12th Conference on the Theory of Quantum Computation, Communication, and Cryptography

TQC 2017, June 14–16, 2017, Paris, France

Edited by

Mark M. Wilde

LIPICS

Editor

Mark M. Wilde
Hearne Institute for Theoretical Physics
Department of Physics and Astronomy
Center for Computation and Technology
Louisiana State University
Baton Rouge, Louisiana 70803, USA `mwilde@lsu.edu`

ACM Classification 1998
E.3 Data Encryption, E.4 Coding and Information Theory, F Theory of Computation

ISBN 978-3-95977-034-7

Published online and open access by
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at http://www.dagstuhl.de/dagpub/978-3-95977-034-7.

Publication date
February, 2018

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 http://dnb.d-nb.de.

Digital Object Identifier: 10.4230/LIPIcs.TQC.2017.0

ISBN 978-3-95977-034-7 **ISSN 1868-8969** **http://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

http://www.dagstuhl.de/lipics

Contents

Papers

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

The 12th Conference on the Theory of Quantum Computation, Communication, and Cryptography was organized by the Université Pierre et Marie Curie and the Paris Centre for Quantum Computing from the 14th to the 16th of June 2017. 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 2016, Freie Universität Berlin, Germany
- TQC 2015, Université libre de Bruxelles, Belgium
- TQC 2014, National University of Singapore, Singapore
- TQC 2013, University of Guelph, Canada
- TQC 2012, The 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, and a poster session. Contributed talks were solicited for two tracks: Conference Track and Workshop Track. The accepted submissions to the Conference Track appear in these Proceedings, as well as a selection of some that were accepted to the Workshop Track. The papers in these proceedings are listed in their order of submission.

The invited talks were given by David Gosset (IBM), Stephen Jordan (National Institute of Standards and Technology / University of Maryland), Stephen Piddock (University of Bristol), and Barbara Terhal (Delft University of Technology).

The conference was possible thanks to generous donations from Microsoft, CryptoWorks21, Paris Centre for Quantum Computing, Laboratoire d'Informatique de Paris 6, as well as the Institute of Physics. I am indebted to the members of the Program Committee and all subreviewers for their precious contribution in reviewing the submissions. I also wish to thank the members of the Local Organizing Committee, especially Damian Markham, for their considerable efforts in organizing the conference. I would like to thank Marc Herbstritt and Michael Wagner (Dagstuhl Publishing) for their technical help. Finally, I would like to thank the members of the Steering Committee for offering me this opportunity and for their support, and I also thank all contributors and participants.

Mark M. Wilde
October 2017

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Conference Organization

Local organizing committee

Damian Markham – chair
Eleni Diamanti – co-chair
Elham Kashefi – co-chair
André Chailloux
Tom Douce
Frédéric Grosshans
Marc Kaplan
Iordanis Kerenidis
Anthony Leverrier
and the entire Quantum Information group at the UPMC

Programme committee

Dominic Berry (Macquarie University)
Mario Berta (Caltech)
Sergey Bravyi (IBM)
Michael Bremner (University Technology Sydney)
Roger Colbeck (University of York)
Nilanjana Datta (University of Cambridge)
David Elkouss (Delft University of Technology)
Omar Fawzi (ENS de Lyon)
Markus Grassl (Max Planck Erlangen)
David Gross (University Freiburg)
Rahul Jain (National University of Singapore)
Zhengfeng Ji (University Technology Sydney)
Stephen Jordan (NIST / University of Maryland)
Shelby Kimmel (University of Maryland / NIST)
Vadym Kliuchnikov (Microsoft)
Francois Le Gall (Kyoto University)
Troy Lee (Nanyang Technological University)
Yeong-Cherng Liang (National Cheng Kung University)
Yi-Kai Liu (NIST / University of Maryland)
Hoi-Kwong Lo (University of Toronto)
Laura Mancinska (University of Bristol)
Prabha Mandayam (IIT Madras)
Tomoyuki Morimae (Gunma University)
Tobias Osborne (University of Hannover)
Lidia del Rio (ETH Zuerich)
Neil J. Ross (University of Maryland / NIST)
Pradeep Sarvepalli (IIT Madras)
Valerio Scarani (National University of Singapore)
Ujjwal Sen (Harish-Chandra Research Institute)
Yaoyun Shi (University Michigan)

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Barbara Terhal (RWTH Aachen University)
Dave Touchette (University of Waterloo / Perimeter Institute)
John Watrous (University of Waterloo)
James Whitfield (Dartmouth College)
Mark M. Wilde (Louisiana State University) (PC Chair)
Man-Hong Yung (South University Science & Technology China)

Steering committee

Anne Broadbent (University of Ottawa)
Wim van Dam (University of California Santa Barbara)
Aram Harrow (Massachusetts Institute of Technology)
Yasuhito Kawano (NTT, Tokyo)
Michele Mosca (Institute for Quantum Computing, Waterloo and Perimeter Institute)
Martin Roetteler (Microsoft Research)
Simone Severini (University College London)
Vlatko Vedral (Oxford University and Centre for Quantum Technologies, Singapore)