1st Conference on Information-Theoretic Cryptography

ITC 2020, June 17–19, 2020, Boston, MA, USA

Edited by

Yael Tauman Kalai
Adam D. Smith
Daniel Wichs

LIPICS

Editors

Yael Tauman Kalai
Microsoft Research New England, Cambridge, MA, USA
yael@microsoft.com

Adam D. Smith
Boston University, MA, USA
ads22@bu.edu

Daniel Wichs
Northeastern University, Boston, MA, USA
NTT Research, Boston, MA, USA
wichs@ccs.neu.edu

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

ISBN 978-3-95977-151-1

PRINT ISBN: 978-1-7138-1472-6

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/978-3-95977-151-1.

Publication date
June, 2020

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 3.0 Unported license (CC-BY 3.0): https://creativecommons.org/licenses/by/3.0/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.2020.0

ISBN 978-3-95977-151-1 **ISSN 1868-8969** **https://www.dagstuhl.de/lipics**

Contents

Preface
Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs 0:vii

Steering Committee
.... 0:ix

Organization
.... 0:xi

Authors
.... 0:xiii–0:xiv

Regular Papers

Separating Local & Shuffled Differential Privacy via Histograms
Victor Balcer and Albert Cheu 1:1–1:14

d-Multiplicative Secret Sharing for Multipartite Adversary Structures
Reo Eriguchi and Noboru Kunihiro 2:1–2:16

Efficient MPC with a Mixed Adversary
Martin Hirt and Marta Mularczyk 3:1–3:23

Practical Relativistic Zero-Knowledge for NP
Claude Crépeau, Arnaud Y. Massenet, Louis Salvail,
Lucas Shigeru Stinchcombe, and Nan Yang 4:1–4:18

Use Your Brain! Arithmetic 3PC for Any Modulus with Active Security
Hendrik Eerikson, Marcel Keller, Claudio Orlandi, Pille Pullonen,
Joonas Puura, and Mark Simkin 5:1–5:24

Expander Graphs Are Non-Malleable Codes
Peter Michael Reichstein Rasmussen and Amit Sahai 6:1–6:10

Leakage-Resilient Secret Sharing in Non-Compartmentalized Models
Fuchun Lin, Mahdi Cheraghchi, Venkatesan Guruswami,
Reihaneh Safavi-Naini, and Huaxiong Wang 7:1–7:24

Lower Bounds for Function Inversion with Quantum Advice
Kai-Min Chung, Tai-Ning Liao, and Luowen Qian 8:1–8:15

Out-Of-Band Authenticated Group Key Exchange: From Strong Authentication to Immediate Key Delivery
Moni Naor, Lior Rotem, and Gil Segev 9:1–9:25

Hardness vs. (Very Little) Structure in Cryptography: A Multi-Prover Interactive Proofs Perspective
Gil Segev and Ido Shahaf 10:1–10:23

Oblivious Parallel Tight Compaction
Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, Enoch Peserico, and Elaine Shi .. 11:1–11:23

1st Conference on Information-Theoretic Cryptography (ITC 2020).
Editors: Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

On Polynomial Secret Sharing Schemes
Anat Paskin-Cherniavsky and Radune Artiom 12:1–12:21

One-One Constrained Pseudorandom Functions
Naty Peter, Rotem Tsabary, and Hoeteck Wee 13:1–13:22

The Power of Synergy in Differential Privacy: Combining a Small Curator with Local Randomizers
Amos Beimel, Aleksandra Korolova, Kobbi Nissim, Or Sheffet, and Uri Stemmer . 14:1–14:25

Pure Differentially Private Summation from Anonymous Messages
Badih Ghazi, Noah Golowich, Ravi Kumar, Pasin Manurangsi, Rasmus Pagh, and Ameya Velingker 15:1–15:23

On Locally Decodable Codes in Resource Bounded Channels
Jeremiah Blocki, Shubhang Kulkarni, and Samson Zhou 16:1–16:23