

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

PRINT ISBN: 978-1-7138-8140-7

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>

■ 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

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

0:vi Contents

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