

6th Conference on Information-Theoretic Cryptography

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

Edited by

Niv Gilboa



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

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>.

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.2025.0

ISBN 978-3-95977-385-0

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

- Christel Baier (TU Dresden, DE)
- Roberto Di Cosmo (Inria and Université Paris Cité, FR)
- Faith Ellen (University of Toronto, CA)
- Javier Esparza (TU München, DE)
- Holger Hermanns (Universität des Saarlandes, Saarbrücken, DE and Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Wadern, DE)
- Daniel Král' (Leipzig University, DE and Max Planck Institute for Mathematics in the Sciences, Leipzig, DE)
- Sławomir Lasota (University of Warsaw, PL)
- Meena Mahajan (Institute of Mathematical Sciences, Chennai, IN – Chair)
- Chih-Hao Luke Ong (Nanyang Technological University, SG)
- Eva Rotenberg (Technical University of Denmark, Lyngby, DK)
- Pierre Senellart (ENS, Université PSL, Paris, France)
- Alexandra Silva (Cornell University, Ithaca, US)

ISSN 1868-8969

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

Contents

Preface	
<i>Niv Gilboa</i>	0:vii
Steering Committee	
.....	0:ix
Organization	
.....	0:xi
 Papers	
Amortized Locally Decodable Codes for Insertions and Deletions	
<i>Jeremiah Blocki and Justin Zhang</i>	1:1–1:23
Powerful Primitives in the Bounded Quantum Storage Model	
<i>Mohammed Barhoush and Louis Salvail</i>	2:1–2:20
Leakage-Resilience of Shamir’s Secret Sharing: Identifying Secure Evaluation Places	
<i>Jihun Hwang, Hemanta K. Maji, Hai H. Nguyen, and Xiuyu Ye</i>	3:1–3:20
Time-Space Tradeoffs of Truncation with Preprocessing	
<i>Krzysztof Pietrzak and Pengxiang Wang</i>	4:1–4:10
Information-Theoretic Random-Index PIR	
<i>Sebastian Kolby, Lawrence Roy, Jure Sternad, and Sophia Yakoubov</i>	5:1–5:15
MetaDORAM: Info-Theoretic Distributed ORAM with Less Communication	
<i>Brett Hemenway Falk, Daniel Noble, and Rafail Ostrovsky</i>	6:1–6:23
Linear-Time Secure Merge in $O(\log \log n)$ Rounds	
<i>Mark Blunk, Paul Bunn, Samuel Dittmer, Steve Lu, and Rafail Ostrovsky</i>	7:1–7:23
On the Definition of Malicious Private Information Retrieval	
<i>Bar Alon and Amos Beimel</i>	8:1–8:23
Revocable Encryption, Programs, and More: The Case of Multi-Copy Security	
<i>Prabhanjan Ananth, Saachi Mutreja, and Alexander Poremba</i>	9:1–9:23
Multi-Source Randomness Extraction and Generation in the Random-Oracle Model	
<i>Sandro Coretti, Pooya Farshim, Patrick Harasser, and Karl Southern</i>	10:1–10:23
New Results in Share Conversion, with Applications to Evolving Access Structures	
<i>Tamar Ben David, Varun Narayanan, Olga Nissenbaum, and Anat Paskin-Cherniavsky</i>	11:1–11:23
Key-Agreement with Perfect Completeness from Random Oracles	
<i>Noam Mazon</i>	12:1–12:11



Preface

The sixth Conference on Information-Theoretic Cryptography (ITC 2025) took place from August 16–17, 2025, at the University of California, Santa Barbara, USA. The general chair was Prabhanjan Ananth, and the program chair was Niv Gilboa. As in previous editions, the conference was held in cooperation with the International Association for Cryptologic Research (IACR).

In its sixth year, ITC continued its mission of uniting the cryptography and information theory communities, and advancing research in all aspects of information-theoretic techniques for cryptography and security.

We received a total of 18 submissions, maintaining a high standard of quality. Following our tradition, we facilitated interactive and anonymous discussions with the authors to clarify technical issues. With the assistance of external reviewers, the program committee selected 12 papers for presentation. The proceedings contain the revised versions of these papers. The revisions were not reviewed, and the authors bear full responsibility for the content.

This year, we continued the tradition of featuring “spotlight talks” and invited talks that highlight exciting developments in the field. These talks highlighted notable recent papers from top conferences such as Eurocrypt 2021, Crypto 2024 and TCHES 2025. The talks were given by both established researchers and students. The spotlight and invited talks aimed to provide a comprehensive overview of the most significant recent advances in information-theoretic cryptography.

We are deeply grateful to everyone who contributed to the success of the 6th ITC conference. Our sincere thanks go out to the authors who submitted their papers. We extend our heartfelt 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, for his invaluable guidance. Special thanks are also due to the previous PC chairs, especially Divesh Aggarwal, 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.

Niv Gilboa



■ 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 chair

- Prabhanjan Ananth (University of California, Santa Barbara)

Program chair

- Niv Gilboa (Ben-Gurion University of the Negev)

Program committee

- Akinori Kawachi (Mie University)
- Alex Bredariol Grilo (CNRS/Sorbonne Université)
- Alexander Golovnev (Georgetown University)
- Amos Beimel (Ben-Gurion University of the Negev)
- Antonia Wachter-Zeh (Technical University of Munich)
- Dana Dachman-Soled (University of Maryland)
- Daniele Venturi (Sapienza University of Rome)
- Eylon Yogev (Bar-Ilan University)
- Hemanta Maji (Purdue University)
- Kevin Yeo (Google Research)
- Krzysztof Pietrzak (IST Austria)
- Luisa Siniscalchi (Technical University of Denmark)
- Maciej Obremski (National University of Singapore)
- Mahdi Cheraghchi (University of Michigan Ann Arbor)
- Mohammad Hajiabadi (University of Waterloo)
- Noah Golowich (MIT)
- Or Sheffet (Bar-Ilan University)
- Pasin Manurangsi (Google Research)
- Salim El Rouayheb (Rutgers University)
- Sandro Coretti (IOG)
- Stefano Tessaro (University of Washington)
- Wei-Kai Lin (University of Virginia)

External reviewers

Alper Cakan, Ananta Mukherjee, Anasuya Acharya, Angus Gruen, Changrui Mu, Gal Arnon, Ilan Komargodski, Jihun Hwang, Samuel King, Saswata Mukherjee, Sidhant Saraogi, Xiuyu Ye.



