

10th Conference on the Theory of Quantum Computation, Communication and Cryptography

TQC'15, May 20–22, 2015, Brussels, Belgium

Edited by

Salman Beigi

Robert König



Editors

Salman Beigi
Institute for Research in
Fundamental Sciences
Tehran, Iran
salman.beigi@gmail.com

Robert König
Institute for Advanced Study
and Zentrum Mathematik
Technische Universität München
Garching, Germany
robert.koenig@tum.de

ACM Classification 1998

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

ISBN 978-3-939897-96-5

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/978-3-939897-96-5>.

Publication date

November, 2015

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>.

License

This work is licensed under a Creative Commons Attribution 3.0 Unported license (CC-BY 3.0): <http://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.2015.i

ISBN 978-3-939897-96-5

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.

Editorial Board

- Susanne Albers (TU München)
- Chris Hankin (Imperial College London)
- Deepak Kapur (University of New Mexico)
- Michael Mitzenmacher (Harvard University)
- Madhavan Mukund (Chennai Mathematical Institute)
- Catuscia Palamidessi (INRIA)
- Wolfgang Thomas (*Chair*, RWTH Aachen)
- Pascal Weil (CNRS and University Bordeaux)
- Reinhard Wilhelm (Saarland University)

ISSN 1868-8969

<http://www.dagstuhl.de/lipics>

■ Contents

Oracles with Costs <i>Shelby Kimmel, Cedric Yen-Yu Lin, and Han-Hsuan Lin</i>	1
The Resource Theory of Steering <i>Rodrigo Gallego and Leandro Aolita</i>	27
How Many Quantum Correlations Are Not Local? <i>Carlos E. González-Guillén, C. Hugo Jiménez, Carlos Palazuelos, and Ignacio Villanueva</i>	39
The Spin-2 AKLT State on the Square Lattice is Universal for Measurement-based Quantum Computation <i>Tzu-Chieh Wei and Robert Raussendorf</i>	48
Quantum Capacity Can Be Greater Than Private Information for Arbitrarily Many Uses <i>David Elkouss and Sergii Strelchuk</i>	64
Semidefinite Programs for Randomness Extractors <i>Mario Berta, Omar Fawzi, and Volkher B. Scholz</i>	73
New Constructions for Quantum Money <i>Marios Georgiou and Iordanis Kerenidis</i>	92
Decoherence in Open Majorana Systems <i>Earl T. Campbell</i>	111
On the Closure of the Completely Positive Semidefinite Cone and Linear Approximations to Quantum Colorings <i>Sabine Burgdorf, Monique Laurent, and Teresa Piovesan</i>	127
Making Existential-unforgeable Signatures Strongly Unforgeable in the Quantum Random-oracle Model <i>Edward Eaton and Fang Song</i>	147
A Universal Adiabatic Quantum Query Algorithm <i>Mathieu Brandeho and Jérémie Roland</i>	163
Quantum Enhancement of Randomness Distribution <i>Raul Garcia-Patron, William Matthews, and Andreas Winter</i>	180
Implementing Unitary 2-Designs Using Random Diagonal-unitary Matrices <i>Yoshifumi Nakata, Christoph Hirche, Ciara Morgan, and Andreas Winter</i>	191
Round Elimination in Exact Communication Complexity <i>Jop Briët, Harry Buhrman, Debbie Leung, Teresa Piovesan, and Florian Speelman</i>	206
On the Robustness of Bucket Brigade Quantum RAM <i>Srinivasan Arunachalam, Vlad Gheorghiu, Tomas Jochym-O'Connor, Michele Mosca, and Priyaa Varshinee Srinivasan</i>	226
Interferometric Versus Projective Measurement of Anyons <i>Claire Leveillant and Michael Freedman</i>	245



■ Preface

The 10th Conference on the Theory of Quantum Computation, Communication and Cryptography was held at the Université libre de Bruxelles from the 20th to the 22nd of May 2015. 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 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. The invited talks were given by David DiVincenzo (RWTH Aachen & FZ Jülich), Sean Hallgren (Pennsylvania State University), Laura Mančinska (CQT Singapore) and Ronald de Wolf (CWI Amsterdam). The conference was possible thanks to the financial support of the Belgian Fund for Scientific Research (FNRS), Visit Brussels, Journal of Physics A, Cryptoworks21, the Engineering and Physical Research Council (EPSRC), as well as the Royal Society. 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 Marc Herbstritt and Michael Wagner (Dagstuhl Publishing) for their 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, we thank all contributors and participants!

August 2015

Salman Beigi and Robert König



■ Local Organizing Committee

Nicolas Cerf
Université libre de Bruxelles

Serge Massar
Université libre de Bruxelles

Stefano Pironio
Université libre de Bruxelles (chair)

Jérémie Roland
Université libre de Bruxelles (chair)

Philippe Spindel
Université de Mons

Frank Verstraete
Ghent University



■ Program Committee

Salman Beigi, IPM (chair)
Andrew Childs, University of Maryland
Matthias Christandl, Copenhagen
Toby Cubitt, Cambridge
Andrew Doherty, University of Sydney
Frédéric Dupuis, Aarhus
Sevag Gharibian, UC Berkeley and Virginia Commonwealth
Saikat Guha, BBN Technologies
Michał Horodecki, University of Gdansk
Peter Høyer, Calgary
Iordanis Kerenidis, Paris Diderot
Robert König, Technische Universität München (chair)
Troy Lee, NTU & CQT Singapore
Tobias Osborne, Hannover
Carlos Palazuelos, UCM Madrid
David Pérez-García, UCM Madrid
Ben Reichardt, University of Southern California
Kristan Temme, Caltech
Barbara Terhal, RWTH Aachen
Marco Tomamichel, University of Sydney
Christian Schaffner, University of Amsterdam
Tamás Vértesi, MTA Atomki
Thomas Vidick, Caltech
Pawel Wocjan, University of Central Florida



■ Steering Committee

Wim van Dam
University of California, Santa Barbara, USA

Yasuhito Kawano
NTT, Japan

Michele Mosca
IQC and University of Waterloo, Canada

Martin Roetteler
Microsoft Research, USA

Simone Severini
University College London, UK

Vlatko Vedral
University of Oxford, UK &
National University of Singapore, Singapore



