

# 15th Conference on the Theory of Quantum Computation, Communication and Cryptography

TQC 2020, June 9–12, 2020, Riga, Latvia

Edited by

Steven T. Flammia



*Editors*

**Steven T. Flammia** 

University of Sydney, Australia  
steven.flammia@sydney.edu.au

*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 978-3-95977-146-7**

*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/978-3-95977-146-7>.

*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.TQC.2020.0

ISBN 978-3-95977-146-7

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*, Gran Sasso Science Institute and Reykjavik University)
- Christel Baier (TU Dresden)
- Mikolaj Bojanczyk (University of Warsaw)
- Roberto Di Cosmo (INRIA and University Paris Diderot)
- Javier Esparza (TU München)
- Meena Mahajan (Institute of Mathematical Sciences)
- Dieter van Melkebeek (University of Wisconsin-Madison)
- Anca Muscholl (University Bordeaux)
- Luke Ong (University of Oxford)
- Catuscia Palamidessi (INRIA)
- Thomas Schwentick (TU Dortmund)
- Raimund Seidel (Saarland University and Schloss Dagstuhl – Leibniz-Zentrum für Informatik)

**ISSN 1868-8969**

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



## ■ Contents

Preface	
<i>Steven T. Flammia</i> .....	0:vii
Conference Organization	
.....	0:ix
Exponential Quantum Communication Reductions from Generalizations of the Boolean Hidden Matching Problem	
<i>João F. Doriguello and Ashley Montanaro</i> .....	1:1–1:16
Improved Approximate Degree Bounds for $k$ -Distinctness	
<i>Nikhil S. Mande, Justin Thaler, and Shuchen Zhu</i> .....	2:1–2:22
Building Trust for Continuous Variable Quantum States	
<i>Ulysse Chabaud, Tom Douce, Frédéric Grosshans, Elham Kashefi, and Damian Markham</i> .....	3:1–3:15
Uncloneable Quantum Encryption via Oracles	
<i>Anne Broadbent and Sébastien Lord</i> .....	4:1–4:22
Quasirandom Quantum Channels	
<i>Tom Bannink, Jop Briët, Farrokh Labib, and Hans Maassen</i> .....	5:1–5:20
Towards Quantum One-Time Memories from Stateless Hardware	
<i>Anne Broadbent, Sevag Gharibian, and Hong-Sheng Zhou</i> .....	6:1–6:25
Beyond Product State Approximations for a Quantum Analogue of Max Cut	
<i>Anurag Anshu, David Gosset, and Karen Morenz</i> .....	7:1–7:15
Simpler Proofs of Quantumness	
<i>Zvika Brakerski, Venkata Koppula, Umesh Vazirani, and Thomas Vidick</i> .....	8:1–8:14
Quantum Algorithms for Computational Geometry Problems	
<i>Andris Ambainis and Nikita Larka</i> .....	9:1–9:10
Quantum Coupon Collector	
<i>Srinivasan Arunachalam, Aleksandrs Belovs, Andrew M. Childs, Robin Kothari, Ansis Rosmanis, and Ronald de Wolf</i> .....	10:1–10:17
Fast and Effective Techniques for T-Count Reduction via Spider Nest Identities	
<i>Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang</i> .....	11:1–11:23
A Device-Independent Protocol for XOR Oblivious Transfer <sup>1</sup>	
<i>Srijita Kundu, Jamie Sikora, and Ernest Y.-Z. Tan</i> .....	12:1–12:15

<sup>1</sup> Note of the publisher: Unfortunately, this article was accidentally skipped in the first version of the conference proceedings published on June 8, 2020 and was subsequently published on August 19, 2020.





## ■ Preface

The 15th Conference on the Theory of Quantum Computation, Communication and Cryptography was hosted by the University of Latvia, and held online from June 9–12, 2020.

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 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, a rump session, and a business meeting. The invited talks were given by Elena Kirshanova (Immanuel Kant Baltic Federal University), Thomas Monz (University of Innsbruck), Xin Wang (Baidu Research), and Henry Yuen (University of Toronto).

The conference was possible thanks to financial support from the European Regional Development Fund (project 1.1.1.5/18/I/016), Baidu, and the University of Latvia.

We wish to thank the members of the Program Committee and all subreviewers for their precious help. Our warm thanks also go to the members of the Local Organizing Committee, for their considerable efforts in organizing the conference. We would like to thank Michael Wagner (Dagstuhl Publishing) for his technical help. Finally, we would like to thank the members of the Steering Committee for giving us the opportunity to work for TQC. And, of course, all contributors and participants!

April 2020  
Steven T. Flammia







# ■ Conference Organization

## Local Organizing Committee

- Andris Ambainis (chair)  
Latvia
- Kaspars Čikste  
Latvia
- Jelena Polakova  
Latvia
- Juris Smotrovs  
Latvia
- Aleksandrs Rivoss  
Latvia
- Dace Sostoka  
Latvia

## Program Committee

- Victor Albert  
Caltech
- Itai Arad  
Technion
- Rotem Arnon-Friedman  
Berkeley
- Salman Beigi  
IPM, Tehran
- Chris Chubb  
Sherbrooke
- Richard Cleve  
Waterloo
- Elizabeth Crosson  
New Mexico
- Gemma De las Cuevas  
Innsbruck
- Lída del Rio  
ETH Zurich
- Steven Flammia (chair)  
University of Sydney
- Keisuke Fujii  
Osaka
- David Gosset (co-chair)  
Waterloo
- Markus Grassl  
Gdańsk
- Min-Hsiu Hsieh  
University of Technology, Sydney
- Shelby Kimmel  
Middlebury
- Martin Kliesch  
Düsseldorf
- Cécilia Lancien  
Toulouse
- Angelo Lucia  
Caltech
- Prabha Mandayam  
IIT Madras
- Ashley Montanaro  
Bristol
- Hui Khoo Ng  
NUS
- Mark Wilde  
Louisiana State
- Xiaodi Wu  
Maryland
- Sisi Zhou  
Chicago

## Steering Committee

- Gorjan Alagic  
Maryland
- Andris Ambainis  
Latvia
- Anne Broadbent (chair)  
Ottawa
- Aram Harrow  
MIT
- Stacey Jeffery  
QuSoft, CWI
- Laura Mančinska  
Copenhagen
- Marco Tomamichel  
UTS

15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020).  
Editor: Steven T. Flammia



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



