REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT DATE	3. DATES COVERED *(From - To)*
05-09-2003	Final	01-08-2002 to 31-03-2003

4. TITLE AND SUBTITLE

Quantum Computing Program at the Mathematical Sciences Research Institute

Final Report

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N00014-02-1-0747

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Robert Megginson, Deputy Director

Hugo Rossi, Deputy Director

5d. PROJECT NUMBER
02PR12722-00

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Mathematical Sciences Research Institute
17 Gauss Way
Berkeley, CA 94720-5070

8. PERFORMING ORGANIZATION REPORT NUMBER
ONR N00014-02-1-0747
Final

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
Ballston Centre Tower One
800 North Quincy Street
Arlington, VA 22217-5660

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

12. DISTRIBUTION AVAILABILITY STATEMENT

Approved for Public Release; distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Through the grant for which this report is written, five workshops in quantum computing were partially funded, as well as senior researchers in mathematics, computer science, physics, and related fields, to participate in the workshops and other activities held concurrently at MSRI. This final report describes the workshops and their schedules, and details the participants funded through this grant.

15. SUBJECT TERMS

quantum computing workshops MSRI

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPONE NUMBER *(Include area code)*

Quantum Computing Program
at the
Mathematical Sciences Research Institute (MSRI)
August 19, 2002 to December 20, 2002

Final Report

The Scientific Program

This program brought together mathematicians, computer scientists and physicists during a four month period to exchange information on the latest research on problems of quantum computing, particularly the development of quantum algorithms, and to collaborate on the further development of the subject. At any time during this period there were at least 30 scientists involved in the program, all of whom stayed for at least a month, and many of whom stayed for three months or longer. MSRI funded X postdoctoral fellows (researchers 3 years or less from their Ph.D.) in connection with this program, who were in residence for the five month period August-December, 2002.

In addition to the regular weekly seminars and discussion groups, there were four one-week workshops to which scientists from outside MSRI are invited, as well as regular MSRI members. These workshops featured 3-4 lectures daily for a population of 80 or more workshop participants. The first of these is the Introductory workshop, concentrating on a survey of the status of the field at the initiation of the program; the other three were programmatic workshops, presenting the most recent research in a particular topic, in both lecture and discussion formats.

The funding from this grant was used in two ways: to fund the long-term stays of certain central researchers, and to cover the expenses of invited participants to the three programmatic workshops. Both were crucial to the success of the program; the first in keeping people key to the program in residence and focused on the objectives of the program, and the second in providing opportunity for cross-fertilization of ideas among large groups of people.

Key Personnel

Here we provide a brief description of the contribution of each person supported by the program.

Michael Ben-Or, Computer Science, Hebrew University, Jerusalem. . In residence for four months (the entire program). An expert in the security of quantum key distribution protocols. He gave two of the introductory talks on security, and a research talk on quantum security in December.

Samuel Lomonaco, Computer Science & Electrical Engineering, University of Maryland, Baltimore. In residence for three months. Originally trained as a topologist and geometer, turned to computer science, and now works on applications of quantum computation to theoretical problems. He gave a workshop talk on Feynman integrals.

Dominic Mayers, Mathématiques et Informatique Université de Sherbrooke. In residence for three months. An expert on quantum cryptography, he gave a seminar talk and a workshop talk on quantum information theory.

Michele Mosca, Mathematics, University of Waterloo. In residence 6 weeks, September and December. She gave two talks on quantum searching and algorithms in the introductory workshop, and a research exposition of derandomization of quantum algorithms in December.

Miklo Santha, Senior Researcher LRI, Universite de Paris-Sud, 11. In residence for four months (the entire program). His field of interest is computational complexity; has developed an efficient quantum algorithm for the hidden translation problem. He gave several talks.

Leonard Schulman, Department of Computer Science, California Institute of Technology. In residence for four months (the entire program). An expert on algorithms and communications protocols, with a strong background in combinatorics and probability. He was one of the organizers of, and gave a talk in the introductory workshop and was a key seminar leader during the entire program.

John Waltrous, Mathematics, University of Calgary. In residence one month (November-December). His area of interest is phase estimation and factoring of quantum algorithms. He gave two talks in the introductory workshop, and another seminar in the workshop on Quantum Information Processing (for which he was one of the organizers).

Wojcieh Zurek, Fellow, LANL In residence 5 weeks. His area of interest is quantum cryptography; he gave a seminar talk.

Workshop Descriptions

Introductory workshop in quantum computation (August 26–30, 2002). Organized by: Dorit Aharonov, Leonard Schulman, and Umesh Vazirani.

This workshop provided a mathematical introduction to the fundamental topics of quantum computation. The topics included quantum information theory, quantum computational complexity theory, the representation theory of finite groups and properties of quantum fourier transforms, quantum algorithms, quantum communication complexity, quantum error-correcting codes and fault-tolerant quantum computation, and quantum cryptography.

Quantum algorithms and complexity (at Banff International Research Station, September 23–27, 2002). Organized by: Richard Cleve, Peter Shor, and Umesh Vazirani

This workshop discussed models for quantum computation, quantum algorithms (including quantum Fourier transforms, period finding, hidden subgroup problems), quantum complexity theory (including quantum complexity classes, quantum lower-bounds, quantum communication complexity, quantum NP-completeness and quantum interactive proofs), fault-tolerance (including quantum error-correction, concatenation codes, decoherence-free subspaces).

Due to the Oberwolfach-style setting of the workshop, the model adopted was somewhat different from that of MSRI's usual workshop. The workshop was organized around talks early and late in the day, with substantial time between the early and late talks for participants to interact with each other in small groups and to work on individual problems of interest.

Models of quantum computing (at the Institute for Pure and Applied Mathematics in Los Angeles, October 21–23, 2002). Organized by: David Di Vincenzo (Watson-IBM), and Peter Shor (AT&T), Chair

This workshop focused on models and implementation for quantum computing. The proposed physical architectures for quantum computers have been quite diverse, as well as the corresponding mathematical models they are based on. In many cases, the interplay between mathematical models and proposed physical architectures has proven to be quite fruitful, resulting in advances in both the physics and the mathematics of quantum computers. Still there are many open problems, including decoherence, fault tolerance, and materials properties. In this workshop we explored these interactions further. This workshop brought together experts representing a variety of different approaches to quantum computing: semiconductors, superconductors, NMR and trapped particles, as well as more novel approaches such as anyons. The aim of the workshop was to promote research on quantum computing and the different approaches to its implementation and to help bring the open problems in this field to the attention of mathematicians and nanosystem researchers.

Quantum information and cryptography (November 4–8, 2002). Organized by: Richard Jozsa and Mary Beth Ruskai

This workshop was dedicated to mathematical aspects of quantum information theory and quantum cryptography. Fundamental issues included the study of entanglement (its manipulation, classification and

quantification), compression and coding theorems for quantum information, quantum channel capacities, structural properties of quantum operations (including related theory of operator algebras), and mathematical questions arising from quantum cryptographic protocols such as security proofs and other novel features of quantum encryptions.

Although the focus was on mathematical aspects of quantum information theory, the participants came from a broad spectrum of backgrounds in mathematics, physics, engineering and computer science. Some of the cryptography talks included discussion of recent experiments and feasibility of various protocols, which is valuable for those concerned with such topics as security for realistic, as well as idealized, systems. The talks were uniformly well attended, often followed by lively discussion. In the breaks there was active scientific discussion, indicating an effective selection of participants, as well as stimulating talks. Most participants would agree that the highlight of the week was the announcement by Peter Shor of a new fundamental cornerstone result of the subject viz. a general formula for the quantum information capacity of a general noisy quantum channel. An extra session in a lunch break was organized to allow further exposure of the proof's details.

In addition to the program of invited 45 min talks, there was a session of short 15 min contributed talks which was organized at the workshop itself on the first day. The aim was to give younger workers or new (less established) workers in the field an opportunity to announce their results to the assembled audience that included many of the foremost established researchers in the subject. It was possible to include nine such contributed talks and the session was highly successful, also in enhancing communication between participants during the workshop.

Since the workshop took place during the MSRI semester on quantum computation, it was possible to allot a considerable part of the workshop funding to support post-docs and younger workers. This was of particular benefit as the subject of quantum information theory currently enjoys a high international profile and is consequently attracting new younger workers of high quality.

Overall the workshop was very successful both in the uniformly excellent quality of talks and the interactions between participants. Although there was a fairly full schedule of talks, they were spaced to allow informal discussion in between, and many participants remarked that the balance was good. The organizers commented that they could not identify any particular weaknesses. In particular, they commented that he facilities and general ambience at MSRI were very good.

Quantum information processing (December 13–17, 2002). Organized by: Dorit Aharonov, Charles Bennett, Harry Buhrman, Isaac Chuang, Mike Mosca, Umesh Vazirani, and John Watrous

Quantum information processing lives at the intersection of quantum mechanics and computer science. It tries to improve on classical computers and classical complexity bounds by making use of quantum mechanical phenomena. After Peter Shor's 1994 discovery of efficient quantum algorithms for factoring and the discrete log (threatening current "classical" cryptography), the field has grown explosively in both computer science and physics. This workshop featured interdisciplinary presentations by leading mathematicians, computer scientists, and physicists working in this area.

There were five talks a day for each of the five days. On the first day the talks centered about issues of polynomial time quantum algorithms, hidden translations and some coding problems. The workshop turned then toward probabilistic methods in quantum computing. This series of talks was succeeded by a series on quantum computational complexity, entanglement and quantum protocols. The final topics were: quantum codes, decoding codes and secure coding keys.

Introductory Workshop in Quantum Computation

Schedule

Date	Time	Speaker	Title
Monday, Aug 26	9:30 am to 10:30 am	**Umesh Vazirani**	*Introduction to quantum computing*
	11:00 am to 12:00 pm	**Michele Mosca**	*Introduction to quantum algorithms: The basics*
	2:00 pm to 3:00 pm	**Ashwin V. Nayak**	*Quantum information theory, part 1*
	3:30 pm to 4:30 pm	**Gilles Brassard**	*Quantum cryptography*
	4:30 pm to 4:45 pm	**Henry A. Warchall**	*NSF funding for quantum computation*
Tuesday, Aug 27	9:30 am to 10:30 am	**Sean Hallgren**	*Quantum Fourier transforms*
	11:00 am to 12:00 pm	**John Watrous**	*Quantum algorithms: Phase estimation and factoring*
	2:00 pm to 3:00 pm	**Dave Bacon**	*Quantum error correction*
	3:30 pm to 4:30 pm	**Leonard J. Schulman**	*Group representation theory and quantum algorithms*
Wednesday, Aug 28	9:30 am to 10:30 am	**Ashwin Nayak**	*Quantum information theory, part 2*
	11:00 am to 12:00 pm	**Michele Mosca**	*Quantum searching, counting and generalizations*
Thursday, Aug 29	9:30 am to 10:30 am	**Gilles Brassard**	*Quantum teleportation and applications*
	11:00 am to 12:00 pm	**Michael Ben-Or**	*Security of quantum key distribution protocols, part 1*
	2:00 pm to 3:00 pm	**Michael Ben-Or**	*Security of quantum key distribution protocols, part 2*
	3:30 pm to 4:30 pm	**Scott Aaronson**	*Quantum lower bounds*
Friday, Aug 30	9:30 am to 10:30 am	**Dorit Aharonov**	*Fault-tolerant quantum computation*
	11:00 am to 12:00 pm	**John Watrous**	*Quantum interactive proofs*
	2:00 pm to 3:00 pm	**Ronald de Wolf**	*Quantum communication complexity*
	3:30 pm to 4:30 pm	**Dave Bacon**	*Novel models for quantum computation*

Quantum Algorithms and Complexity (held at the Banff International Research Station)

Schedule

Date	Time	Speaker	Title
Monday, Sep 23	9:30 am to 10:30 am	**Sean Hallgren**	*Polynomial-time algorithms for Pell's equation and the principal ideal problem*
	11:00 am to 11:30 am	**Miklos Santha**	*An efficient algorithm for the hidden translation problem*
	6:00 pm to 7:00 pm	**John Watrous**	*One-dimensional quantum walks*
Tuesday, Sep 24	9:30 am to 10:30 am	**Scott Aaronson**	*Quantum lower bounds you haven't seen before*
	11:00 am to 11:30 am	**Yaoyun Shi**	*Review of lower bounds for the collision problem*
	6:00 pm to 7:00 pm	**Oded Regev**	*Quantum computation and lattice problems*
Wednesday, Sep 25	9:30 am to 10:30 am	**Dorit Aharonov**	*Quantum sampling, SZK and Markov chains: A different framework for quantum algorithms*
	11:00 am to 11:30 am	**Willem van Dam**	*Efficient quantum algorithms for estimating Gauss sums (joint work with Gadiel Seroussi)*
Thursday, Sep 26	9:30 am to 10:30 am	**Mario Szegedy**	*Quantum decision trees and semidefinite programming*
	11:00 am to 11:45 am	**Ronald de Wolf**	*Quantum computing and locally decodable codes*
	6:00 pm to 7:00 pm	**Andris Ambainis**	*Quantum communication complexity of set disjointness*
Friday, Sep 27	9:30 am to 10:15 am	**Dave Bacon**	*Digitizing quantum correlations*
	10:45 am to 11:30 pm	**Harry Buhrman**	*Combinatorics and quantum nonlocality*
	6:00 pm to 7:00 pm	**Tal Mor**	*Quantum computation without entanglement*

Models of Quantum Computing (joint workshop with the Institute for Pure and Applied Mathematics; held at IPAM)

Schedule

Date	Time	Speaker	Title
Monday, Oct 21	9:30 am to 10:30 am	**Manny Knill**	*On the power of models of quantum computation*
	11:00 am to 12:00 pm	**Jonathan Dowling**	*Linear optics and projective measurements*
	2:00 pm to 3:00 pm	**Hans Briegel**	*Measurement-based quantum computation*
	3:30 pm to 4:30 pm	**Ivan Deutsch**	*Quantum control with ultracold atoms*
	4:30 pm to 5:30 pm	**Eli Yablonovitch**	*The prospects for storing and manipulating quantum information stored on electron spins in semiconductors*
Tuesday, Oct 22	9:00 am to 10:00 am	**John Goodkind**	*Qubits using single electrons over a dielectric*
	10:30 am to 11:30 am	**Atac Imamoglu**	*Quantum dot single photon source: Prospects for applications in quantum information processing*
	11:30 am to 12:30 pm	**Tim Havel**	*Quantum dynamical semigroup tomography*
	2:00 pm to 3:00 pm	**Carl Williams**	*Scalable quantum architectures using efficient nonlocal interactions*
	3:30 pm to 4:30 pm	**Poul Jessen**	*Qubits and quantum gates in optical lattices*
	4:30 pm to 5:30 pm	**Luming Duan**	*Engineering many-body Hamiltonians with ultracold atoms in optical lattices*
Wednesday, Oct 23	9:30 am to 10:30 am	**Daniel Gottesman**	*Beyond the DiVincenzo criteria: Requirements and desiderata for fault-tolerance*
	11:00 am to 12:00 pm	**Vwani Roychowdhury**	*Models of computation for high-performance computing systems*
	2:00 pm to 3:00 pm	**Vadim Smelyanskiy**	*Dynamics of quantum adiabatic computations in random NP-complete problems*
	3:30 pm to 4:30 pm	**Birgitta Whaley**	*Encoded universality: Adapting quantum proce3ssing to physical interactions*
	4:30 pm to 5:30 pm	**Alexei Kitaev**	*Physical models for fault-tolerant quantum computation*

Quantum Information and Cryptography

Schedule

Date	Time	Speaker	Title
Monday, Nov 04	9:15 am to 9:30 am	**MSRI Staff**	*Welcome and Introduction*
	9:30 am to 10:15 pm	**Michal Andrzej Horodecki**	*Information and entanglement in distributed systems: An interplay of resources*
	10:45 am to 11:30 am	**Ignacio Cirac**	*Entanglement properties of Gaussian states*
	11:30 am to 12:15 pm	**Andreas Johannes Winter**	*Remarks on additivity of the Holevo channel capacity and of entanglement of formation*
	2:15 pm to 3:00 pm	**Wojciech Hubert Zurek**	*Environment-assisted invariance, ignorance, and information in quantum physics*
	4:10 pm to 5:10 pm	**Peter Shor**	*Quantum error correction*
Tuesday, Nov 05	9:30 am to 10:15 am	**Christopher King**	*Capacity of the depolarizing channel*
	10:45 am to 11:30 am	**Peter W. Shor**	*Quantum capacity and coherent information*
	11:30 am to 12:15 pm	**Mary Beth Ruskai**	*The structure of completely positive maps and entanglement breaking channels*
	2:15 pm to 3:00 pm	**Denes Petz**	*Monotonicity of quantum relative entropy revisited*
	3:30 pm to 4:15 pm	**Mitsuru Hamada**	*Symplectic codes and quantum capacity of noisy channels*
Wednesday, Nov 06	9:30 am to 10:15 am	**Patrick Marc Hayden**	*The communication cost of entanglement transformations*
	10:45 am to 11:30 am	**Masato Koashi**	*Indistinguishablity and compressibility of quantum states*
	11:30 am to 12:15 pm	**Anthony Chefles**	*General theory of probabilistic quantum state transformations*
	2:00 pm to 2:45 pm	**Debbie Wun Chi Leung**	*Nonlocal quantum resource transformation and unitary bidirectional quantum channels*
	3:15 pm to 5:00 pm	**Various (TBA)**	*Short talks (15 minutes each)*
Thursday, Nov 07	9:30 am to 10:15 am	**Dominic Mayers**	*Quantum universal composability*
	10:45 am to 11:30 pm	**Claude Crepeau**	*Authentication of quantum messages*
	11:30 am to	**Daniel Eric Gottesman**	*Uncloneable encryption*

	12:15 am		
	2:15 pm to 3:00 pm	**Hoi-Kwong Lo**	*Security of quantum key distribution with imperfect devices*
	3:30 pm to 4:15 pm	**Richard John Hughes**	*Quantum cryptography for secure communications*
	4:15 pm to 5:00 pm	**Norbert Lutkenhaus**	*Quantum information and cryptography*
Friday, Nov 08	9:30 am to 10:15 am	**Andrew Charles Doherty**	*Local hidden variable theories for quantum states*
	10:45 am to 11:30 am	**Guifre Vidal**	*Entanglement in quantum phase transitions*
	11:30 am to 12:15 pm	**Karl Gerd Hinrich Vollbrecht**	*Distillation rates beyond qubits*

Quantum Information Processing

Schedule

Date	Time	Speaker	Title
Friday, Dec 13	9:00 am to 9:15 am	**MSRI Staff**	*Welcome and Introduction*
	9:15 am to 10:00 am	**Sean Hallgren**	*Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem*
	10:30 am to 11:15 am	**Miklos Santha**	*Hidden translation and orbit coset in quantum computing*
	11:15 am to 12:00 pm	**Oded Regev**	*On the dihedral hidden subgroup problem*
	2:00 pm to 2:45 pm	**Ruediger Schack**	*Unknown quantum operations: A de Finetti representation theorem*
	2:45 pm to 3:30 pm	**Keiji Matsumoto**	*Universal source coding, soft tomography, and universal concentration*
	4:00 pm to 4:45 pm	**Michael Aaron Nielsen**	*Majorization and quantum information*
Saturday, Dec 14	9:15 am to 10:00 am	**Edward H. Farhi**	*Speedup by quantum walk*
	10:30 am to 11:15 am	**Dorit Aharonov**	*Adiabatic quantum computation: Universality and tools*
	11:15 am to 12:00 pm	**Michele Mosca**	*On the quantum derandomization of algorithms*
	2:00 pm to 2:45 pm	**John Watrous**	*Capturing quantum complexity classes via quantum channels*
	2:45 pm to 3:30 pm	**Claude Crepeau**	*A length n QECC probabilistically correcting (n-1)/2 arbitrary errors*
	4:00 pm to 4:45 pm	**Mary Beth Ruskai**	*Non-Abelian stabilizer codes for quantum error correction*
Sunday, Dec 15	9:15 am to 10:00 am	**Louis Kauffman & Samuel Lomonaco**	*Quantum entanglement*
	10:30 am to 11:15 am	**Willem van Dam**	*Qualifying entanglement with knot theory*
	11:15 am to 12:00 pm	**Leonid Gurvits**	*Classical complexity and quantum entanglement of bipartite mixed states*
	2:00 pm to 2:45 pm	**Gilles Brassard**	*Quantum computation without entanglement*
	2:45 pm to 3:30 pm	**Andreas Johannes Winter**	*Remote preparation of quantum states*

	4:00 pm to 4:45 pm	**Guifre Vidal**	*Entanglement in quantum critical phenomena*
Monday, Dec 16	9:15 am to 10:00 am	**John Preskill**	*Secure quantum key distribution with an uncharacterized source*
	10:30 am to 11:15 am	**Dominic Mayers**	*Composing quantum protocols*
	11:15 am to 12:00 pm	**Sandu Popescu**	*Multi-party entanglement*
	2:00 pm to 5:00 pm	**Variety of Speakers**	*Contributed talks*
Tuesday, Dec 17	9:15 am to 10:00 am	**Alexei Kitaev**	*Quantum coin-flipping*
	10:30 am to 11:15 am	**Michael Ben-Or**	*Simple security proof for quantum key distribution*
	11:15 am to 12:00 pm	**Ronald M. de Wolf**	*Quantum computing, locally decodable codes, and private information retrieval*
	2:00 pm to 2:45 pm	**Rahul Jain**	*Quantum communication complexity of set membership*
	2:45 pm to 3:30 pm	**Patrick Marc Hayden**	*Hiding quantum data*
	4:00 pm to 4:45 pm	**Charles H. Bennett**	*Towards a quantum reverse Shannon theorem*