

Kobbi Nissim  
Brent Waters (Eds.)

LNCS 13043

# Theory of Cryptography

19th International Conference, TCC 2021  
Raleigh, NC, USA, November 8–11, 2021  
Proceedings, Part II

2  
Part II



 Springer

## 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>

Kobbi Nissim · Brent Waters (Eds.)

# Theory of Cryptography

19th International Conference, TCC 2021  
Raleigh, NC, USA, November 8–11, 2021  
Proceedings, Part II

*Editors*

Kobbi Nissim  
Georgetown University  
Washington, WA, USA

Brent Waters  
The University of Texas at Austin  
Austin, TX, USA

NTT Research  
Sunnyvale, CA, USA

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-90452-4              ISBN 978-3-030-90453-1 (eBook)  
<https://doi.org/10.1007/978-3-030-90453-1>

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2021

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 19th Theory of Cryptography Conference (TCC 2021) was held during November 8–11, 2021 at North Carolina State University in Raleigh, USA. It was sponsored by the International Association for Cryptologic Research (IACR). The general chair of the conference was Alessandra Scafuro.

The conference received 161 submissions, of which the Program Committee (PC) selected 66 for presentation giving an acceptance rate of 41%. Each submission was reviewed by at least four PC members. The 43 PC members (including PC chairs), all top researchers in our field, were helped by 197 external reviewers, who were consulted when appropriate. These proceedings consist of the revised version of the 66 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 Submission and 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 seventh 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: “Keyword Search and Oblivious Pseudorandom Functions” by Michael Freedman, Yuval Ishai, Benny Pinkas, and Omer Reingold. The award committee recognized this paper for “introducing and formalizing the notion of Oblivious Pseudorandom Functions, and identifying connections to other primitives such as keyword search, inspiring a vast amount of theoretical and practical work”.

We are greatly indebted to many people who were involved in making TCC 2021 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, Kevin McCurley, Kay McKelly, and the TCC Steering Committee.

October 2021

Kobbi Nissim  
Brent Waters

# Organization

## General Chair

Alessandra Scafuro North Carolina State University, USA

## Program Chairs

Kobbi Nissim Georgetown University, USA  
Brent Waters NTT Research and University of Texas at Austin, USA

## Program Committee

Masayuki Abe NTT, Japan  
Ittai Abraham VMware, Israel  
Benny Applebaum Tel Aviv University, Israel  
Gilad Asharov Bar-Ilan University, Israel  
Amos Beimel Ben-Gurion University, Israel  
Andrej Bogdanov Chinese University of Hong Kong, Hong Kong  
Elette Boyle IDC Herzliya, Israel  
Chris Brzuska Aalto University, Finland  
Mark Bun Boston University, USA  
Yilei Chen Tsinghua University, China  
Itai Dinur Ben-Gurion University, Israel  
Pooya Farshim University of York, UK  
Sanjam Garg NTT Research and UC Berkeley, USA  
Rishab Goyal MIT, USA  
Siyao Guo NYU Shanghai, China  
Iftach Haitner Tel Aviv University, Israel  
Mohammad Hajiabadi University of Waterloo, Canada  
Carmit Hazay Bar-Ilan University, Israel  
Yuval Ishai Technion, Israel  
Abhishek Jain Johns Hopkins University, USA  
Stacey Jeffery CWI, The Netherlands  
Lisa Kohl CWI, The Netherlands  
Ilan Komargodski NTT Research and Hebrew University, Israel  
Benoit Libert CNRS and ENS de Lyon, France  
Huijia Lin University of Washington, USA  
Alex Lombardi MIT, USA  
Vadim Lyubashevsky IBM Research - Zurich, Switzerland  
Jesper Buus Nielsen Aarhus University, Denmark  
Ryo Nishimaki NTT, USA  
Omkant Pandey Stony Brook University, USA

Omer Paneth	Tel Aviv University, Israel
Manoj Prabhakaran	ITT Bombay, India
Leo Reyzin	Boston University, USA
Alon Rosen	Bocconi University, Italy, and IDC Herzliya, Israel
Guy Rothblum	Weizmann Institute of Science, Israel
Christian Schaffner	QuSoft and University of Amsterdam, The Netherlands
Peter Scholl	Aarhus University, Denmark
Gil Segev	Hebrew University, Israel
Justin Thaler	Georgetown University, USA
Muthu Venkitasubramaniam	Georgetown University, USA
Mark Zhandry	NTT Research and Princeton University, USA

## External Reviewers

Christian Badertscher	Leo De Castro	Jiaxin Guan
Mingyuan Wang	Suvradip Chakraborty	Divya Gupta
Damiano Abram	Sun Chao	Shai Halevi
Anasuya Acharya	Nai-Hui Chia	Mathias Hall-Andersen
Shweta Agrawal	Arka Rai Choudhuri	Hamidreza Khoshakhlagh
Adi Akavia	Ashish Choudhury	Patrick Harasser
Gorjan Alagic	Hao Chung	Dominik Hartmann
Bar Alon	Kai-Min Chung	Brett Hemenway
Pedro Alves	Michele Ciampi	Justin Holmgren
Miguel Ambrona	Geoffroy Couteau	Thibaut Horel
Prabhanjan Ananth	Jan Czajkowski	Pavel Hubacek
Ananya Appan	Amit Deo	Aayush Jain
Anirudh C.	Jelle Don	Dingding Jia
Gal Arnon	Xiaoqi Duan	Zhengzhong Jin
Thomas Attema	Leo Ducas	Eliran Kachlon
Benedikt Bünz	Yfke Dulek	Gabriel Kaptchuk
Laasya Bangalore	Christoph Egger	Pihla Karanko
James Bartusek	Jaiden Keith Fairoze	Akinori Kawachi
Balthazar Bauer	Islam Faisal	Jiseung Kim
Sina Shiehian	Luca de Feo	Fuyuki Kitagawa
Ward Beullens	Cody Freitag	Susumu Kiyoshima
Rishabh Bhaduria	Georg Fuchsbauer	Anders Konrig
Kaartik Bhushan	Chaya Ganesh	Venkata Koppula
Nir Bitansky	Juan Garay	Ben Kuykendall
Olivier Blazy	Rachit Garg	Changmin Lee
Alex Block	Romain Gay	Baiyu Li
Estuardo Alperez Bock	Nicholas Genise	Xiao Liang
Jonathan Bootle	Ashruijit Ghoshal	Wei-Kai Lin
Lennart Braun	Niv Gilboa	Jiahui Liu
Konstantinos Brazitikos	Aarushi Goel	Qipeng Liu
Ignacio Cascudo	Junqing Gong	Tianren Liu



Sébastien Lord	Alexander Poremba	Atsushi Takayasu
Julian Loss	Kirthivaasan Puniamurthy	Aishwarya
George Lu	Willy Quach	Thiruvengadam
Ji Luo	Yuan Quan	Søren Eller Thomsen
Fermi Ma	Rajeev Raghunath	Pratyush Ranjan Tiwari
Bernardo Magri	Divya Ravi	Alin Tomescu
Mohammad Mahmoody	João Ribeiro	Junichi Tomida
Sven Maier	Peter Rindal	Ni Trieu
Monosij Maitra	Felix Rohrbach	Eliad Tsfadia
Christian Majenz	Lior Rotem	Rohit Chatterjee
Nikolaos Makriyannis	Ron Rothblum	Xiao Liang
Giulio Malavolta	Mike Rosulek	Neekon Vafa
Noam Mazor	Rahul B. S.	Mayank Varia
Audra McMillan	Benjamin Schlosser	Prashant Vasudevan
Jeremias Mechler	André Schrottenloher	Satyanarayana Vusirikala
Pierre Meyer	Gili Schul-Ganz	Alexandre Wallet
Peihan Miao	Nikolaj Schwartzbach	Mingyuan Wang
Brice Minaud	Sruthi Sekar	Mor Weiss
Pratyush Mishra	Srinath Setty	Douglas Wickstorm
Tarik Moataz	Sina Shiehian	David Wu
Tamer Mour	Manasi Shingane	Keita Xagawa
Varun Narayanan	Omri Shmueli	Zhuolun Xiang
Ngoc Khanh Nguyen	Jad Silbak	Shota Yamada
Oded Nir	Mark Simkin	Takashi Yamakawa
Ariel Nof	Jaspal Singh	Avishay Yanai
Adam O'Neill	Luisa Siniscalchi	Kevin Yeo
Sabine Oechsner	Adam Smith	Wang Yuyu
Eran Omri	Pratik Soni	Shang Zehua
Jiaxing Pan	Jana Sotáková	Chen-Da Liu Zhang
Anat Paskin-Cherniavsky	Akshayaram Srinivasan	Cong Zhang
Alain Passelègue	Noah	Jiapeng Zhang
Naty Peter	Stephens-Davidowitz	Yiding Zhang
Thomas Peters	Gilad Stern	Yinuo Zhang
Rolando La Placa	Patrick Struck	Yupeng Zhang
Bertram Poettering	Hyung Tae	Giorgos Zirdelis
Antigoni Polychroniadou	Mehrdad Tahmasbi	Sebastian Zur

## Contents – Part II

Dory: Efficient, Transparent Arguments for Generalised Inner Products and Polynomial Commitments . . . . .	1
<i>Jonathan Lee</i>	
On Communication-Efficient Asynchronous MPC with Adaptive Security . . .	35
<i>Annick Chopard, Martin Hirt, and Chen-Da Liu-Zhang</i>	
Efficient Perfectly Secure Computation with Optimal Resilience . . . . .	66
<i>Itai Abraham, Gilad Asharov, and Avishay Yanai</i>	
On Communication Models and Best-Achievable Security in Two-Round MPC . . . . .	97
<i>Aarushi Goel, Abhishek Jain, Manoj Prabhakaran, and Rajeev Raghunath</i>	
Generalized Pseudorandom Secret Sharing and Efficient Straggler-Resilient Secure Computation . . . . .	129
<i>Fabrice Benhamouda, Elette Boyle, Niv Gilboa, Shai Halevi, Yuval Ishai, and Ariel Nof</i>	
Blockchains Enable Non-interactive MPC . . . . .	162
<i>Vipul Goyal, Elisaweta Masserova, Bryan Parno, and Yifan Song</i>	
Multi-party PSM, Revisited: Improved Communication and Unbalanced Communication. . . . .	194
<i>Léonard Assouline and Tianren Liu</i>	
Multi-Party Functional Encryption. . . . .	224
<i>Shweta Agrawal, Rishab Goyal, and Junichi Tomida</i>	
Succinct LWE Sampling, Random Polynomials, and Obfuscation . . . . .	256
<i>Lalita Devadas, Willy Quach, Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs</i>	
ABE for DFA from LWE Against Bounded Collusions, Revisited. . . . .	288
<i>Hoeteck Wee</i>	
Distributed Merkle’s Puzzles . . . . .	310
<i>Itai Dinur and Ben Hasson</i>	
Continuously Non-malleable Secret Sharing: Joint Tampering, Plain Model and Capacity . . . . .	333
<i>Gianluca Brian, Antonio Faonio, and Daniele Venturi</i>	

Disappearing Cryptography in the Bounded Storage Model . . . . .	365
<i>Jiaxin Guan and Mark Zhandry</i>	
Trojan-Resilience Without Cryptography . . . . .	397
<i>Suvradip Chakraborty, Stefan Dziembowski, Małgorzata Galązka, Tomasz Lizurej, Krzysztof Pietrzak, and Michelle Yeo</i>	
On Derandomizing Yao’s Weak-to-Strong OWF Construction . . . . .	429
<i>Chris Brzuska, Geoffroy Couteau, Pihla Karanko, and Felix Rohrbach</i>	
Simple Constructions from (Almost) Regular One-Way Functions . . . . .	457
<i>Noam Mazon and Jiapeng Zhang</i>	
On Treewidth, Separators and Yao’s Garbling . . . . .	486
<i>Chethan Kamath, Karen Klein, and Krzysztof Pietrzak</i>	
Oblivious Transfer from Trapdoor Permutations in Minimal Rounds . . . . .	518
<i>Arka Rai Choudhuri, Michele Ciampi, Vipul Goyal, Abhishek Jain, and Rafail Ostrovsky</i>	
The Cost of Adaptivity in Security Games on Graphs . . . . .	550
<i>Chethan Kamath, Karen Klein, Krzysztof Pietrzak, and Michael Walter</i>	
Concurrent Composition of Differential Privacy . . . . .	582
<i>Salil Vadhan and Tianhao Wang</i>	
Direct Product Hardness Amplification . . . . .	605
<i>David Lanzemberger and Ueli Maurer</i>	
On the (Ir)Replaceability of Global Setups, or How (Not) to Use a Global Ledger . . . . .	626
<i>Christian Badertscher, Julia Hesse, and Vassilis Zikas</i>	
BKW Meets Fourier New Algorithms for LPN with Sparse Parities . . . . .	658
<i>Dana Dachman-Soled, Huijing Gong, Hunter Kippen, and Aria Shahverdi</i>	
Computational Robust (Fuzzy) Extractors for CRS-Dependent Sources with Minimal Min-entropy . . . . .	689
<i>Hanwen Feng and Qiang Tang</i>	
Polynomial-Time Targeted Attacks on Coin Tossing for Any Number of Corruptions . . . . .	718
<i>Omid Etesami, Ji Gao, Saeed Mahloujifar, and Mohammad Mahmoody</i>	
<b>Author Index</b> . . . . .	<b>751</b>