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

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

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.

ISSN 1868-8969

https://www.dagstuhl.de/lipics

Contents

Papers

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

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

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

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)

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

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.

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