

## 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 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

*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

© International Association for Cryptologic Research 2019

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 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	University of Rochester, USA
Venkitasubramaniam	
Yu Yu	Shanghai Jiaotong University, China

## External Reviewers

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

## Contents – Part II

Succinct Arguments in the Quantum Random Oracle Model. . . . .	1
<i>Alessandro Chiesa, Peter Manohar, and Nicholas Spooner</i>	
Delegating Quantum Computation in the Quantum Random Oracle Model. . .	30
<i>Jiayu Zhang</i>	
Tighter Proofs of CCA Security in the Quantum Random Oracle Model . . . .	61
<i>Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, and Edoardo Persichetti</i>	
Attribute Based Encryption for Deterministic Finite Automata from DLIN . . .	91
<i>Shweta Agrawal, Monosij Maitra, and Shota Yamada</i>	
CPA-to-CCA Transformation for KDM Security . . . . .	118
<i>Fuyuki Kitagawa and Takahiro Matsuda</i>	
New Approaches to Traitor Tracing with Embedded Identities . . . . .	149
<i>Rishab Goyal, Venkata Koppula, and Brent Waters</i>	
A Unified and Composable Take on Ratcheting . . . . .	180
<i>Daniel Jost, Ueli Maurer, and Marta Mularczyk</i>	
Continuously Non-malleable Secret Sharing for General Access Structures. . .	211
<i>Gianluca Brian, Antonio Faonio, and Daniele Venturi</i>	
Interactive Non-malleable Codes . . . . .	233
<i>Nils Fleischhacker, Vipul Goyal, Abhishek Jain, Anat Paskin-Cherniavsky, and Slava Radune</i>	
Stronger Lower Bounds for Online ORAM . . . . .	264
<i>Pavel Hubáček, Michal Koucký, Karel Král, and Veronika Slívová</i>	
Adaptively Secure Garbling Schemes for Parallel Computations . . . . .	285
<i>Kai-Min Chung and Luowen Qian</i>	
Statistical Difference Beyond the Polarizing Regime . . . . .	311
<i>Itay Berman, Akshay Degwekar, Ron D. Rothblum, and Prashant Nalini Vasudevan</i>	
Estimating Gaps in Martingales and Applications to Coin-Tossing: Constructions and Hardness . . . . .	333
<i>Hamidreza Amini Khorasgani, Hemanta K. Maji, and Tamalika Mukherjee</i>	

<b>Fully Homomorphic NIZK and NIWI Proofs . . . . .</b>	<b>356</b>
<i>Prabhanjan Ananth, Apoorvaa Deshpande, Yael Tauman Kalai, and Anna Lysyanskaya</i>	
<b>Lower and Upper Bounds on the Randomness Complexity of Private Computations of AND. . . . .</b>	<b>386</b>
<i>Eyal Kushilevitz, Rafail Ostrovsky, Emmanuel Prouff, Adi Rosén, Adrian Thillard, and Damien Vergnaud</i>	
<b>Leveraging Linear Decryption: Rate-1 Fully-Homomorphic Encryption and Time-Lock Puzzles . . . . .</b>	<b>407</b>
<i>Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta</i>	
<b>Compressible FHE with Applications to PIR . . . . .</b>	<b>438</b>
<i>Craig Gentry and Shai Halevi</i>	
<b>Permuted Puzzles and Cryptographic Hardness . . . . .</b>	<b>465</b>
<i>Elette Boyle, Justin Holmgren, and Mor Weiss</i>	
<b>Linear-Size Constant-Query IOPs for Delegating Computation . . . . .</b>	<b>494</b>
<i>Eli Ben-Sasson, Alessandro Chiesa, Lior Goldberg, Tom Gur, Michael Riabzev, and Nicholas Spooner</i>	
<b>On the (In)security of Kilian-Based SNARGs . . . . .</b>	<b>522</b>
<i>James Bartusek, Liron Bronfman, Justin Holmgren, Fermi Ma, and Ron D. Rothblum</i>	
<b>Incrementally Verifiable Computation via Incremental PCPs. . . . .</b>	<b>552</b>
<i>Moni Naor, Omer Paneth, and Guy N. Rothblum</i>	
<b>Author Index . . . . .</b>	<b>577</b>

# Contents – Part I

Algebraically Structured LWE, Revisited . . . . .	1
<i>Chris Peikert and Zachary Pepin</i>	
Lattice Trapdoors and IBE from Middle-Product LWE . . . . .	24
<i>Alex Lombardi, Vinod Vaikuntanathan, and Thuy Duong Vuong</i>	
Matrix PRFs: Constructions, Attacks, and Applications to Obfuscation . . . . .	55
<i>Yilei Chen, Minki Hhan, Vinod Vaikuntanathan, and Hoeteck Wee</i>	
Obfuscated Fuzzy Hamming Distance and Conjunctions from Subset Product Problems . . . . .	81
<i>Steven D. Galbraith and Lukas Zobernig</i>	
A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement . . . . .	111
<i>Daniele Friolo, Daniel Masny, and Daniele Venturi</i>	
Synchronous Consensus with Optimal Asynchronous Fallback Guarantees . . .	131
<i>Erica Blum, Jonathan Katz, and Julian Loss</i>	
Predicate Encryption from Bilinear Maps and One-Sided Probabilistic Rank . . . . .	151
<i>Josh Alman and Robin Hui</i>	
Optimal Bounded-Collusion Secure Functional Encryption . . . . .	174
<i>Prabhanjan Ananth and Vinod Vaikuntanathan</i>	
From FE Combiners to Secure MPC and Back . . . . .	199
<i>Prabhanjan Ananth, Saikrishna Badrinarayanan, Aayush Jain, Nathan Manohar, and Amit Sahai</i>	
(Pseudo) Random Quantum States with Binary Phase . . . . .	229
<i>Zvika Brakerski and Omri Shmueli</i>	
General Linear Group Action on Tensors: A Candidate for Post-quantum Cryptography . . . . .	251
<i>Zhengfeng Ji, Youming Qiao, Fang Song, and Aaram Yun</i>	
Composable and Finite Computational Security of Quantum Message Transmission . . . . .	282
<i>Fabio Banfi, Ueli Maurer, Christopher Portmann, and Jiamin Zhu</i>	

On Fully Secure MPC with Solitary Output . . . . .	312
<i>Shai Halevi, Yuval Ishai, Eyal Kushilevitz, Nikolaos Makriyannis, and Tal Rabin</i>	
Secure Computation with Preprocessing via Function Secret Sharing . . . . .	341
<i>Elette Boyle, Niv Gilboa, and Yuval Ishai</i>	
Efficient Private PEZ Protocols for Symmetric Functions . . . . .	372
<i>Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta</i>	
The Function-Inversion Problem: Barriers and Opportunities . . . . .	393
<i>Henry Corrigan-Gibbs and Dmitry Kogan</i>	
On the Complexity of Collision Resistant Hash Functions: New and Old Black-Box Separations. . . . .	422
<i>Nir Bitansky and Akshay Degwekar</i>	
Characterizing Collision and Second-Preimage Resistance in Linicrypt. . . . .	451
<i>Ian McQuoid, Trevor Swope, and Mike Rosulek</i>	
Efficient Information-Theoretic Secure Multiparty Computation over $\mathbb{Z}/p^k\mathbb{Z}$ via Galois Rings . . . . .	471
<i>Mark Abspoel, Ronald Cramer, Ivan Damgård, Daniel Escudero, and Chen Yuan</i>	
Is Information-Theoretic Topology-Hiding Computation Possible?. . . . .	502
<i>Marshall Ball, Elette Boyle, Ran Cohen, Tal Malkin, and Tal Moran</i>	
Channels of Small Log-Ratio Leakage and Characterization of Two-Party Differentially Private Computation . . . . .	531
<i>Iftach Haitner, Noam Mazon, Ronen Shaltiel, and Jad Silbak</i>	
On Perfectly Secure 2PC in the OT-Hybrid Model . . . . .	561
<i>Bar Alon and Anat Paskin-Cherniavsky</i>	
<b>Author Index . . . . .</b>	<b>597</b>