

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, 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

Yasuhito Kawano Michele Mosca (Eds.)

Theory of Quantum Computation, Communication, and Cryptography

Third Workshop, TQC 2008

Tokyo, Japan, January 30–February 1, 2008

Revised Selected Papers

Volume Editors

Yasuhito Kawano

NTT Communication Science Laboratories

3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan

E-mail: kawano@theory.brl.ntt.co.jp

Michele Mosca

Institute for Quantum Computing

University of Waterloo

Waterloo, Ontario 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: 2008938495

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 3-540-89303-2 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-89303-5 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 is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2008

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12443833 06/3180 5 4 3 2 1 0

Preface

The Workshop on Theory of Quantum Computation, Communication, and Cryptography (TQC) focuses on theoretical aspects of quantum computation, quantum communication, and quantum cryptography, which are part of a larger interdisciplinary field that casts information science in a quantum mechanical framework.

The third TQC was held from January 30 to February 1, 2008, at the University of Tokyo, Tokyo, Japan. It consisted of invited talks, contributed talks and a poster session. A selection of these contributors were invited to submit a paper to this *Lecture Notes in Computer Science* (LNCS) proceedings.

The field of quantum information processing is rapidly growing in depth and in breadth. TQC is a workshop dedicated to the presentation and discussion of original research. While most research in quantum information is published in a wide range of journals and conference proceedings in computer science, physics, mathematics and other traditional areas of science, there is a growing niche for high-quality journals and proceedings dedicated to research in quantum information. TQC is one of the first such conferences or workshops that has decided to publish a selection of the submissions in an official proceedings of the workshop to be published in the LNCS series.

We are extremely fortunate to have had the support and advice of our Program Committee (listed here) and are very grateful for all their hard work. We also appreciate the help of the following additional reviewers: Jean-Christian Boileau, Jop Briet, David Feder, Francois Le Gall, Hector Garcia, Tohya Hiroshima, and Casey Myers.

We also extend our sincere thanks to the local Organizing Committee for pulling together all the local and logistical aspects of the workshop so successfully.

Lastly, many thanks to NTT for sponsoring TQC 2008, to the University of Tokyo for their generous support, and to Springer for agreeing to publish these proceedings in the LNCS series.

May 2008

Yasuhito Kawano
Michele Mosca

Organization

Program Committee

| | |
|-------------------|---|
| Michele Mosca | Institute for Quantum Computing (UW), and Perimeter Institute, Waterloo, Chair |
| Richard Cleve | Institute for Quantum Computing (UW), and Perimeter Institute, Waterloo |
| Masahito Hayashi | JST ERATO-SORST/Tohoku University |
| Peter Høyer | University of Calgary |
| Hiroshi Imai | University of Tokyo/JST ERATO-SORST |
| Nobuyuki Imoto | Osaka University |
| Kazuo Iwama | Kyoto University |
| Richard Jozsa | University of Bristol |
| Yasuhito Kawano | NTT |
| Takeshi Koshihara | Saitama University |
| Hoi-Kwong Lo | University of Toronto |
| Igor L. Markov | University of Michigan |
| Mio Murao | University of Tokyo |
| Tatsuaki Okamoto | NTT |
| Masanao Ozawa | Tohoku University |
| Adam Smith | Pennsylvania State University |
| Barbara Terhal | IBM T.J. Watson Research Center |
| Guifre Vidal | University of Queensland |
| Shigeru Yamashita | Nara Institute of Science and Technology |

Organizing Committee

| | |
|--------------------|---------------------|
| Yasuhito Kawano | NTT, Chair |
| Go Kato | NTT |
| Yumi Nakajima | NTT |
| Yasuhiro Takahashi | NTT |
| Seiichiro Tani | NTT/JST ERATO-SORST |

Table of Contents

| | |
|--|-----|
| Classical and Quantum Algorithms for Exponential Congruences | 1 |
| <i>Wim van Dam and Igor E. Shparlinski</i> | |
| Quantum Algorithms for Evaluating MIN-MAX Trees | 11 |
| <i>Richard Cleve, Dmitry Gavinsky, and D.L. Yonge-Mallo</i> | |
| Irreversibility of Entanglement Loss | 16 |
| <i>Francesco Buscemi</i> | |
| Quadratic Form Expansions for Unitaries | 29 |
| <i>Niel de Beaudrap, Vincent Danos, Elham Kashefi, and Martin Roetteler</i> | |
| Improved Constructions of Quantum Automata | 47 |
| <i>Andris Ambainis and Nikolajs Nahimovs</i> | |
| An Application of the Deutsch-Jozsa Algorithm to Formal Languages and the Word Problem in Groups | 57 |
| <i>Michael Batty, Andrea Casaccino, Andrew J. Duncan, Sarah Rees, and Simone Severini</i> | |
| An Elementary Optical Gate for Expanding Symmetrically Shared Entanglement | 70 |
| <i>Toshiyuki Tashima, Şahin Kaya Özdemir, Takashi Yamamoto, Masato Koashi, and Nobuyuki Imoto</i> | |
| Security Bounds for Quantum Cryptography with Finite Resources | 83 |
| <i>Valerio Scarani and Renato Renner</i> | |
| On the Design and Optimization of a Quantum Polynomial-Time Attack on Elliptic Curve Cryptography | 96 |
| <i>Donny Cheung, Dmitri Maslov, Jimson Mathew, and Dhiraj K. Pradhan</i> | |
| Architecture of a Quantum Multicomputer Implementing Shor's Algorithm | 105 |
| <i>Rodney Van Meter, W.J. Munro, and Kae Nemoto</i> | |
| Author Index | 115 |