1st Conference on Information-Theoretic Cryptography

ITC 2020, June 17–19, 2020, Boston, MA, USA

Edited by

Yael Tauman Kalai
Adam D. Smith
Daniel Wichs

Editors

Yael Tauman Kalai
Microsoft Research New England, Cambridge, MA, USA
yael@microsoft.com

Adam D. Smith
Boston University, MA, USA
ads22@bu.edu

Daniel Wichs
Northeastern University, Boston, MA, USA
NTT Research, Boston, MA, USA
wichs@ccs.neu.edu

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

ISBN 978-3-95977-151-1

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/978-3-95977-151-1.

Publication date
June, 2020

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.2020.0

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

Regular Papers

1st Conference on Information-Theoretic Cryptography (ITC 2020).
Editors: Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

The first Conference on Information-Theoretic Cryptography (ITC 2020) was originally planned to take place at Boston University, Boston, MA USA on June 17-19, 2020. However, due to the COVID-19 pandemic, the conference is being held entirely virtually. The general chairs are Yael Tauman Kalai and Adam D. Smith, and the program chair is Daniel Wichs. The conference is held in cooperation with the IACR.

The conference received 39 submissions, of which the Program Committee (PC) accepted 16. Since this was the first iteration of the conference, we felt the need to set a very high bar for quality to cement its standing as a top venue in the field. Each submission was reviewed by at least three PC members, often more. The 19 PC members, were helped by many additional external reviewers. The proceedings consist of the revised version of the 16 accepted papers. The revisions were not reviewed, and the authors bear full responsibility for the content.

We used Shai Halevi's excellent web-review software, and are extremely indebted to him for having written it, for setting it up for us, and for patiently providing much technical help whenever we had any questions. In addition to asking reviewers for an overall score, we asked reviewers to also give numeric scores for "Importance of End Results", "Conceptual Novelty", and "Technical Novelty". Although we did not rely on these scores in the final decision making process, we felt that they helped frame the discussion and clarified what aspects reviewers liked and disliked about the paper.

In addition to the accepted papers, the conference includes six invited talks. These were selected by the PC and represent the "greatest hits" results in the area of information theoretic cryptography from the last few years.

We would like to thank the many people who made ITC a success. First of all, a big thanks to all the authors who submitted papers to the conference. There were many excellent submissions, and in our goal to keep the quality high, it is all but certain that we rejected some papers whose importance we failed to grasp. We would like to thank all the PC members for their efforts in providing detailed reviews, verifying correctness, and discussing the merits and limitations in depth. We are also thankful to the external reviewers for providing valuable expert opinions. We are grateful to the ITC Steering Committee, and especially Benny Applebaum, for guidance and advice. And last, but not least, we thank all the invited speakers, presenting authors, and participants for committing their time to making the virtual conference a success, despite all the difficulties of the ongoing COVID-19 pandemic.

1st Conference on Information-Theoretic Cryptography (ITC 2020).
Editors: Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs
Leibniz International Proceedings in Informatics
LIPICS 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 (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)

1st Conference on Information-Theoretic Cryptography (ITC 2020).
Editors: Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Organization

General Chairs

- Yael Tauman Kalai (MSR and MIT)
- Adam Smith (BU)

Program Chair

- Daniel Wichs (Northeastern and NTT Research)

Program Committee

- Shweta Agrawal (IIT Madras)
- Amos Beimel (Ben Gurion University)
- Anne Broadbent (University of Ottawa)
- Mahdi Cheraghchi (University of Michigan Ann Arbor)
- Kai-Min Chung (Academia Sinica)
- Stefan Dziembowski (University of Warsaw)
- Serge Fehr (CWI Amsterdam and Leiden University)
- Siyao Guo (New York University Shanghai)
- Iftach Haitner (Tel Aviv University)
- Mohammad Hajiabadi (UC Berkeley)
- Ilan Komargodski (NTT Research)
- Hemanta Maji (Purdue University)
- Moni Naor (Weizmann Institute of Science)
- Jesper Buus Nielsen (Aarhus University)
- Christian Schaffner (QuSoft and University of Amsterdam)
- Stefano Tessaro (University of Washington)
- Jonathan Ullman (Northeastern University)
- Mary Wootters (Stanford University)
- Mark Zhandry (Princeton University and NTT Research)

External Reviewers

Mark Abspoel, Alexander Barg, James Bartusek, Jeremiah Blocki, Christian Badertscher, Clement Canonne, Andre Chailloux, Suvradip Chakraborty, Eshan Chattopadhyay, Albert Cheu, Ran Cohen, Wei Dai, Pratik Dand, Akshay Degwekar, Itai Dinur, Jack Doerner, Jelle Don, Yfke Dulek, Bill Fefferman, Venkatesan Guruswami, Brett Hemenway, Viet Tung Hoang, Joseph Jaeger, Matthew Joseph, Raza Ali Kazmi, Xiao Liang, Qipeng Liu, Tianren Liu, Yanyi Liu, Sébastien Lord, Fermi Ma, Mohammad Mahmoody, Nikolaos Makriyannis, Aleksandar (Sasho) Nikolov, Maciej Obremski, Naty Peter, Supartha Podder, Antigoni Polychroniadou, Divya Ravi, Joao Ribeiro, Lior Rotem, Sruthi Sekar, Or Sheffet, Pratik Soni, Jad Silbak, Mark Simkin,Florian Speelman, Akshayaram Srinivasan, Benjamin Terner, Ameya Velingker, Vanessa Vitse, Mingyuan Wang, Tianhao Wang, Chris Williamson, Jiapeng Zhang, Vincent Zucca

1st Conference on Information-Theoretic Cryptography (ITC 2020).
Editors: Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

List of Authors

Radune Artiom (12)
Ariel University, Ariél, Israel; The Open University, Raanana, Israel

Gilad Asharov (11)
Bar-Ilan University, Ramat-Gan, Israel

Victor Balcer (1)
School of Engineering & Applied Sciences, Harvard University, Cambridge, MA, United States

Amos Beimel (14)
Dept. of Computer Science, Ben-Gurion University, Beer-Sheva, Israel

Jeremiah Blocki (16)
Purdue University, West Lafayette, IN, USA

Mahdi Cheraghchi (7)
EECS Department, University of Michigan, Ann Arbor, MI, USA

Albert Cheu (1)
Khoury College of Computer Sciences, Northeastern University, Boston, MA, United States

Kai-Min Chung (8)
Academia Sinica, Taipei, Taiwan

Claude Crépeau (4)
School of Computer Science, McGill University, Montréal, Québec, Canada

Hendrik Eerikson (5)
Cybernetica AS, Tartu, Estonia

Reo Eriguchi (2)
Graduate School of Information Science and Technology, The University of Tokyo, Japan

Badih Ghazi (15)
Google Research, Mountain View, CA, USA

Noah Golowich (15)
Google Research, Mountain View, CA, USA; MIT, Cambridge, MA, USA

Venkatesan Guruswami (7)
Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, USA

Martin Hirt (3)
ETH Zurich, Switzerland

Marcel Keller (5)
CSIRO's Data61, Eveleigh, Australia

Ilan Komargodski (11)
NTT Research, East Palo Alto, CA, USA

Aleksandra Korolova (14)
Dept. of Computer Science, University of Southern California, Los Angeles, CA, USA

Shubhang Kulkarni (16)
Purdue University, West Lafayette, IN, USA

Ravi Kumar (15)
Google Research, Mountain View, CA, USA

Noboru Kunihiro (2)
Department of Computer Science, University of Tsukuba, Japan

Tai-Ning Liao (8)
National Taiwan University, Taipei, Taiwan

Fuchun Lin (7)
Department of Electrical and Electronic Engineering, Imperial College London, UK

Wei-Kai Lin (11)
Cornell University, Ithaca, NY, USA

Pasin Manurangsi (15)
Google Research, Mountain View, CA, USA

Arnaud Y. Massenet (4)
École Normale Supérieure Paris-Saclay, Gif-sur-Yvette, France

Marta Mularczyk (3)
ETH Zurich, Switzerland

Moni Naor (9)
Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel

Kobbi Nissim (14)
Dept. of Computer Science, Georgetown University, Washington, DC, USA

Claudio Orlandi (5)
Department of Computer Science, DIGIT, Aarhus University, Denmark

Rasmus Pagh (15)
Google Research, Mountain View, CA, USA; IT University of Copenhagen, Denmark; Basic Algorithms Research Copenhagen, Denmark

Anat Paskin-Cherniavsky (12)
Ariel University, Ariél, Israel

1st Conference on Information-Theoretic Cryptography (ITC 2020).
Editors: Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Enoch Peserico (11)
Università degli Studi di Padova, Italy

Naty Peter (13)
Ben-Gurion University of the Negev, Beer-Sheva, Israel

Pille Pullonen (5)
Cybernetica AS, Tartu, Estonia

Joonas Puura (5)
Institute of Computer Science, University of Tartu, Estonia

Luowen Qian (8)
Boston University, MA, USA

Peter Michael Reichstein Rasmussen (6)
Basic Algorithms Research Copenhagen, University of Copenhagen, Denmark

Lior Rotem (9)
School of Computer Science and Engineering, Hebrew University of Jerusalem, Jerusalem 91904, Israel

Reihaneh Safavi-Naini (7)
Department of Computer Science, University of Calgary, CA

Amit Sahai (6)
UCLA, Los Angeles, CA, USA

Louis Salvail (4)
Département d'Informatique et de R.O., Université de Montréal, Montréal, Québec, Canada

Gil Segev (9, 10)
School of Computer Science and Engineering, Hebrew University of Jerusalem, Jerusalem 91904, Israel

Ido Shahaf (10)
School of Computer Science and Engineering, Hebrew University of Jerusalem, Jerusalem, Israel

Or Sheffet (14)
Faculty of Engineering, Bar-Ilan University, Ramat Gan, Israel

Elaine Shi (11)
Cornell University, Ithaca, NY, USA

Mark Simkin (5)
Department of Computer Science, DIGIT, Aarhus University, Denmark

Uri Stemmer (14)
Dept. of Computer Science, Ben-Gurion University, Beer-Sheva, Israel; Google Research

Lucas Shigeru Stinchcombe (4)
Bloomberg L.P., Tokyo, Japan

Rotem Tsabary (13)
Weizmann Institute of Science, Rehovot, Israel

Ameya Velingker (15)
Google Research, Mountain View, CA, USA

Huaxiong Wang (7)
Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, SG

Hoeteck Wee (13)
CNRS, ENS, PSL, Paris, France

Nan Yang (4)
Canadian Centre for Cyber Security, Ottawa, Ontario, Canada; Concordia University, Montréal, Québec, Canada

Samson Zhou (16)
Carnegie Mellon University, Pittsburgh, PA, USA