Lecture Notes in Computer Science 13747

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

Moti Yung
Columbia University, New York, NY, USA

More information about this series at https://link.springer.com/bookseries/558

Eike Kiltz · Vinod Vaikuntanathan (Eds.)

Theory of Cryptography

20th International Conference, TCC 2022
Chicago, IL, USA, November 7–10, 2022
Proceedings, Part I

Springer

Editors
Eike Kiltz
Ruhr University Bochum
Bochum, Germany

Vinod Vaikuntanathan
Massachusetts Institute of Technology
Cambridge, MA, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-22317-4 ISBN 978-3-031-22318-1 (eBook)
https://doi.org/10.1007/978-3-031-22318-1

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2022
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 20th Theory of Cryptography Conference (TCC 2022) was held during November 7–10, 2022, at the University of Chicago, USA. It was sponsored by the International Association for Cryptologic Research (IACR). The general chair of the conference was David Cash.

The conference received 139 submissions, of which the Program Committee (PC) selected 60 for presentation giving an acceptance rate of 43%. Each submission was reviewed by at least three PC members in a single-blind process. The 44 PC members (including PC chairs), all top researchers in our field, were helped by 116 external reviewers, who were consulted when appropriate. These proceedings consist of the revised version of the 60 accepted papers. The revisions were not reviewed, and the authors bear full responsibility for the content of their papers.

We are extremely grateful to Kevin McCurley for providing fast and reliable technical support for the HotCRP review software 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 those about suspected bugs or unclear connections to prior work. We believe this approach improved our understanding of the papers and the quality of the review process. We also thank Kay McKelly for her fast and meticulous help with the conference website.

This was the eighth 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 2011: “Perfectly secure oblivious RAM without random oracles” by Ivan Damgård, Sigurd Meldgaard, and Jesper Buus Nielsen. The award committee recognized this paper for “the first perfectly secure unconditional Oblivious RAM scheme and for setting the stage for future Oblivious RAM and PRAM schemes”. The authors were invited to deliver a talk at TCC 2022. The conference also featured two other invited talks, by Rahul Santhanam and by Eran Tromer.

This year, TCC awarded a Best Young Researcher Award for the best paper authored solely by young researchers. The award was given to the paper “A Tight Computational Indistinguishability Bound of Product Distributions” by Nathan Geier.

We are greatly indebted to the many people who were involved in making TCC 2022 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 their correctness, and discussing the papers in depth. We thank the University of Chicago Computer Science department, Google Research, Algorand Foundation, NTT Research, and Duality Technologies for their generous sponsorship of the conference. A special thanks goes to the general chair David Cash, and to Brian LaMacchia, Kevin McCurley, Kay McKelly, Sandry Quarles, Douglas Stebila, and the

TCC Steering Committee. Finally, we are thankful to the thriving and vibrant community of theoretical cryptographers. Long Live TCC!

September 2022

Eike Kiltz
Vinod Vaikuntanathan

Organization

General Chair

David Cash	University of Chicago, USA

Program Committee Chairs

Eike Kiltz	Ruhr-Universität Bochum, Germany
Vinod Vaikuntanathan	MIT, USA

Steering Committee

Jesper Buus Nielsen	Aarhus University, Denmark
Krzysztof Pietrzak	Institute of Science and Technology, Austria
Huijia (Rachel) Lin	UCSB, USA
Yuval Ishai	Technion, Israel
Tal Malkin	Columbia University, USA
Manoj M. Prabhakaran	IIT Bombay, India
Salil Vadhan	Harvard University, USA

Program Committee

Gilad Asharov	Bar-Ilan University, Israel
Marshall Ball	New York University, USA
Amos Beimel	Ben Gurion University, Israel
Fabrice Benhamouda	Algorand Foundation, USA
Nir Bitansky	Tel Aviv University, Israel
Zvika Brakerski	Weizmann Institute of Science, Israel
Anne Broadbent	University of Ottawa, Canada
Yilei Chen	Tsinghua University, China
Ran Cohen	Reichman University, Israel
Geoffroy Couteau	CNRS, IRIF, Université Paris Cité, France
Nils Fleischhacker	Ruhr University Bochum, Germany
Rishab Goyal	University of Wisconsin-Madison, USA
Siyao Guo	NYU Shanghai, China
Dennis Hofheinz	ETH Zurich, Switzerland
Gabe Kaptchuk	Boston University, USA
Jonathan Katz	University of Maryland, USA

Dakshita Khurana	UIUC, USA
Susumu Kiyoshima	NTT Research, USA
Karen Klein	ETH Zurich, Switzerland
Venkata Koppula	Indian Institute of Technology Delhi, India
Eyal Kushilevitz	Technion, Israel
Alex Lombardi	University of California, Berkeley, USA
Julian Loss	CISPA Helmholtz Center for Information Security, Germany
Fermi Ma	Simons Institute and UC Berkeley, USA
Mohammad Mahmoody	University of Virginia, USA
Ryo Nishimaki	NTT Corporation, Japan
Adam O'Neill	University of Massachusetts Amherst, USA
Emmanuela Orsini	KU Leuven, Belgium
Omer Paneth	Tel Aviv University, Israel
Alon Rosen	Bocconi University, Italy
Lior Rotem	The Hebrew University, Israel
Ron Rothblum	Technion, Israel
Peter Scholl	Aarhus University, Denmark
Sruthi Sekar	UC Berkeley, USA
Katerina Sotiraki	UC Berkeley, USA
Nicholas Spooner	University of Warwick, UK
Noah Stephens-Davidowitz	Cornell University, USA
Stefano Tessaro	University of Washington, USA
Prashant Vasudevan	National University of Singapore, Singapore
David Wu	University of Texas at Austin, USA
Yu Yu	Shanghai Jiao Tong University, China
Mark Zhandry	NTT Research and Princeton University, USA

Additional Reviewers

Damiano Abram
Amit Agarwal
Shweta Agrawal
Nicolas Alhaddad
Benedikt Auerbach
Renas Bacho
Christian Badertscher
Saikrishna Badrinarayanan
James Bartusek
Gabrielle Beck
Alexander Bienstock
Dung Bui
Suvradip Chakraborty
Rohit Chatterjee
Arka Rai Choudhuri
Kelong Cong
Hongrui Cui
Eric Culf
Dana Dachman-Soled
Pratish Datta
Lalita Devadas
Nico Döttling
Thomas Espitau
Jaiden Fairoze
Oriol Farràs
Weiqi Feng
Ben Fisch
Danilo Francati
Tore Frederiksen
Cody Freitag
Rachit Garg
Romain Gay
Nicholas Genise
Suparno Ghoshal
Aarushi Goel
Eli Goldin
Shai Halevi
Mathias Hall-Andersen
Dominik Hartmann

Alexandra Henzinger
Martin Hirt
Viet Tung Hoang
Charlotte Hoffmann
Justin Holmgren
James Hulett
Yuval Ishai
Palak Jain
Ruta Jawale
Zhengzhong Jin
Daniel Jost
Chethan Kamath
Martti Karvonen
Julia Kastner
Shuichi Katsumata
Fuyuki Kitagawa
Sabrina Kunzweiler
Ulysse Lechine
Derek Leung
Hanjun Li
Baiyu Li
Xiao Liang
Yao-Ting Lin
Tianren Liu
Qipeng Liu
Chen-Da Liu-Zhang
Sébastien Lord
George Lu
Takahiro Matsuda
Pierre Meyer
Pratyush Mishra
Tamer Mour
Marta Mularczyk
Alice Murphy
Varun Narayanan
Hai Nguyen
Maciej Obremski
Michele Orrù
Hussien Othman
Tapas Pal
Giorgos Panagiotakos
Dimitris Papachristoudis
Guillermo Pascual Perez
Anat Paskin-Cherniavsky
Robi Pedersen
Luowen Qian
Willy Quach
Nicholas Resch
Lawrence Roy
Yusuke Sakai
Pratik Sarkar
Benjamin Schlosser
Akash Shah
Yixin Shen
Omri Shmueli
Min Jae Song
Fang Song
Pratik Soni
Shravan Srinivasan
Igors Stepanovs
Dominique Unruh
Neekon Vafa
Benedikt Wagner
Hendrik Waldner
Mingyuan Wang
Hoeteck Wee
Ke Wu
Zhiye Xie
Sophia Yakoubov
Takashi Yamakawa
Eylon Yogev
Peter Yuen
Rachel Zhang
Jiaheng Zhang
Vassilis Zikas
Leo de Castro
Akin Ünal

Contents – Part I

Post-quantum Cryptography

Post-quantum Insecurity from LWE 3
Alex Lombardi, Ethan Mook, Willy Quach, and Daniel Wichs

Adaptive Versus Static Multi-oracle Algorithms, and Quantum Security of a Split-Key PRF 33
Jelle Don, Serge Fehr, and Yu-Hsuan Huang

The Parallel Reversible Pebbling Game: Analyzing the Post-quantum Security of iMHFs 52
Jeremiah Blocki, Blake Holman, and Seunghoon Lee

Quantum Rewinding for Many-Round Protocols 80
Russell W. F. Lai, Giulio Malavolta, and Nicholas Spooner

Interactive Proofs

Fiat-Shamir Transformation of Multi-round Interactive Proofs 113
Thomas Attema, Serge Fehr, and Michael Klooß

Steganography-Free Zero-Knowledge 143
Behzad Abdolmaleki, Nils Fleischhacker, Vipul Goyal, Abhishek Jain, and Giulio Malavolta

Vector Commitments over Rings and Compressed Σ-Protocols 173
Thomas Attema, Ignacio Cascudo, Ronald Cramer, Ivan Damgård, and Daniel Escudero

Universally Composable Σ-protocols in the Global Random-Oracle Model 203
Anna Lysyanskaya and Leah Namisa Rosenbloom

Quantum Cryptography

Pseudorandom (Function-Like) Quantum State Generators: New Definitions and Applications 237
Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen

Candidate Trapdoor Claw-Free Functions from Group Actions with Applications to Quantum Protocols 266
Navid Alamati, Giulio Malavolta, and Ahmadreza Rahimi

Collusion Resistant Copy-Protection for Watermarkable Functionalities 294
Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry

Secret-Sharing and Applications

On Secret Sharing, Randomness, and Random-less Reductions for Secret Sharing 327
Divesh Aggarwal, Eldon Chung, Maciej Obremski, and João Ribeiro

Leakage-resilient Linear Secret-sharing Against Arbitrary Bounded-size Leakage Family 355
Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, and Albert Yu

Asymptotically Free Broadcast in Constant Expected Time via Packed VSS 384
Ittai Abraham, Gilad Asharov, Shravani Patil, and Arpita Patra

Succinct Proofs

On Black-Box Constructions of Time and Space Efficient Sublinear Arguments from Symmetric-Key Primitives 417
Laasya Bangalore, Rishabh Bhadauria, Carmit Hazay, and Muthuramakrishnan Venkitasubramaniam

A Toolbox for Barriers on Interactive Oracle Proofs 447
Gal Arnon, Amey Bhangale, Alessandro Chiesa, and Eylon Yogev

Scalable and Transparent Proofs over All Large Fields, via Elliptic Curves: (ECFFT Part II) 467
Eli Ben–Sasson, Dan Carmon, Swastik Kopparty, and David Levit

Doubly Efficient Interactive Proofs over Infinite and Non-commutative Rings 497
Eduardo Soria-Vazquez

Fully Succinct Batch Arguments for NP from Indistinguishability Obfuscation 526
Rachit Garg, Kristin Sheridan, Brent Waters, and David J. Wu

Identity-Based Encryption and Functional Encryption

Lower Bounds for the Number of Decryption Updates in Registration-Based Encryption 559
Mohammad Mahmoody, Wei Qi, and Ahmadreza Rahimi

IBE with Incompressible Master Secret and Small Identity Secrets 588
Nico Döttling, Sanjam Garg, Sruthi Sekar, and Mingyuan Wang

Bounded Functional Encryption for Turing Machines: Adaptive Security from General Assumptions 618
Shweta Agrawal, Fuyuki Kitagawa, Anuja Modi, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa

Attribute-Based Encryption and Functional Encryption

Multi-authority ABE from Lattices Without Random Oracles 651
Brent Waters, Hoeteck Wee, and David J. Wu

ABE for Circuits with Constant-Size Secret Keys and Adaptive Security 680
Hanjun Li, Huijia Lin, and Ji Luo

Multi-Input Quadratic Functional Encryption: Stronger Security, Broader Functionality 711
Shweta Agrawal, Rishab Goyal, and Junichi Tomida

Author Index 741

Contents – Part II

Encryption

Forward-Secure Encryption with Fast Forwarding 3
Yevgeniy Dodis, Daniel Jost, and Harish Karthikeyan

Rate-1 Incompressible Encryption from Standard Assumptions 33
Pedro Branco, Nico Döttling, and Jesko Dujmović

Achievable CCA2 Relaxation for Homomorphic Encryption 70
Adi Akavia, Craig Gentry, Shai Halevi, and Margarita Vald

Multi-party Computation I

Round-Optimal Honest-Majority MPC in Minicrypt and with Everlasting Security: (Extended Abstract) 103
Benny Applebaum, Eliran Kachlon, and Arpita Patra

Sublinear Secure Computation from New Assumptions 121
Elette Boyle, Geoffroy Couteau, and Pierre Meyer

How to Obfuscate MPC Inputs 151
Ian McQuoid, Mike Rosulek, and Jiayu Xu

Statistical Security in Two-Party Computation Revisited 181
Saikrishna Badrinarayanan, Sikhar Patranabis, and Pratik Sarkar

Protocols: Key Agreement and Commitments

On the Worst-Case Inefficiency of CGKA 213
Alexander Bienstock, Yevgeniy Dodis, Sanjam Garg, Garrison Grogan, Mohammad Hajiabadi, and Paul Rösler

Adaptive Multiparty NIKE 244
Venkata Koppula, Brent Waters, and Mark Zhandry

On the Impossibility of Algebraic Vector Commitments in Pairing-Free Groups 274
Dario Catalano, Dario Fiore, Rosario Gennaro, and Emanuele Giunta

Four-Round Black-Box Non-malleable Schemes from One-Way Permutations 300
Michele Ciampi, Emmanuela Orsini, and Luisa Siniscalchi

Theory I: Sampling and Friends

A Tight Computational Indistinguishability Bound for Product Distributions 333
Nathan Geier

Secure Sampling with Sublinear Communication 348
Seung Geol Choi, Dana Dachman-Soled, S. Dov Gordon, Linsheng Liu, and Arkady Yerukhimovich

Secure Non-interactive Simulation from Arbitrary Joint Distributions 378
Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen

Secure Non-interactive Reducibility is Decidable 408
Kaartik Bhushan, Ankit Kumar Misra, Varun Narayanan, and Manoj Prabhakaran

Multi-party Computation II

Round-Optimal Black-Box Secure Computation from Two-Round Malicious OT 441
Yuval Ishai, Dakshita Khurana, Amit Sahai, and Akshayaram Srinivasan

Fully-Secure MPC with Minimal Trust 470
Yuval Ishai, Arpita Patra, Sikhar Patranabis, Divya Ravi, and Akshayaram Srinivasan

SCALES: MPC with Small Clients and Larger Ephemeral Servers 502
Anasuya Acharya, Carmit Hazay, Vladimir Kolesnikov, and Manoj Prabhakaran

On Perfectly Secure Two-Party Computation for Symmetric Functionalities with Correlated Randomness 532
Bar Alon, Olga Nissenbaum, Eran Omri, Anat Paskin-Cherniavsky, and Arpita Patra

Lattices

Public-Key Encryption from Homogeneous CLWE 565
Andrej Bogdanov, Miguel Cueto Noval, Charlotte Hoffmann, and Alon Rosen

PPAD is as Hard as LWE and Iterated Squaring 593
Nir Bitansky, Arka Rai Choudhuri, Justin Holmgren, Chethan Kamath, Alex Lombardi, Omer Paneth, and Ron D. Rothblum

Parallelizable Delegation from LWE 623
Cody Freitag, Rafael Pass, and Naomi Sirkin

How to Sample a Discrete Gaussian (and more) from a Random Oracle 653
George Lu and Brent Waters

Anonymity, Verifiability and Robustness

Anonymous Whistleblowing over Authenticated Channels 685
Thomas Agrikola, Geoffroy Couteau, and Sven Maier

Poly Onions: Achieving Anonymity in the Presence of Churn 715
Megumi Ando, Miranda Christ, Anna Lysyanskaya, and Tal Malkin

The Price of Verifiability: Lower Bounds for Verifiable Random Functions 747
Nicholas Brandt, Dennis Hofheinz, Julia Kastner, and Akin Ünal

Bet-or-Pass: Adversarially Robust Bloom Filters 777
Moni Naor and Noa Oved

Author Index 809

Contents – Part III

ORAM, OT and PIR

Verifiable Private Information Retrieval . . . 3
Shany Ben-David, Yael Tauman Kalai, and Omer Paneth

Random-Index Oblivious RAM . . . 33
Shai Halevi and Eyal Kushilevitz

On the Optimal Communication Complexity of Error-Correcting Multi-server PIR . . . 60
Reo Eriguchi, Kaoru Kurosawa, and Koji Nuida

Oblivious-Transfer Complexity of Noisy Coin-Toss via Secure Zero Communication Reductions . . . 89
Saumya Goyal, Varun Narayanan, and Manoj Prabhakaran

Theory II

One-Time Programs from Commodity Hardware . . . 121
Harry Eldridge, Aarushi Goel, Matthew Green, Abhishek Jain, and Maximilian Zinkus

Universal Reductions: Reductions Relative to Stateful Oracles . . . 151
Benjamin Chan, Cody Freitag, and Rafael Pass

Permissionless Clock Synchronization with Public Setup . . . 181
Juan Garay, Aggelos Kiayias, and Yu Shen

Beyond Uber: Instantiating Generic Groups via PGGs . . . 212
Balthazar Bauer, Pooya Farshim, Patrick Harasser, and Adam O'Neill

Author Index . . . 243