16th Conference on the Theory of Quantum Computation, Communication and Cryptography

TQC 2021, July 5–8, 2021, Virtual Conference

Edited by

Min-Hsiu Hsieh

Editors

Min-Hsiu Hsieh
Hon Hai (Foxconn) Quantum Computing Research Center, Taipei, Taiwan
minhsiuh@gmail.com

ACM Classification 2012
Theory of computation → Quantum computation theory; Theory of computation → Quantum complexity theory; Theory of computation → Quantum information theory; Theory of computation → Quantum communication complexity; Hardware → Quantum communication and cryptography; Hardware → Quantum error correction and fault tolerance

ISBN 978-3-95977-198-6

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/978-3-95977-198-6.

Publication date
June, 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.TQC.2021.0

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
Min-Hsiu Hsieh 0:vii

Conference Organization
..... 0:ix–0:x

List of Authors
..... 0:xi

Regular Papers

Quantum Time-Space Tradeoff for Finding Multiple Collision Pairs
Yassine Hamoudi and Frédéric Magniez 1:1–1:21

Quantum Pseudorandomness and Classical Complexity
William Kretschmer 2:1–2:20

Sample Efficient Algorithms for Learning Quantum Channels in PAC Model and the Approximate State Discrimination Problem
Kai-Min Chung and Han-Hsuan Lin 3:1–3:22

StoqMA Meets Distribution Testing
Yupan Liu 4:1–4:22

Fault-Tolerant Syndrome Extraction and Cat State Preparation with Fewer Qubits
Prithviraj Prabhu and Ben W. Reichardt 5:1–5:13

A Note About Claw Function with a Small Range
Andris Ambainis, Kaspars Balodis, and Jānis Iraids 6:1–6:5

Fast and Robust Quantum State Tomography from Few Basis Measurements
Daniel Stilck França, Fernando G.S L. Brandão, and Richard Kueng 7:1–7:13

Pauli Error Estimation via Population Recovery
Steven T. Flammia and Ryan O'Donnell 8:1–8:16

Quantum Probability Oracles & Multidimensional Amplitude Estimation
Joran van Apeldoorn 9:1–9:11

Quantum Logarithmic Space and Post-Selection
François Le Gall, Harumichi Nishimura, and Abuzer Yakaryılmaz 10:1–10:17

16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021).
Editor: Min-Hsiu Hsieh
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

The 16th Conference on the Theory of Quantum Computation, Communication and Cryptography was hosted by the University of Latvia, and held online from July 5–8, 2021.

Quantum computation, quantum communication, and quantum cryptography are subfields of quantum information processing, an interdisciplinary field of information science and quantum mechanics. The TQC conference series focuses on theoretical aspects of these subfields. The objective of the conference is to bring together researchers so that they can interact with each other and share problems and recent discoveries.

A list of the previous editions of TQC follows:

- TQC 2020, University of Latvia, Latvia
- TQC 2019, University of Maryland, USA
- TQC 2018, University of Technology Sydney, Australia
- TQC 2017, Université Pierre et Marie Curie, France
- TQC 2016, Freie Universität Berlin, Germany
- TQC 2015, Université libre de Bruxelles, Brussels, Belgium
- TQC 2014, National University of Singapore, Singapore
- TQC 2013, University of Guelph, Canada
- TQC 2012, University of Tokyo, Japan
- TQC 2011, Universidad Complutense de Madrid, Spain
- TQC 2010, University of Leeds, UK
- TQC 2009, Institute for Quantum Computing, University of Waterloo, Canada
- TQC 2008, University of Tokyo, Japan
- TQC 2007, Nara Institute of Science and Technology, Nara, Japan
- TQC 2006, NTT R&D Center, Atsugi, Kanagawa, Japan

The conference consisted of invited talks, contributed talks, a poster session, and a business meeting. The invited talks were given by Scott Aaronson (UT Austin), Srinivasan Arunachalam (IBM T. J. Watson Research Center), Cécilia Lancien (Institut de Mathématiques de Toulouse and CNRS), and Kai-Min Chung (Academia Sinica).

16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021).
Editor: Min-Hsiu Hsieh
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Conference Organization

Local Organizing Committee

- Andris Ambainis (chair)
  Latvia
- Kaspars Čikste
  Latvia
- Jelena Glušakova
  Latvia
- Juris Smotrovs
  Latvia
- Aleksandrs Rivoss
  Latvia
- Dace Šostaka
  Latvia
- Jevgēnijs Vihrovs
  Latvia
- Jānis Iraids
  Latvia
- Mārtiņš Kālis
  Latvia
- Andis Draguns
  Latvia
- Matıss Apinis
  Latvia

Program Committee

- Barbara Amaral
  Universidade de São Paulo
- Anurag Anshu
  University of California, Berkeley
- Srinivasan Arunachalam
  IBM T. J. Watson Research Center
- Juani Bermejo-Vega
  University of Granada
- Hao-Chung Cheng
  National Taiwan University
- Giulio Chiribella
  QICI, The University of Hong Kong
- Patrick Coles
  Los Alamos National Laboratory
- Matthew Coudron
  NIST/UMD
- Yfke Dulek
  QuSoft/CWI, Amsterdam
- Bill Fefferman
  University of Chicago
- Christoph Hirche
  Københavns Universitet
- Min-Hsiu Hsieh (Chair)
  Hon Hai Quantum Computing Center
- Rahul Jain
  National University of Singapore
- Anna Jenčovà
  Slovak Academy of Sciences
- Maria Kieferova
  University of Technology Sydney
- Isaac Kim
  University of Sydney
- Ludovico Lami
  Universität Ulm
- Felix Leditzky
  University of Illinois at Urbana-Champaign
- Anthony Leverrier
  Inria
- Guang-Hao Low
  Microsoft
- Chandrashekar C M
  Institute of Mathematical Sciences
- Xiongfeng Ma
  Tsinghua University
- Tomoyuki Morimae
  Kyoto University
- Anand Natarajan
  MIT
- Miguel Navascues
  IQOQI Vienna
- Yingkai Ouyang
  National University of Singapore
- Dave Touchette
  Université de Sherbrooke

16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021).
Editor: Min-Hsiu Hsieh
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

- Anna Vershynina
  University of Houston
- Julio I. de Vicente
  Universidad Carlos III de Madrid
- Mischa Woods
  ETH
- Penghui Yao
  Nanjing University
- Jon Yard
  IQC/Perimeter Institute
- Quntao Zhuang
  University of Arizona

Steering Committee

- Gorjan Alagic
  Maryland
- Andris Ambainis
  Latvia
- Anne Broadbent
  Ottawa
- Eric Chitambar
  UIUC
- Steven Flammia
  AWS
- Stacey Jeffery (chair)
  QuSoft, CWI
- Laura Mančinska
  Copenhagen
- Marco Tomamichel
  NUS

List of Authors

Andris Ambainis (6)
Center for Quantum Computer Science, Faculty of Computing, University of Latvia, Riga, Latvia

Kaspars Balodis (6)
Center for Quantum Computer Science, Faculty of Computing, University of Latvia, Riga, Latvia

Fernando G.S L. Brandão (7)
AWS Center for Quantum Computing, Pasadena, CA, USA; Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA, USA

Kai-Min Chung (3)
Institute of Information Science, Academia Sinica, Taipei, Taiwan

Steven T. Flammia (8)
AWS Center for Quantum Computing, Pasadena, CA, USA; IQIM, California Institute of Technology, Pasadena, CA, USA

Daniel Stilck França (7)
QMATH, Department of Mathematical Sciences, University of Copenhagen, Denmark

Yassine Hamoudi (1)
Université de Paris, IRIF, CNRS, F-75013 Paris, France

Jānis Iraids (6)
Center for Quantum Computer Science, Faculty of Computing, University of Latvia, Riga, Latvia

William Kretschmer (2)
University of Texas at Austin, TX, USA

Richard Kueng (7)
Institute for Integrated Circuits, Johannes Kepler University Linz, Austria

François Le Gall (10)
Graduate School of Mathematics, Nagoya University, Japan

Han-Hsuan Lin (3)
Department of Computer Science, National Tsing Hua University, Hsinchu, Taiwan

Yupan Liu (4)
Shenzhen, China

Frédéric Magniez (1)
Université de Paris, IRIF, CNRS, F-75013 Paris, France

Harumichi Nishimura (10)
Graduate School of Informatics, Nagoya University, Japan

Ryan O'Donnell (8)
Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, USA

Prithviraj Prabhu (5)
Department of Electrical and Computer Engineering, University of Southern California, Los Angeles, CA, USA

Ben W. Reichardt (5)
Department of Electrical and Computer Engineering, University of Southern California, Los Angeles, CA, USA

Joran van Apeldoorn (9)
Institute for Information Law, University of Amsterdam, The Netherlands; QuSoft, Centrum Wiskunde & Informatica, Amsterdam, The Netherlands

Abuzer Yakaryılmaz (10)
Center for Quantum Computer Science, University of Latvia, Rīga, Latvia; QWorld Association, Tallinn, Estonia

16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021).
Editor: Min-Hsiu Hsieh
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany