

# 5th Conference on Information-Theoretic Cryptography

ITC 2024, August 14–16, 2024, Stanford, CA, USA

Edited by

Divesh Aggarwal



*Editors*

**Divesh Aggarwal** 

National University of Singapore, Singapore  
divesh@comp.nus.edu.sg

*ACM Classification 2012*

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

**ISBN 978-3-95977-333-1**

*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/978-3-95977-333-1>.

*Publication date*

August, 2024

*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.2024.0

ISBN 978-3-95977-333-1

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*

- Luca Aceto (Reykjavik University, IS and Gran Sasso Science Institute, IT)
- 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)
- Daniel Král' (Masaryk University, Brno, CZ)
- Meena Mahajan (*Chair*, Institute of Mathematical Sciences, Chennai, IN)
- Anca Muscholl (University of Bordeaux, FR)
- Chih-Hao Luke Ong (Nanyang Technological University, SG)
- Phillip Rogaway (University of California, Davis, US)
- Eva Rotenberg (Technical University of Denmark, Lyngby, DK)
- Raimund Seidel (Universität des Saarlandes, Saarbrücken, DE and Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Wadern, DE)
- Pierre Senellart (ENS, Université PSL, Paris, FR)

**ISSN 1868-8969**

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



## ■ Contents

Preface	
<i>Divesh Aggarwal</i> .....	0:vii
Steering Committee	
.....	0:ix
Organization	
.....	0:xi

### Papers

Information-Theoretic Topology-Hiding Broadcast: Wheels, Stars, Friendship, and Beyond	
<i>D’or Banoun, Elette Boyle, and Ran Cohen</i> .....	1:1–1:13
Communication Complexity vs Randomness Complexity in Interactive Proofs	
<i>Benny Applebaum, Kaartik Bhushan, and Manoj Prabhakaran</i> .....	2:1–2:16
Are Your Keys Protected? Time Will Tell	
<i>Yoav Ben Dov, Liron David, Moni Naor, and Elad Tzalik</i> .....	3:1–3:28
Pure-DP Aggregation in the Shuffle Model: Error-Optimal and Communication-Efficient	
<i>Badih Ghazi, Ravi Kumar, and Pasin Manurangsi</i> .....	4:1–4:13
On the Power of Adaptivity for Function Inversion	
<i>Karthik Gajulapalli, Alexander Golovnev, and Samuel King</i> .....	5:1–5:10
Information-Theoretic Single-Server PIR in the Shuffle Model	
<i>Yuval Ishai, Mahimna Kelkar, Daniel Lee, and Yiping Ma</i> .....	6:1–6:23
Improved Trade-Offs Between Amortization and Download Bandwidth for Linear HSS	
<i>Keller Blackwell and Mary Wootters</i> .....	7:1–7:21
Breaking RSA Generically Is Equivalent to Factoring, <i>with Preprocessing</i>	
<i>Dana Dachman-Soled, Julian Loss, and Adam O’Neill</i> .....	8:1–8:24
Time-Space Tradeoffs for Finding Multi-Collisions in Merkle-Damgård Hash Functions	
<i>Akshima</i> .....	9:1–9:22
Secure Multiparty Computation of Symmetric Functions with Polylogarithmic Bottleneck Complexity and Correlated Randomness	
<i>Reo Eriguchi</i> .....	10:1–10:22
Fast Secure Computations on Shared Polynomials and Applications to Private Set Operations	
<i>Pascal Giorgi, Fabien Laguillaumie, Lucas Ottow, and Damien Vergnaud</i> .....	11:1–11:24





## ■ Preface

The fifth Conference on Information-Theoretic Cryptography (ITC 2024) took place from August 14–16, 2024, at Stanford University, USA. The general chairs were Mary Wootters and Dan Boneh, and the program chair was Divesh Aggarwal. As in previous editions, the conference was held in cooperation with the International Association for Cryptologic Research (IACR).

In its fifth 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. This year, we introduced a new Highlights Track, aimed at showcasing outstanding recent results from other venues.

We received a total of 21 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 11 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” that highlight exciting developments in the field. Additionally, the newly introduced Highlights Track featured invited talks on notable recent papers from top conferences such as STOC 2024, Eurocrypt 2024, FOCS 2023, Crypto 2023, Asiacrypt 2023, TCC 2023, and STOC 2023 presented by students or postdocs. These tracks aimed to provide a comprehensive overview of the most significant advancements in information-theoretic cryptography.

We are deeply grateful to everyone who contributed to the success of the 5th 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 Kai-Min Chung and Stefano Tessaro, 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.

Divesh Aggarwal







## ■ 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 chairs

- Mary Wootters (Stanford University)
- Dan Boneh (Stanford University)

### Program chair

- Divesh Aggarwal (National University of Singapore)

### Program Committee

- Akshayaram Srinivasan (University of Toronto)
- Amos Beimel (Ben Gurion University)
- Damiano Abram (Aarhus University)
- Daniele Venturi (Sapienza University of Rome)
- Giulio Malavolta (Bocconi University & MPI-SP)
- Hemanta Maji (Purdue University)
- Ilan Komargodski (The Hebrew University of Jerusalem and NTT Research)
- Jesse Goodman (UT Austin)
- Joao Ribeiro (Universidade Nova de Lisboa)
- Maciej Obremski (National University of Singapore)
- Manoj Prabhakaran (IIT Bombay)
- Mark Simkin (Ethereum Foundation)
- Mingyuan Wang (UC Berkeley)
- Mor Weiss (Bar-Ilan University)
- Mukul Kulkarni (TII Abu Dhabi)
- Noah Stephens-Davidowitz (Cornell University)
- Noam Mazor (Tel Aviv University)
- Sruthi Sekar (UC Berkeley)
- Srijita Kundu (University of Waterloo)
- Tianren Liu (Peking University)
- Xin Li (Johns Hopkins University)
- Yiannis Tselekounis (Royal Holloway University of London)

### External Reviewers

Albert Yu, Alexander Bienstock, Eldon Chung, Hamidreza Amini Khorasgani, Hannah Keller, Naty Peter, Pedro Branco, Seunghoon Lee, Suparno Ghoshal, Varun Narayanan, Wei Cheng, Xiuyu Ye, Zeyong Li.



