2nd Conference on Information-Theoretic Cryptography

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

Edited by

Stefano Tessaro

LIPICS

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.

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.

ISSN 1868-8969

https://www.dagstuhl.de/lipics

Contents

Regular Papers

2nd Conference on Information-Theoretic Cryptography (ITC 2021).
Editor: Stefano Tessaro
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

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.

2nd Conference on Information-Theoretic Cryptography (ITC 2021).
Editor: Stefano Tessaro
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

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)

2nd Conference on Information-Theoretic Cryptography (ITC 2021).
Editor: Stefano Tessaro
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

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 Lanzenberger, 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