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

Springer

Lecture Notes in Computer Science 13043

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

Springer

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

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 Bhadauria	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 Alpirez Bock	Nicholas Genise	Xiao Liang
Jonathan Bootle	Ashrujit Ghoshal	Wei-Kai Lin
Lennart Braun	Niv Gilboa	Jiahui Liu
Konstantinos Brazitikos	Aarushi Goel	Qipeng Liu
Ignacio Cascudo	Junqing Gong	Tianren Liu

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

Contents – Part II