6th Conference on Information-Theoretic Cryptography

ITC 2025, August 16–17, 2025, University of California, Santa Barbara, CA, USA

Edited by

Niv Gilboa

LIPIcs – Vol. 343 – ITC 2025 www.dagstuhl.de/lipics

Editors

Niv Gilboa
Ben-Gurion University of the Negev, Beer-Sheva, Israel
gilboan@bgu.ac.il

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

ISBN 978-3-95977-385-0
PRINT ISBN 979-8-3313-2609-8

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/978-3-95977-385-0.

Publication date
September, 2025

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists all publications of this volume in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at https://portal.dnb.de.

Digital Object Identifier: 10.4230/LIPIcs.ITC.2025.0

Contents

Preface
Niv Gilboa 0:vii

Steering Committee
.... 0:ix

Organization
.... 0:xi

Papers

Amortized Locally Decodable Codes for Insertions and Deletions
Jeremiah Blocki and Justin Zhang 1:1–1:23

Powerful Primitives in the Bounded Quantum Storage Model
Mohammed Barhoush and Louis Salvail 2:1–2:20

Leakage-Resilience of Shamir's Secret Sharing: Identifying Secure Evaluation Places
Jihun Hwang, Hemanta K. Maji, Hai H. Nguyen, and Xiuyu Ye 3:1–3:20

Time-Space Tradeoffs of Truncation with Preprocessing
Krzysztof Pietrzak and Pengxiang Wang 4:1–4:10

Information-Theoretic Random-Index PIR
Sebastian Kolby, Lawrence Roy, Jure Sternad, and Sophia Yakoubov 5:1–5:15

MetaDORAM: Info-Theoretic Distributed ORAM with Less Communication
Brett Hemenway Falk, Daniel Noble, and Rafail Ostrovsky 6:1–6:23

Linear-Time Secure Merge in O(loglog n) Rounds
Mark Blunk, Paul Bunn, Samuel Dittmer, Steve Lu, and Rafail Ostrovsky 7:1–7:23

On the Definition of Malicious Private Information Retrieval
Bar Alon and Amos Beimel 8:1–8:23

Revocable Encryption, Programs, and More: The Case of Multi-Copy Security
Prabhanjan Ananth, Saachi Mutreja, and Alexander Poremba 9:1–9:23

Multi-Source Randomness Extraction and Generation in the Random-Oracle Model
Sandro Coretti, Pooya Farshim, Patrick Harasser, and Karl Southern 10:1–10:23

New Results in Share Conversion, with Applications to Evolving Access Structures
Tamar Ben David, Varun Narayanan, Olga Nissenbaum, and Anat Paskin-Cherniavsky 11:1–11:23

Key-Agreement with Perfect Completeness from Random Oracles
Noam Mazor 12:1–12:11

6th Conference on Information-Theoretic Cryptography (ITC 2025).
Editor: Niv Gilboa
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany