

# 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**

*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>

## 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 (*Chair*, Reykjavik University, IS and Gran Sasso Science Institute, IT)
- Christel Baier (TU Dresden, DE)
- Mikolaj Bojanczyk (University of Warsaw, PL)
- Roberto Di Cosmo (Inria and Université de Paris, FR)
- Faith Ellen (University of Toronto, CA)
- Javier Esparza (TU München, DE)
- Daniel Král' (Masaryk University - Brno, CZ)
- Meena Mahajan (Institute of Mathematical Sciences, Chennai, IN)
- Anca Muscholl (University of Bordeaux, FR)
- Chih-Hao Luke Ong (University of Oxford, GB)
- 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)

**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 Venkatasubramanian, 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 Yeo</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

## ■ Preface

In its second edition, the conference on Information-Theoretic Cryptography (ITC) was once again affected by the COVID-19 pandemic. After an initial optimistic attempt to organize a hybrid conference in Bertinoro, Italy, with Daniele Venturi as the general chair, the organizers had to finally revert, once again, to a virtual event.

The importance of ITC in the landscape of cryptography conferences is very evident, as information-theoretic cryptography continues to flourish, in old and new forms. It is rare to find cryptographic problems whose study does not give rise to interesting information-theoretic questions, and this year's program is a clear testament to this. It covers a diverse and exciting range of topics, from foundations all the way to real-world applications.

We have received a total of forty-six submissions, and the nineteen members of our program committee, helped by a number of external reviewers, accepted twenty-six of them. As in the previous edition, we have set a high bar for selection, without targeting a particular number of accepted papers. The unusually high acceptance rate is solely an indication of the high quality of these submissions. And despite our best efforts, I am quite certain we have still managed to reject submissions that were well deserving of acceptance. The conference also includes six spotlight talks, and possibly other events, which are still being arranged at the time of finalizing this volume.

None of this would be possible without all of those who have contributed to making ITC a success. First of all, I would like to thank the authors of all papers (accepted or not) for submitting their works. I am also indebted to all PC members for their tireless reviewing efforts and their insightful discussions, and to all external reviewers for dedicating their time to this effort. Once again, the members of the ITC Steering Committee, led by Benny Applebaum, have been giving extremely valuable advice while organizing a conference in such uncertain times. I also want to particularly thank Daniele Venturi, this year's general chair, for his work on the logistics of the conference, and for his attempts to bring ITC physically to Italy. And of course, I want to thank all invited speakers, presenting authors, and participants for committing their time to making this second edition a success, despite all circumstances.







## ■ 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 (Microsoft Research New England)
- Stefano Tessaro (University of Washington)
- Vinod Vaikuntanathan (MIT)
- Hoeteck Wee (NTT Research)
- Daniel Wichs (Northeastern University and NTT Research)
- Mary Wootters (Stanford)
- Chaoping Xing (Nanyang Technological University)
- Moti Yung (Google)





## ■ Organization

### General Chair

- Daniele Venturi (Sapienza University of Rome)

### Program Chair

- Stefano Tessaro (University of Washington)

### Program Committee

- Anat Paskin-Cherniavsky (Ariel University)
- Arpita Patra (Indian Institute of Science)
- Christian Majenz (QuSoft and CWI)
- Divesh Aggarwal (National University of Singapore)
- Eyal Kushilevitz (Technion)
- Fang Song (Portland State University)
- Gilad Asharov (Bar-Ilan University)
- Ignacio Cascudo (IMDEA Software Institute)
- Kai-Min Chung (Academia Sinica)
- Krzysztof Pietrzak (IST Austria)
- Mark Bun (Boston University)
- Marshall Ball (Columbia University and University of Washington)
- Martin Hirt (ETH Zurich)
- Mary Wootters (Stanford University)
- Mohammad Mahmoody (University of Virginia)
- Sidharth Jaggi (Chinese University of Hong Kong and University of Bristol)
- Siyao Guo (NYU Shanghai)
- Uri Stemmer (Ben-Gurion University)
- Vipul Goyal (CMU and NTT Research)

### External Reviewers

Navid Alamati, Daniel Apon, Fabio Banfi, Mihir Bellare, Varsha Bhat, Eldon Chung, Alexandru Cojocaru, Wei Dai, Dean Doron, Antonio Faonio, Serge Fehr, Kai Gallert, Konstantin Gegier, Emanuele Giunta, Aarushi Goel, Jesse Goodman, Alex B. Grilo, Koki Hamada, Aditya Hegde, Yao-Ching Hsieh, Mi-Ying Huang, Shih-Han Hung, Joseph Jaeger, Eliran Kachlon, Ilan Komargodski, Ashutosh Kumar, Rajendra Kumar, David Lanzemberger, Zeyong Li, Jyun-Jie Liao, Wei-Kai Lin, Yao-Ting Lin, Chen-Da Liu Zhang, Pasin Manurangsi, Maciej Obremski, Periklis A. Papakonstantinou, Protik Paul, Alice Pellet-Mary, Christopher Portmann, Youming Qiao, Guilherme Rito, Fu Shiuan, Yifan Song, Jana Sotáková, Ziteng Sun, Ajith Suresh, Prashant Vasudevan, Daniel Wichs, Zhiye Xie, Takashi Yamakawa, Maki Yoshida, Yanbao Zhang, Sebastian Zur

2nd Conference on Information-Theoretic Cryptography (ITC 2021).  
Editor: Stefano Tessaro



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

