Lecture Notes in Computer Science 5906

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Alfred Kobsa
University of California, Irvine, CA, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
TU Dortmund University, Germany

Madhu Sudan
Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Andrew Childs Michele Mosca (Eds.)

Theory of Quantum Computation, Communication, and Cryptography

4th Workshop,TQC 2009
Waterloo, Canada, May 11-13, 2009
Revised Selected Papers

Springer

Volume Editors

Andrew Childs
Institute for Quantum Computing
and Department of Combinatorics and Optimization
University of Waterloo
Waterloo, ON, N2L 3G1 Canada
E-mail: amchilds@iqc.ca

Michele Mosca
Institute for Quantum Computing
and Department of Combinatorics and Optimization
University of Waterloo
Waterloo, ON, N2L 3G1 Canada
E-mail: mmosca@iqc.ca
and
Perimeter Institute for Theoretical Physics
31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada

Library of Congress Control Number: 2009940405

CR Subject Classification (1998): F, D, C.2, G.1-2, E.3, J.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-642-10697-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-10697-2 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12810949 06/3180 5 4 3 2 1 0

Preface

The Workshop on Theory of Quantum Computation, Communication, and Cryptography (TQC) is an annual workshop on theoretical aspects of quantum information processing. The goal of the workshop is to foster developments in this rapidly growing, interdisciplinary field by providing a forum for the presentation and discussion of original research.

The fourth iteration of TQC was held during May 11–13, 2009, at the Institute for Quantum Computing at the University of Waterloo in Waterloo, Ontario, Canada. The workshop included invited talks, contributed talks, and a poster session, as well as a rump session consisting of short talks on recent developments. Authors of selected contributed talks were invited to submit a paper to these proceedings.

TQC 2009 would not have been possible without the contributions of numerous individuals and organizations, and we sincerely thank them for their support.

In putting together the scientific program, we were very grateful for the hard work and advice of the Program Committee, listed herein. We also appreciate the help of the following additional reviewers: Roger Colbeck, Markus Grassl, Stefan Hengl, Tohya Hiroshima, Min-Hsiu Hsieh, Akinori Kawachi, Harumichi Nishimura, Rudy Raymond, Douglas Stebila, and Tzu-Chieh Wei.

The logistics of the workshop were expertly managed by the Local Organizing Committee, also listed herein, and we thank them for their efforts to make the workshop a success. We are also thankful for the assistance of Kim Kuntz, Wendy Reibel, Alison Conway and Sharon McCalla, who provided administrative support, and Colin Bell, who helped with computing and audiovisual resources.

We would like to thank the invited speakers, Masato Koashi, John Preskill, Miklos Santha, Graeme Smith, and Stephanie Wehner, for their contributions to the program.

TQC 2009 was made possible by financial support from the Institute for Quantum Computing, the Perimeter Institute for Theoretical Physics, the Fields Institute for Research in Mathematical Sciences, MITACS, and QuantumWorks; we thank these organizations for their important contributions. Finally, we would like to thank Springer for publishing the proceedings of TQC in the *Lecture Notes in Computer Science* series.

September 2009

Andrew Childs
Michele Mosca

Organization

Program Committee

Panos Aliferis	IBM T.J. Watson Research Center, USA
Dave Bacon	University of Washington, USA
Andrew Childs	IQC, University of Waterloo, Canada (Chair)
Masahito Hayashi	Tohoku University, Japan
Patrick Hayden	McGill University, Canada
Hiroshi Imai	University of Tokyo/ERATO-SORST, Japan
Kazuo Iwama	Kyoto University, Japan
Yasuhito Kawano	NTT, Japan
Norbert Lütkenhaus	IQC, University of Waterloo, Canada
Chiara Macchiavello	INFM, University of Pavia, Italy
Michele Mosca	IQC, University of Waterloo/Perimeter Institute, Canada
Maarten van den Nest	MPQ, Germany
Masanao Ozawa	Nagoya University, Japan
Robert Raussendorf	University of British Columbia, Canada
Ben Reichardt	IQC, University of Waterloo, Canada
Renato Renner	ETH Zurich, Switzerland
Alain Tapp	Université de Montréal, Canada
Barbara Terhal	IBM T.J.Watson Research Center, USA
John Watrous	IQC, University of Waterloo, Canada
Andreas Winter	University of Bristol, UK/CQT, National University of Singapore
Shigeru Yamashita	Nara Institute of Science and Technology, Japan

Organizing Committee

Anne Broadbent	IQC, University of Waterloo, Canada
Sarah Croke	Perimeter Institute, Canada
Dmitri Maslov	IQC, University of Waterloo, Canada
Michele Mosca	IQC, University of Waterloo/Perimeter Institute, Canada (Chair)
Simone Severini	IQC, University of Waterloo, Canada
Tzu-Chieh Wei	IQC, University of Waterloo, Canada

Table of Contents

Solutions to the Hidden Subgroup Problem on Some Metacyclic Groups 1
Demerson N. Gonçalves, Renato Portugal, and Carlos M.M. Cosme

Quantum Online Memory Checking 10
Wim van Dam and Qingqing Yuan

On the Structure of Protocols for Magic State Distillation 20
Earl T. Campbell and Dan E. Browne

Statistically-Hiding Quantum Bit Commitment from Approximable-Preimage-Size Quantum One-Way Function 33
Takeshi Koshiba and Takanori Odaira

On the Security and Degradability of Gaussian Channels 47
Stefano Pirandola, Samuel L. Braunstein, and Seth Lloyd

Universal Quantum Computation with a Non-Abelian Topological Memory 56
James R. Wootton, Ville Lahtinen, and Jiannis K. Pachos

Conditions for the Approximate Correction of Algebras 66
Cédric Bény

Optimal State Merging without Decoupling 76
Jean-Christian Boileau and Joseph M. Renes

Optimal Trading of Classical Communication, Quantum Communication, and Entanglement 85
Min-Hsiu Hsieh and Mark M. Wilde

On the Power of the PPT Constraint in the Symmetric Extensions Test for Separability 94
Miguel Navascués, Masaki Owari, and Martin B. Plenio

Author Index 107