

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

PRINT ISBN: 979-8-3313-0309-9

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>

■ 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, with Preprocessing	
<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