7th Conference on Information-Theoretic Cryptography

ITC 2026, August 15–16, 2026, University of California, Santa Barbara, CA, USA

Edited by

Yevgeniy Dodis

LIPIcs – Vol. 385 – ITC 2026 www.dagstuhl.de/lipics

Editors

Yevgeniy Dodis
New York University, NY, USA
dodis@cs.nyu.edu

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

ISBN 978-3-95977-426-0

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/978-3-95977-426-0.

Publication date
August, 2026

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.2026.0

ISBN 978-3-95977-426-0 **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.

ISSN 1868-8969

https://www.dagstuhl.de/lipics

Contents

Papers

7th Conference on Information-Theoretic Cryptography (ITC 2026).
Editor: Yevgeniy Dodis
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

The seventh Conference on Information-Theoretic Cryptography (ITC 2026) took place from August 15–16, 2026, at the University of California, Santa Barbara, USA. The general co-chairs were Prabhanjan Ananth, Daniel Collins and Eli Goldin, and the program chair was Yevgeniy Dodis. As in previous editions, the conference was held in cooperation with the International Association for Cryptologic Research (IACR).

In its seventh 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.

Like last year, 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 (like last year). The proceedings contain the revised versions of these papers. The revisions were not reviewed, and the authors bear full responsibility for the content.

Continuing the successful format from previous years, the conference featured a publication track, a spotlight track and a highlights track. The publication track consisted of talks selected among the conference submissions by the program committee for publication and presentation. The spotlight track consisted of invited talks (not published in the proceedings) that highlight the most exciting recent advances in information-theoretic cryptography. The highlights track comprised ITC-related papers that have appeared in the last years including at venues like STOC 2026 and Eurocrypt 2026; these talks were mostly given by students and postdocs.

We are deeply grateful to everyone who contributed to the success of the 7th 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 co-chairs Benny Applebaum and Elette Boyle, for their invaluable guidance. Special thanks are also due to the previous PC chairs for sharing their experience and providing answers to numerous questions. Thank you Prabhanjan Anath for your service as a general co-chair for another successful year. I would be remiss not to mention Daniel Collins and Eli Goldin whose significant efforts on various fronts behind the scenes made this conference possible. 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.

Yevgeniy Dodis

7th Conference on Information-Theoretic Cryptography (ITC 2026).
Editor: Yevgeniy Dodis
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Steering Committee

- Benny Applebaum (Co-Chair, Tel-Aviv University)
- Elette Boyle (Co-Chair, NTT Research and Reichman University)
- Ivan Damgård (Aarhus University)
- Yevgeniy Dodis (New York University)
- Yuval Ishai (Technion and AWS)
- Ueli Maurer (ETH Zurich)
- Kobbi Nissim (Georgetown)
- Krzysztof Pietrzak (IST Austria)
- Manoj Prabhakaran (IIT Bombay)
- Adam Smith (Boston University)
- Yael Tauman Kalai (MIT)
- Stefano Tessaro (University of Washington)
- Vinod Vaikuntanathan (MIT)
- Hoeteck Wee (NTT Research)
- Daniel Wichs (Northeastern University)
- Mary Wootters (Stanford)
- Chaoping Xing (Shanghai Jiao Tong University)
- Moti Yung (Google)

7th Conference on Information-Theoretic Cryptography (ITC 2026).
Editor: Yevgeniy Dodis

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Organization

General chairs

- Prabhanjan Ananth (University of California, Santa Barbara)
- Daniel Collins (New York University and Hebrew University)
- Eli Goldin (New York University)

Program chair

- Yevgeniy Dodis (New York University)

Program committee

- Adam Smith (Boston University)
- Bhavana Kanukurthi (Indian Institute of Science)
- Daniel Collins (New York University and Hebrew University)
- Daniel Tschudi (Concordium)
- Eli Goldin (New York University)
- Eylon Yogev (Bar-Ilan University)
- Hemanta K. Maji (Purdue University)
- Itai Dinur (Ben-Gurion University)
- Lior Rotem (Hebrew University)
- Maciej Obremski (National University of Signapore)
- Miryam Huang (University of Southern California)
- Nico Döttling (Helmholtz Center for Information Security (CISPA))
- Nicolas Resch (University of Amsterdam)
- Noah Golowich (Microsoft Research)
- Noam Mazor (New York University)
- Qipeng Liu (University of California, San Diego)
- Rahul Ilango (Institute for Advanced Study)
- Ran Cohen (Reichman University)
- Roman Langrehr (University of Waterloo)
- Siyao Gao (New York University - Shanghai)
- Tomoyuki Morimae (University of Kyoto)
- Vassilis Zikas (Georgia Institute of Technology)
- Yifan Song (Tsinghua University)
- Zhengzhong Jin (Northeastern University)

External reviewers

Akshima, Liyan Chen, Pouyan Forghani, Hanjun Li, George Lu, Mohammad Mahmoody, Hai Nguyen, Jaspal Singh, Er-cheng Tang, Yu Wei, Zhiye Xie.

7th Conference on Information-Theoretic Cryptography (ITC 2026).
Editor: Yevgeniy Dodis

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany