4th Conference on Information-Theoretic Cryptography

ITC 2023, June 6–8, 2023, Aarhus University, Aarhus, Denmark

Edited by

Kai-Min Chung

LIPIcs – Vol. 267 – ITC 2023 www.dagstuhl.de/lipics

Editors

Kai-Min Chung
Academia Sinica, Taipei City, Taiwan
kmchung@iis.sinica.edu.tw

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

ISBN 978-3-95977-271-6

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/978-3-95977-271-6.

Publication date
July, 2023

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.2023.0

ISBN 978-3-95977-271-6 **ISSN 1868-8969** **https://www.dagstuhl.de/lipics**

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

4th Conference on Information-Theoretic Cryptography (ITC 2023).
Editor: Kai-Min Chung
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

The fourth Conference on Information-Theoretic Cryptography (ITC 2023) took place from June 6–8, 2023, at the Department of Computer Science, Aarhus University, Aarhus, Denmark. For the first time since the COVID-19 pandemic, we were thrilled to hold a fully in-person conference. This year's conference was co-located with the TPMPC 2023 workshop. The general chair was Ivan Damgård, and the program chair was Kai-Min Chung. As with the previous editions, the conference was held in cooperation with the International Association for Cryptologic Research (IACR).

In its fourth year, ITC continued its mission of bringing together the cryptography and information theory communities, and advancing research in all aspects of information-theoretic techniques for cryptography and security. In pursuit of this mission, we invited multiple Program Committee members from the information theory community, and broadened the Call for Papers to encompass emerging topics such as adversarial and robust learning and algorithmic fairness. Although we didn't see a substantial increase in submissions from these areas this year, we remain hopeful that this will be a valuable initiative for future years.

We received a total of 29 submissions which overall were of high quality. As in the last year, we leveraged the small conference size to have interactive and anonymous discussions with the authors to clarify technical issues. With the help of external reviewers, the program committee selected 18 papers. One was conditionally accepted at first but eventually accepted after shepherding. The proceedings contain the revised versions of these 18 papers. The revisions were not reviewed, and the authors bear full responsibility for the content.

Continuing the tradition, the conference featured six "spotlight talks," highlighting the exciting development of information theoretical techniques in the cryptography and information theory community. This year, the selection of spotlight talks was carried out by the steering committee and the program chair. It was our great pleasure this year to feature a historical talk by Ivan Damgård on information-theoretic MPC to celebrate the 35th anniversary of its invention.

We are grateful to everyone who made the 4th ITC conference a success. Our heartfelt thanks go out to the authors who submitted their papers. We extend our sincere thanks to the PC members and external reviewers for their dedicated efforts in providing thorough reviews, insightful discussions, and expert opinions. We are deeply indebted to the steering committee, particularly Benny Applebaum and Hoeteck Wee, for their invaluable guidance. Special thanks are also due to the previous PC chairs, especially Dana Dachman-Soled, for sharing their experience and providing answers to numerous questions. Lastly, we extend our gratitude to all the invited speakers, presenting authors, and participants who devoted their time and energy to ensuring the success of this conference.

Kai-Min Chung

4th Conference on Information-Theoretic Cryptography (ITC 2023).
Editor: Kai-Min Chung
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 (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)

4th Conference on Information-Theoretic Cryptography (ITC 2023).
Editor: Kai-Min Chung
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Organization

General chairs

- Ivan Damgård (Aarhus University)

Program chair

- Kai-Min Chung (Academia Sinica)

Program Committee

- Divesh Aggarwal (National University of Singapore)
- Prabhanjan Ananth (University of California, Santa Barbara)
- Jeremiah Blocki (Purdue University)
- Amos Beimel (Ben Gurion University)
- Rawad Bitar (Technical University of Munich)
- Mahdi Cheraghchi (University of Michigan Ann Arbor)
- Albert Cheu (Georgetown University)
- Suhas Diggavi (University of California, Los Angeles)
- Wei-Kai Lin (Northeastern University)
- Qipeng Liu (Simons Institute)
- Xiao Liang (Rice University)
- Russell W. F. Lai (Aalto University)
- Saeed Mahloujifar (Princeton University)
- Maciej Obremski (National University of Singapore)
- Vinod M. Prabhakaran (Tata Institute of Fundamental Research)
- Anat Paskin-Cherniavsky (Ariel University)
- Lior Rotem (Stanford University)
- João Ribeiro (New University of Lisbon)
- Noga Ron-Zewi (University of Haifa)
- Salim El Rouayheb (Rutgers University)
- Sruthi Sekar (University of California, Berkeley)
- Kevin Yeo (Google NYC and Columbia University)
- Takashi Yamakawa (NTT)
- Yihan Zhang (Institute of Science and Technology Austria)

Local Organization Committee

- Yashvanth Kondi (Aarhus University)
- Divya Ravi (Aarhus University)
- Malene Bisgaard (Aarhus University)

4th Conference on Information-Theoretic Cryptography (ITC 2023).
Editor: Kai-Min Chung
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

External Reviewers

Gilles Zemor, Rafael D'Oliveira, Aditya Gulati, Laszlo Csirmaz, Oded Nir, Elisaweta Masserova, Rahul Rachuri, Obbattu Sai Lakshmi Bhavana, Varun Narayanan, Nathan Manohar, Aarushi Goel, Rohit Chatterjee, Justin Raizes, Ohad Klein, Fatih Kaleoglu, Bar Alon, Alexander Poremba, Chen-Da Liu Zhang, Siyao Guo, Ethan Mook, Sebastian Bitzer