

# 4th Conference on Information-Theoretic Cryptography

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

Edited by

Kai-Min Chung



*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>.

*License*

This work is licensed under a Creative Commons Attribution 4.0 International license (CC-BY 4.0): <https://creativecommons.org/licenses/by/4.0/legalcode>.



In brief, this license authorizes each and everybody to share (to copy, distribute and transmit) the work under the following conditions, without impairing or restricting the authors' moral rights:

- Attribution: The work must be attributed to its authors.

The copyright is retained by the corresponding authors.

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.

### *Editorial Board*

- Luca Aceto (*Chair*, Reykjavik University, IS and Gran Sasso Science Institute, IT)
- Christel Baier (TU Dresden, DE)
- Mikolaj Bojanczyk (University of Warsaw, PL)
- Roberto Di Cosmo (Inria and Université de Paris, FR)
- Faith Ellen (University of Toronto, CA)
- Javier Esparza (TU München, DE)
- Daniel Král' (Masaryk University – Brno, CZ)
- Meena Mahajan (Institute of Mathematical Sciences, Chennai, IN)
- Anca Muscholl (University of Bordeaux, FR)
- Chih-Hao Luke Ong (University of Oxford, GB and Nanyang Technological University, SG)
- Phillip Rogaway (University of California, Davis, US)
- Eva Rotenberg (Technical University of Denmark, Lyngby, DK)
- Raimund Seidel (Universität des Saarlandes, Saarbrücken, DE and Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Wadern, DE)

**ISSN 1868-8969**

**<https://www.dagstuhl.de/lipics>**



## ■ Contents

Preface	
<i>Kai-Min Chung</i> .....	0:vii
Steering Committee	
.....	0:ix
Organization	
.....	0:xi

### Papers

Two-Round Perfectly Secure Message Transmission with Optimal Transmission Rate	
<i>Nicolas Resch and Chen Yuan</i> .....	1:1–1:20
A Lower Bound on the Share Size in Evolving Secret Sharing	
<i>Noam Mazor</i> .....	2:1–2:9
Csirmaz’s Duality Conjecture and Threshold Secret Sharing	
<i>Andrej Bogdanov</i> .....	3:1–3:6
The Cost of Statistical Security in Proofs for Repeated Squaring	
<i>Cody Freitag and Ilan Komargodski</i> .....	4:1–4:23
Interactive Non-Malleable Codes Against Desynchronizing Attacks in the Multi-Party Setting	
<i>Nils Fleischhacker, Suparno Ghoshal, and Mark Simkin</i> .....	5:1–5:26
Asymmetric Multi-Party Computation	
<i>Vipul Goyal, Chen-Da Liu-Zhang, and Rafail Ostrovsky</i> .....	6:1–6:25
Phoenix: Secure Computation in an Unstable Network with Dropouts and Comebacks	
<i>Ivan Damgård, Daniel Escudero, and Antigoni Polychroniadou</i> .....	7:1–7:21
Weighted Secret Sharing from Wiretap Channels	
<i>Fabrice Benhamouda, Shai Halevi, and Lev Stambler</i> .....	8:1–8:19
Quantum Security of Subset Cover Problems	
<i>Samuel Bouaziz-Ermann, Alex B. Grilo, and Damien Vergnaud</i> .....	9:1–9:17
Distributed Shuffling in Adversarial Environments	
<i>Kasper Green Larsen, Maciej Obremski, and Mark Simkin</i> .....	10:1–10:15
MPC with Low Bottleneck-Complexity: Information-Theoretic Security and More	
<i>Hannah Keller, Claudio Orlandi, Anat Paskin-Cherniavsky, and Divya Ravi</i> .....	11:1–11:22
Randomness Recoverable Secret Sharing Schemes	
<i>Mohammad Hajiabadi, Shahram Khazaei, and Behzad Vahdani</i> .....	12:1–12:25
Secure Communication in Dynamic Incomplete Networks	
<i>Ivan Damgård, Divya Ravi, Daniel Tschudi, and Sophia Yakubov</i> .....	13:1–13:21

4th Conference on Information-Theoretic Cryptography (ITC 2023).

Editor: Kai-Min Chung



Leibniz International Proceedings in Informatics  
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Locally Covert Learning <i>Justin Holmgren and Ruta Jawale</i> .....	14:1–14:12
Online Mergers and Applications to Registration-Based Encryption and Accumulators <i>Mohammad Mahmoody and Wei Qi</i> .....	15:1–15:23
Lower Bounds for Secret-Sharing Schemes for $k$ -Hypergraphs <i>Amos Beimel</i> .....	16:1–16:13
Differentially Private Aggregation via Imperfect Shuffling <i>Badih Ghazi, Ravi Kumar, Pasin Manurangsi, Jelani Nelson, and Samson Zhou</i> .....	17:1–17:22
Exponential Correlated Randomness Is Necessary in Communication-Optimal Perfectly Secure Two-Party Computation <i>Keitaro Hiwatashi and Koji Nuida</i> .....	18:1–18:16

## ■ 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







## ■ 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)





# ■ 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  
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