

2nd Conference on Information-Theoretic Cryptography

ITC 2021, July 23–26, 2021, Virtual Conference

Edited by

Stefano Tessaro



Editor

Stefano Tessaro

University of Washington, Seattle, WA, USA
tessaro@cs.washington.edu

ACM Classification 2012

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

ISBN 978-3-95977-197-9

PRINT ISBN: 978-1-7138-3445-8

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/978-3-95977-197-9>.

Publication date

July, 2021

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.2021.0

ISBN 978-3-95977-197-9

ISSN 1868-8969

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

■ Contents

Preface	
<i>Stefano Tessaro</i>	0:vii

Regular Papers

Group Structure in Correlations and Its Applications in Cryptography <i>Guru-Vamsi Policharla, Manoj Prabhakaran, Rajeev Raghunath, and Parjanya Vyas</i>	1:1–1:23
More Communication Lower Bounds for Information-Theoretic MPC <i>Ivan Bjerre Damgård, Boyang Li, and Nikolaj Ignatieff Schwartzbach</i>	2:1–2:18
On Prover-Efficient Public-Coin Emulation of Interactive Proofs <i>Gal Arnon and Guy N. Rothblum</i>	3:1–3:15
On the Randomness Complexity of Interactive Proofs and Statistical Zero-Knowledge Proofs <i>Benny Applebaum and Eyal Golombek</i>	4:1–4:23
Line-Point Zero Knowledge and Its Applications <i>Samuel Dittmer, Yuval Ishai, and Rafail Ostrovsky</i>	5:1–5:24
ZK-PCPs from Leakage-Resilient Secret Sharing <i>Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, and Mor Weiss</i>	6:1–6:21
Secure Merge with $O(n \log \log n)$ Secure Operations <i>Brett Hemenway Falk and Rafail Ostrovsky</i>	7:1–7:29
Perfectly Oblivious (Parallel) RAM Revisited, and Improved Constructions <i>T-H. Hubert Chan, Elaine Shi, Wei-Kai Lin, and Kartik Nayak</i>	8:1–8:23
On the Complexity of Anonymous Communication Through Public Networks <i>Megumi Ando, Anna Lysyanskaya, and Eli Upfal</i>	9:1–9:25
Broadcast Secret-Sharing, Bounds and Applications <i>Ivan Bjerre Damgård, Kasper Green Larsen, and Sophia Yakoubov</i>	10:1–10:20
Locally Reconstructable Non-Malleable Secret Sharing <i>Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, Sruthi Sekar, and Jenit Tomy</i>	11:1–11:19
Linear Threshold Secret-Sharing with Binary Reconstruction <i>Marshall Ball, Alper Çakan, and Tal Malkin</i>	12:1–12:22
Doubly-Affine Extractors, and Their Applications <i>Yevgeniy Dodis and Kevin Ye</i>	13:1–13:23
Online Linear Extractors for Independent Sources <i>Yevgeniy Dodis, Siyao Guo, Noah Stephens-Davidowitz, and Zhiye Xie</i>	14:1–14:14
Code Offset in the Exponent <i>Luke Demarest, Benjamin Fuller, and Alexander Russell</i>	15:1–15:23

2nd Conference on Information-Theoretic Cryptography (ITC 2021).

Editor: Stefano Tessaro



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

P_4 -free Partition and Cover Numbers & Applications <i>Alexander R. Block, Simina Brânzei, Hemanta K. Maji, Himanshi Mehta, Tamalika Mukherjee, and Hai H. Nguyen</i>	16:1–16:25
Replacing Probability Distributions in Security Games via Hellinger Distance <i>Kenji Yasunaga</i>	17:1–17:15
Differentially Private Approximations of a Convex Hull in Low Dimensions <i>Yue Gao and Or Sheffet</i>	18:1–18:16
Differentially Oblivious Database Joins: Overcoming the Worst-Case Curse of Fully Oblivious Algorithms <i>Shumo Chu, Danyang Zhuo, Elaine Shi, and T-H. Hubert Chan</i>	19:1–19:24
Communication Complexity of Private Simultaneous Quantum Messages Protocols <i>Akinori Kawachi and Harumichi Nishimura</i>	20:1–20:19
Quantum-Access Security of the Winternitz One-Time Signature Scheme <i>Christian Majenz, Channele Matadah Manfouo, and Maris Ozols</i>	21:1–21:22
On the Security of Proofs of Sequential Work in a Post-Quantum World <i>Jeremiah Blocki, Seunghoon Lee, and Samson Zhou</i>	22:1–22:27
Fooling an Unbounded Adversary with a Short Key, Repeatedly: The Honey Encryption Perspective <i>Xinze Li, Qiang Tang, and Zhenfeng Zhang</i>	23:1–23:21
T_5 : Hashing Five Inputs with Three Compression Calls <i>Yevgeniy Dodis, Dmitry Khovratovich, Nicky Mouha, and Mridul Nandi</i>	24:1–24:23
Post-Compromise Security in Self-Encryption <i>Gwangbae Choi, F. Betül Durak, and Serge Vaudenay</i>	25:1–25:23
Generic-Group Identity-Based Encryption: A Tight Impossibility Result <i>Gili Schul-Ganz and Gil Segev</i>	26:1–26:23