen*

On the Round Complexity of the Shuffle Model . . . . . 683
*Amos Beimel, Iftach Haitner, Kobbi Nissim, and Uri Stemmer*

**Author Index** . . . . . 713

# Contents – Part III

Universal Composition with Global Subroutines: Capturing Global Setup Within Plain UC . . . . . 1
*Christian Badertscher, Ran Canetti, Julia Hesse, Björn Tackmann, and Vassilis Zikas*

Security Analysis of *SPAKE2+* . . . . . 31
*Victor Shoup*

Schrödinger's Pirate: How to Trace a Quantum Decoder . . . . . 61
*Mark Zhandry*

Quantum Encryption with Certified Deletion . . . . . 92
*Anne Broadbent and Rabib Islam*

Secure Quantum Extraction Protocols . . . . . 123
*Prabhanjan Ananth and Rolando L. La Placa*

Non-interactive Classical Verification of Quantum Computation . . . . . 153
*Gorjan Alagic, Andrew M. Childs, Alex B. Grilo, and Shih-Han Hung*

Classical Verification of Quantum Computations with Efficient Verifier . . . . . 181
*Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa*

Coupling of Random Systems . . . . . 207
*David Lanzenberger and Ueli Maurer*

Towards Defeating Backdoored Random Oracles: Indifferentiability with Bounded Adaptivity . . . . . 241
*Yevgeniy Dodis, Pooya Farshim, Sogol Mazaheri, and Stefano Tessaro*

Zero-Communication Reductions . . . . . 274
*Varun Narayanan, Manoj Prabhakaran, and Vinod M. Prabhakaran*

Lower Bounds on the Time/Memory Tradeoff of Function Inversion . . . . . 305
*Dror Chawin, Iftach Haitner, and Noam Mazor*

Super-Linear Time-Memory Trade-Offs for Symmetric Encryption . . . . . 335
*Wei Dai, Stefano Tessaro, and Xihu Zhang*

Algebraic Distinguishers: From Discrete Logarithms to Decisional Uber Assumptions . . . . . 366
*Lior Rotem and Gil Segev*

On the Security of Time-Lock Puzzles and Timed Commitments . . . . . 390
*Jonathan Katz, Julian Loss, and Jiayu Xu*

Expected-Time Cryptography: Generic Techniques and Applications to Concrete Soundness . . . . . 414
*Joseph Jaeger and Stefano Tessaro*

On the Complexity of Arithmetic Secret Sharing . . . . . 444
*Ronald Cramer, Chaoping Xing, and Chen Yuan*

Robust Secret Sharing with Almost Optimal Share Size and Security Against Rushing Adversaries . . . . . 470
*Serge Fehr and Chen Yuan*

The Share Size of Secret-Sharing Schemes for Almost All Access Structures and Graphs . . . . . 499
*Amos Beimel and Oriol Farràs*

Transparent Error Correcting in a Computationally Bounded World . . . . . 530
*Ofer Grossman, Justin Holmgren, and Eylon Yogev*

New Techniques in Replica Encodings with Client Setup . . . . . 550
*Rachit Garg, George Lu, and Brent Waters*

Non-malleable Codes, Extractors and Secret Sharing for Interleaved Tampering and Composition of Tampering . . . . . 584
*Eshan Chattopadhyay and Xin Li*

On Average-Case Hardness in TFNP from One-Way Functions . . . . . 614
*Pavel Hubáček, Chethan Kamath, Karel Král, and Veronika Slívová*

On Pseudorandom Encodings . . . . . 639
*Thomas Agrikola, Geoffroy Couteau, Yuval Ishai, Stanisław Jarecki, and Amit Sahai*

**Author Index** . . . . . 671