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
Print ISBN 978-1-7138-5894-2

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.

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.2022.0

ISBN 978-3-95977-238-9 **ISSN 1868-8969** **https://www.dagstuhl.de/lipics**

Contents

Preface
Dana Dachman-Soled 0:vii

Steering Committee
.... 0:ix

Organization
.... 0:xi

Papers

Multi-Server PIR with Full Error Detection and Limited Error Correction
Reo Eriguchi, Kaoru Kurosawa, and Koji Nuida 1:1–1:20

Property-Preserving Hash Functions and Combinatorial Group Testing
Kazuhiko Minematsu 2:1–2:14

Protecting Distributed Primitives Against Leakage: Equivocal Secret Sharing and More
Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, and Mor Weiss 3:1–3:24

Maliciously Circuit-Private FHE from Information-Theoretic Principles
Nico Döttling and Jesko Dujmovic 4:1–4:21

From Privacy-Only to Simulatable OT: Black-Box, Round-Optimal, Information-Theoretic
Varun Madathil, Chris Orsini, Alessandra Scafuro, and Daniele Venturi 5:1–5:20

On the Distributed Discrete Logarithm Problem with Preprocessing
Pavel Hubáček, Ľubica Jančová, and Veronika Králová 6:1–6:19

A Note on the Complexity of Private Simultaneous Messages with Many Parties
Marshall Ball and Tim Randolph 7:1–7:12

Multiparty Computation with Covert Security and Public Verifiability
Peter Scholl, Mark Simkin, and Luisa Siniscalchi 8:1–8:13

On Seedless PRNGs and Premature Next
Sandro Coretti, Yevgeniy Dodis, Harish Karthikeyan, Noah Stephens-Davidowitz, and Stefano Tessaro 9:1–9:20

Refuting the Dream XOR Lemma via Ideal Obfuscation and Resettable MPC
Saikrishna Badrinarayanan, Yuval Ishai, Dakshita Khurana, Amit Sahai, and Daniel Wichs 10:1–10:21

Revisiting Collision and Local Opening Analysis of ABR Hash
Chandranan Dhar, Yevgeniy Dodis, and Mridul Nandi 11:1–11:22

A Fully-Constructive Discrete-Logarithm Preprocessing Algorithm with an Optimal Time-Space Tradeoff
Lior Rotem and Gil Segev 12:1–12:16

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

Revisiting the Uber Assumption in the Algebraic Group Model: Fine-Grained Bounds in Hidden-Order Groups and Improved Reductions in Bilinear Groups
Lior Rotem 13:1–13:13

Universally Composable Almost-Everywhere Secure Computation
Nishanth Chandran, Pouyan Forghani, Juan Garay, Rafail Ostrovsky, Rutvik Patel, and Vassilis Zikas 14:1–14:25

Static vs. Adaptive Security in Perfect MPC: A Separation and the Adaptive Security of BGW
Gilad Asharov, Ran Cohen, and Oren Shochat 15:1–15:16

Tight Estimate of the Local Leakage Resilience of the Additive Secret-Sharing Scheme & Its Consequences
Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, and Albert Yu 16:1–16:19

Information-Theoretic Distributed Point Functions
Elette Boyle, Niv Gilboa, Yuval Ishai, and Victor I. Kolobov 17:1–17:14