

9th Conference on the Theory of Quantum Computation, Communication and Cryptography

TQC 2014, May 21–23, 2014, National University of Singapore,
Singapore

Edited by

Steven T. Flammia

Aram W. Harrow



Editors

Steven T. Flammia
Department of Physics
University of Sydney

steven.flammia@sydney.edu.au

Aram W. Harrow
Department of Physics
Massachusetts Institute of Technology
aram@mit.edu

ACM Classification 1998

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

ISBN 978-3-939897-73-6

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/978-3-939897-73-6>.

Publication date

November 2014

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.2014.i

ISBN 978-3-939897-73-6

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 (Humboldt University Berlin)
- 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 (RWTH Aachen)
- Pascal Weil (*Chair*, University Bordeaux)
- Reinhard Wilhelm (Saarland University, Schloss Dagstuhl)

ISSN 1868-8969

www.dagstuhl.de/lipics

■ Contents

More Randomness From Noisy Sources <i>Jean-Daniel Bancal and Valerio Scarani</i>	1
Exact Classical Simulation of the GHZ Distribution <i>Gilles Brassard, Luc Devroye, and Claude Gravel</i>	7
On the Parallel Repetition of Multi-Player Games: The No-Signaling Case <i>Harry Buhrman, Serge Fehr, and Christian Schaffner</i>	24
Quantum Communication Complexity with Coherent States and Linear Optics <i>Juan Miguel Arrazola and Norbert Lütkenhaus</i>	36
Bounds on Entanglement Assisted Source-channel Coding Via the Lovász ϑ Number and Its Variants <i>Toby Cubitt, Laura Mančinska, David Roberson, Simone Severini, Dan Stahlke, and Andreas Winter</i>	48
Strong Converse for the Quantum Capacity of the Erasure Channel for Almost All Codes <i>Mark M. Wilde and Andreas Winter</i>	52
Graph-theoretical Bounds on the Entangled Value of Non-local Games <i>André Chailloux, Laura Mančinska, Giannicola Scarpa, and Simone Severini</i>	67
Optimal Bounds for Parity-Oblivious Random Access Codes with Applications <i>André Chailloux, Iordanis Kerenidis, Srijita Kundu, and Jamie Sikora</i>	76
Convexity Properties of the Quantum Rényi Divergences, with Applications to the Quantum Stein's Lemma <i>Milán Mosonyi</i>	88
Quantum Learning of Classical Stochastic Processes: The Completely-Positive Realization Problem <i>Alex Monras</i>	99
Hidden Subgroup Quantum Algorithms for a Class of Semi-Direct Product Groups <i>Wim van Dam and Siladitya Dey</i>	110
Difficult Instances of the Counting Problem for 2-quantum-SAT are Very Atypical <i>Niel de Beaudrap</i>	118
Circuit Obfuscation Using Braids <i>Gorjan Alagic, Stacey Jeffery, and Stephen Jordan</i>	141
Classical Simulation of Yang-Baxter Gates <i>Gorjan Alagic, Aniruddha Bapat, and Stephen Jordan</i>	161
Blindness and Verification of Quantum Computation with One Pure Qubit <i>Theodoros Kapourniotis, Elham Kashefi, and Animesh Datta</i>	176
Device-independent Randomness Extraction for Arbitrarily Weak Min-entropy Source <i>Jan Bouda, Marcin Pawłowski, Matej Pivoluska, and Martin Plesch</i>	205

Graph Homomorphisms for Quantum Players <i>Laura Mančinská and David Roberson</i>	212
Quantum Linear Network Coding as One-way Quantum Computation <i>Niel de Beaudrap and Martin Roetteler</i>	217

■ Preface

The 9th Conference on the Theory of Quantum Computation, Communication and Cryptography was held at the National University of Singapore, from the 21st to the 23rd May 2014.

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 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, a poster session, a rump session, and a business meeting. The invited talks were given by Fernando G. S. L. Brandão (University College London, London), Vittorio Giovannetti (NEST, Scuola Normale Superiore, Pisa) and Yaoyun Shi (University of Michigan, Ann Arbor).

The conference was possible thanks to the financial support of the Centre for Quantum Technologies, Singapore.

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, all contributors and participants!

November 2014

Steven T. Flammia and Aram W. Harrow



■ Local Organizing Committee

Rahul Jain
Centre for Quantum Technologies, NUS,
Singapore

Hartmut Klauck
Nanyang Technological University and
Centre for Quantum Technologies, NUS,
Singapore

Troy Lee (Chair)
Nanyang Technological University and
Centre for Quantum Technologies, NUS,
Singapore

Miklos Santha
Universite Paris Diderot – Paris 7, France
and Centre for Quantum Technologies, NUS,
Singapore

Evon Tan (Secretariat)
Centre for Quantum Technologies, NUS,
Singapore



■ Program Committee

Koenraad Audenaert
University of London, UK

Xiaodi Wu
MIT, USA

Michael Bremner
University of Technology Sydney, Australia

Jon Yard
Microsoft Research, USA

Jianxin Chen
IQC, University of Waterloo, Canada

Giulio Chiribella
Institute for Interdisciplinary Information
Sciences, Tsinghua University, China

Steve Flammia (co-chair)
The University of Sydney, Australia

Sean Hallgren
The Pennsylvania State University, USA

Aram Harrow (chair)
MIT, USA

Masahito Hayashi
Nagoya University, Japan and Centre for
Quantum Technologies, NUS, Singapore

Zhengfeng Ji
IQC, University of Waterloo, Canada

Robert Koenig
IQC, University of Waterloo, Canada

Ashley Montanaro
University of Bristol, UK

Marco Piani
University of Waterloo, Canada

Beth Ruskai
Tufts University, USA

Peter Turner
University of Tokyo, Japan

Frank Verstraete
University of Vienna, Austria

John Watrous
University of Waterloo, Canada

Mark Wilde
Louisiana State University, USA

9th Conference on the Theory of Quantum Computation, Communication and Cryptography.
Editors: Steven T. Flammia and Aram W. Harrow



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



■ 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



