3rd Conference on Information-Theoretic Cryptography

ITC 2022, July 5–7, 2022, Cambridge, MA, USA

Edited by

Dana Dachman-Soled

LIPICS

LIPIcs – Vol. 230 – ITC 2022 www.dagstuhl.de/lipics

Editors

Dana Dachman-Soled
University of Maryland, College Park, MD, USA
danadach@umd.edu

ACM Classification 2012
Security and privacy → Cryptography; Mathematics of computing → Information theory; Theory of computation → Computational complexity and cryptography

ISBN 978-3-95977-238-9

Published online and open access by
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at https://www.dagstuhl.de/dagpub/978-3-95977-238-9.

Publication date
July, 2022

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at https://portal.dnb.de.

Digital Object Identifier: 10.4230/LIPIcs.ITC.2022.0

LIPIcs – Leibniz International Proceedings in Informatics

LIPIcs is a series of high-quality conference proceedings across all fields in informatics. LIPIcs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

ISSN 1868-8969

https://www.dagstuhl.de/lipics

Contents

Papers

3rd Conference on Information-Theoretic Cryptography (ITC 2022).
Editor: Dana Dachman-Soled
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

The third Conference on Information-Theoretic Cryptography (ITC 2022) was held in-person in Cambridge, MA on July 5–7, 2022, with virtual attendance an option. Yael Tauman Kalai and Vinod Vaikuntanathan were the general chairs and Dana Dachman-Soled was the program chair. The conference was held in cooperation with the International Association for Cryptologic Research (IACR).

In its third year, ITC has continued to fill the role in the cryptographic community of disseminating research advances on all aspects of information-theoretic security. The breadth of topics covered by the papers and invited talks reflects the fact that information theoretic techniques are pervasive in essentially all areas of cryptography. ITC has also sought to foster the creation of a community bringing together researchers from coding theory, information theory (classical and quantum), theory of computation, privacy, and cryptography.

This year, the conference received 30 submissions, of which the Program Committee (PC) accepted 17. The 19 PC members were helped in selecting the program by many external reviewers. The small size of the conference afforded the reviewers the opportunity to send anonymous questions to the authors to clarify technical issues. In several cases, this interactive process consisted of multiple rounds and continued until the questions were resolved. The proceedings consist of the revised version of the 17 accepted papers. The revisions were not reviewed, and the authors bear full responsibility for the content.

In addition to the accepted papers, the conference included six invited talks. They were selected by the PC to be "spotlight talks," highlighting the most exciting recent advances in cryptography and theoretical computer science that interest the ITC community.

Many individuals helped make ITC 2022 a success. We offer our sincere thanks to: All the authors who chose to submit their papers to this conference; the PC members for providing thorough reviews, for their dedication to resolving technical issues, and for their active participation in discussing each paper; the external reviewers for providing us with their valuable expert opinions; the ITC Steering Committee, and especially Benny Applebaum, for providing support, guidance, and advice throughout the process; and last but not least, the invited speakers, presenting authors, and participants for committing their time to making the conference a success.

Dana Dachman-Soled

3rd Conference on Information-Theoretic Cryptography (ITC 2022).
Editor: Dana Dachman-Soled
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Steering Committee

- Benny Applebaum (Chair, Tel-Aviv University)
- Ivan Damgård (Aarhus University)
- Yevgeniy Dodis (New York University)
- Yuval Ishai (Technion)
- Ueli Maurer (ETH Zurich)
- Kobbi Nissim (Georgetown)
- Krzysztof Pietrzak (IST Austria)
- Manoj Prabhakaran (IIT Bombay)
- Adam Smith (Boston University)
- Yael Tauman Kalai (MIT and Microsoft Research New England)
- Stefano Tessaro (University of Washington)
- Vinod Vaikuntanathan (MIT)
- Hoeteck Wee (ENS Paris)
- Daniel Wichs (Northeastern University and NTT Research)
- Mary Wootters (Stanford)
- Chaoping Xing (Nanyang Technological University)
- Moti Yung (Google)

3rd Conference on Information-Theoretic Cryptography (ITC 2022).
Editor: Dana Dachman-Soled
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Organization

General Chairs

- Yael Tauman Kalai (MIT and Microsoft Research New England)
- Vinod Vaikuntanathan (MIT)

Program Chair

- Dana Dachman-Soled (University of Maryland)

Program Committee

- Gorjan Alagic (University of Maryland and NIST)
- Gilad Asharov (Bar-Ilan University)
- Marshall Ball (New York University)
- Jeremiah Blocki (Purdue University)
- Anne Broadbent (University of Ottawa)
- Eshan Chattopadhyay (Cornell University)
- Kai-Min Chung (Academia Sinica)
- Ivan Damgård (Aarhus University)
- Mohammad Hajiabadi (University of Waterloo)
- Bhavana Kanakurthi (IISc Bangalore)
- Ilan Komargodski (Hebrew University of Jerusalem and NTT Research)
- Mukul Kulkarni (Technology Innovation Institute (TII Abu Dhabi))
- Feng-Hao Liu (Florida Atlantic University)
- Julian Loss (CISPA Helmholtz Center for Information Security)
- Mohammad Mahmoody (University of Virginia)
- Hemanta Maji (Purdue University)
- Krzysztof Pietrzak (IST Austria)
- Aishwarya Thiruvengadam (IIT Madras)
- Mor Weiss (Bar-Ilan University)

External Reviewers

Anirban Chakrabarti, Seung Geol Choi, Arka Rai Choudhuri, Jesse Goodman, Shreyas Gupta, Yao-Ching Hsieh, Wei-Hsiang Hung, Seunghoon Lee, Ray Li, Jyun-Jie Liao, Fermi Ma, Nicky Mouha, Sai Lakshmi Bhavana Obbattu, Maciej Obremski, Adam O'Neill, Sruthi Sekar, Girisha Shankar, Nikki Sigurdson, Dave Touchette, Benedikt Wagner, Chenkai Weng

3rd Conference on Information-Theoretic Cryptography (ITC 2022).
Editor: Dana Dachman-Soled
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany