

# 8th Conference on the Theory of Quantum Computation, Communication and Cryptography

TQC 2013, May 21–23, 2013, Guelph, Ontario, Canada

Edited by

Simone Severini

Fernando Brandao



#### *Editors*

Simone Severini  
Department of Computer Science  
University College London  
s.severini@ucl.ac.uk

Fernando Brandao  
Department of Computer Science  
University College London  
f.brandao@ucl.ac.uk

#### *ACM Classification 1998*

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

### **ISBN 978-3-939897-55-2**

#### *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/978-3-939897-55-2>.

#### *Publication date*

November, 2013

#### *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:

<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.2013.i

**ISBN 978-3-939897-55-2**

**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](http://www.dagstuhl.de/lipics)**



## ■ Contents

Ancilla Driven Quantum Computation with Arbitrary Entangling Strength <i>Kerem Halil Shah and Daniel K. L. Oi</i> .....	1
Another Subexponential-time Quantum Algorithm for the Dihedral Hidden Subgroup Problem <i>Greg Kuperberg</i> .....	20
Universal Entanglers for Bosonic and Fermionic Systems <i>Joel Klassen, Jianxin Chen, and Bei Zeng</i> .....	35
Easy and Hard Functions for the Boolean Hidden Shift Problem <i>Andrew M. Childs, Robin Kothari, Maris Ozols, and Martin Roetteler</i> .....	50
Dequantizing Read-once Quantum Formulas <i>Alessandro Cosentino, Robin Kothari, and Adam Paetznick</i> .....	80
The Minimum Size of Qubit Unextendible Product Bases <i>Nathaniel Johnston</i> .....	93
Robust Online Hamiltonian Learning <i>Christopher E. Granade, Christopher Ferrie, Nathan Wiebe, and D. G. Cory</i> ....	106
Classical and Quantum Algorithms for Testing Equivalence of Group Extensions <i>Kevin C. Zatloukal</i> .....	126
Provable Advantage for Quantum Strategies in Random Symmetric XOR Games <i>Andris Ambainis and Jānis Iraids</i> .....	146
Towards Efficient Decoding of Classical-Quantum Polar Codes <i>Mark M. Wilde, Olivier Landon-Cardinal, and Patrick Hayden</i> .....	157
On the Query Complexity of Perfect Gate Discrimination <i>Giulio Chiribella, Giacomo Mauro D’Ariano, and Martin Roetteler</i> .....	178
Symmetries of Codeword Stabilized Quantum Codes <i>Salman Beigi, Jianxin Chen, Markus Grassl, Zhengfeng Ji, Qiang Wang, and Bei Zeng</i> .....	192
Certifying the Absence of Apparent Randomness under Minimal Assumptions <i>Gonzalo de la Torre, Chirag Dhara, and Antonio Acín</i> .....	207
Is Global Asymptotic Cloning State Estimation? <i>Yuxiang Yang and Giulio Chiribella</i> .....	220
Distillation of Non-Stabilizer States for Universal Quantum Computation <i>Guillaume Duclos-Cianci and Krysta M. Svore</i> .....	235
Realistic Cost for the Model of Coherent Computing <i>Akira SaiToh</i> .....	244
Optimal Robust Self-Testing by Binary Nonlocal XOR Games <i>Carl A. Miller and Yaoyun Shi</i> .....	254



Exact Quantum Query Complexity of EXACT and THRESHOLD <i>Andris Ambainis, Jānis Iraids, and Juris Smotrovs</i> .....	263
The Quantum Entropy Cone of Stabiliser States <i>Noah Linden, František Matúš, Mary Beth Ruskai, and Andreas Winter</i> .....	270
Kitaev's $\mathbb{Z}_d$ -Codes Threshold Estimates <i>Guillaume Duclos-Cianci and David Poulin</i> .....	285
Optimal Quantum Circuits for Nearest-Neighbor Architectures <i>David J. Rosenbaum</i> .....	294
Access Structure in Graphs in High Dimension and Application to Secret Sharing <i>Anne Marin, Damian Markham, and Simon Perdrix</i> .....	308

## ■ Preface

The 8th Conference on the Theory of Quantum Computation, Communication and Cryptography was held at the University of Guelph, from the 21st to the 23rd May 2013.

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 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 Jop Briët (CWI, Amsterdam), Aram Harrow (MIT, Cambridge), Iordanis Kerenidis (CNRS – Université Paris Diderot-Paris 7, Paris), Thomas Vidick (MIT, Cambridge), and Stephanie Wehner (National University of Singapore, Singapore).

The conference was possible thanks to the financial support of the Institute for Quantum Computing (IQC) at the University of Waterloo, the Perimeter Institute for Theoretical Physics (PI), the Fields Institute for Research in Mathematical Sciences, and the University of Guelph.

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, and to Sarah Plosker, James Howard, and Tyler Jackson, for their help at the registration desk. 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!

October 2013

Fernando Brandao and Simone Severini







## ■ Conference Organization

### Local Organizing Committee

Jianxin Chen	University of Guelph, Canada
Zhengfeng Ji	IQC and University of Waterloo, Canada
David Kribs ( <i>Chair</i> )	University of Guelph, Canada
Bei Zeng ( <i>Co-chair</i> )	University of Guelph, Canada

### Program Committee

Antonio Acin	ICFO Barcelona, Spain
Gorjan Alagic	Caltech, USA
Salman Beigi	Institute for Research in Fundamental Sciences, Iran
Michael Ben-Or	The Hebrew University of Jerusalem, Israel
Fernando Brandao ( <i>Co-chair</i> )	ETH Zürich, Switzerland & UCL, UK
Sergey Bravyi	IBM, USA
Francesco Buscemi	University of Nagoya, Japan
Eric Chitambar	Southern Illinois University, USA
Runyao Duan	University of Technology Sydney, Australia
Michał Horodecki	University of Gdańsk, Poland
Kazuo Iwama	Kyoto University, Japan
Julia Kempe	University of Paris, France & Tel Aviv University, Israel
David Kribs	University of Guelph, Canada
Troy Lee	National University of Singapore, Singapore
Stefano Mancini	Università degli Studi di Camerino, Italy
Ashley Montanaro	University of Cambridge, UK
Ashwin Nayak	IQC and University of Waterloo, Canada
Harumichi Nishimura	Nagoya University, Japan
Stefano Pironio	Université Libre de Bruxelles, Belgium
Pranab Sen	Tata Institute of Fundamental Research, India
Simone Severini ( <i>Chair</i> )	UCL, UK
Rolando Somma	Los Alamos National Laboratory, USA
Xiaoming Sun	China Academy of Science, P. R. China
Pawel Wocjan	University of Central Florida, USA
Bei Zeng	University of Guelph, Canada

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



